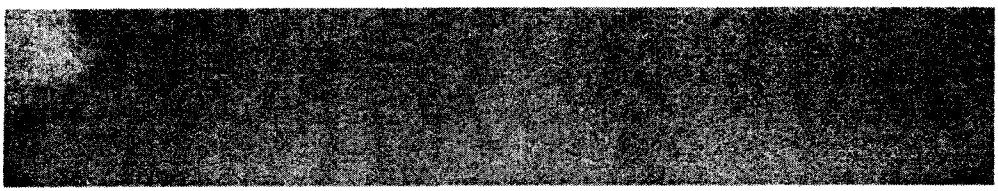


TROUBLESHOOTING, MAINTAINING & REPAIRING NETWORKS

TROUBLESHOOTING, MAINTAINING & REPAIRING NETWORKS

STEPHEN J. BIGELOW

McGraw-Hill/Osborne
New York Chicago San Francisco
Lisbon London Madrid Mexico City
Milan New Delhi San Juan
Seoul Singapore Sydney Toronto

Стивен Дж. Бигелоу

СЕТИ

ПОИСК НЕИСПРАВНОСТЕЙ, ПОДДЕРЖКА И ВОССТАНОВЛЕНИЕ

Санкт-Петербург
«БХВ-Петербург»
2005

УДК 681.3.06
ББК 32.973.202
Б59

Бигелоу С.

Б59 Сети: поиск неисправностей, поддержка и восстановление: Пер. с англ. — СПб.: БХВ-Петербург, 2005. — 1200 с.: ил.

ISBN 5-94157-338-3

Описаны симптомы и проблемы, возникающие в любой области функционирования современных компьютерных сетей, а также вопросы их правильной диагностики. Рассмотрены архитектуры, протоколы, операционные системы, а также все особенности сетевого оборудования: кабелей, сетевых карт, накопителей, адаптеров, хабов, роутеров и т. п. Изложены общие принципы поиска неисправностей и приведены сотни их специфических признаков. Представлены практические приемы сетевого администрирования, резервирования и восстановления данных, обеспечения безопасности.

Для сетевых администраторов

УДК 681.3.06
ББК 32.973.202

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Григорий Добин*
Перевод с английского	*Юрия Гороховского*
Редакторы:	*Леонид Мирошенков, Наталья Довгулевич*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Зинаида Дмитриева*
Дизайн обложки	*Игоря Цырульникова*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 30.11.04.
Формат 70×100$^{1}/_{16}$. Печать офсетная. Усл. печ. л. 96,75.
Тираж 4000 экз. Заказ № 1053
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Гигиеническое заключение на продукцию, товар № 77.99.02.953.Д.001537.03.02 от 13.03.2002 г. выдано Департаментом ГСЭН Минздрава России.

Отпечатано с готовых диапозитивов
в ОАО "Техническая книга"
190005, Санкт-Петербург, Измайловский пр., 29

ISBN 0-07-222257-3 (англ.)
ISBN 5-94157-338-3 (рус.)

Содержание

Об авторе

Стивен Дж. Бигелоу (Stephen J. Bigelow) является основателем и президентом Dynamic Learning Systems (Системы активного обучения) — компании, которая занимается разработкой технической документации, исследованиями и небольшой издательской деятельностью и специализируется в области обслуживания электронного и компьютерного оборудования. Бигелоу является автором 15 объемных книг, вышедших в издательстве TAB/McGraw-Hill, и более 100 больших статей, написанных для таких крупных журналов по электронике, как "Popular Electronics", "Electronics NOW", "Circuit Cellar INK" и "Electronic Service & Technology". Бигелоу сотрудничает в качестве внештатного редактора с журналом "CNET", в котором он делает колонку под названием "PC Mechanic", а также публикует ключевые статьи. Его статьи также регулярно появляются в журнале "SmartComputing". Кроме того, Бигелоу является редактором и издателем "The PC Toolbox" — первого информационного бюллетеня, рассчитанного на любителей и специалистов в области обслуживания компьютерного оборудования. Бигелоу получил диплом и степень бакалавра по специальности "инженер-электрик" Центрального новоанглийского колледжа (Central New England College) города Вустера (Worcester, США, штат Массачусетс). Связаться с автором можно на сайте **www.dlspubs.com**.

Технические редакторы

Гэри К. Кеслер (Gary C. Kessler) является адъюнкт-профессором и директором программ по компьютерным сетям в колледже Шамплейн (Champlain College) города Берлингтон (Burlington, США, штат Вермонт). Кроме того, он — директор проектов по безопасности в Центре информационных технологий штата Вермонт (Vermont Information Technology Center). Также он является независимым консультантом, специализирующимся на вопросах, связанных с безопасностью компьютеров и компьютерных сетей, протоколов и приложений сети Интернет и TCP/IP, электронной коммерции и телекоммуникационных технологий и прикладных программ. Гэри часто выступает на конференциях. Он автор двух книг и более чем 60 статей, посвященных разнообразным вопросам технологии. У Гэри двое детей, студентов колледжа, он живет в городе Колчестер (США, штат Вермонт). Более подробную информацию можно найти на сайте **http://www.garykessler.net/**.

Ричард Каррара (Richard Carrara), CCIE (№ 7288) (Cisco Certified Installation Engineer — инженер по установке, сертификат компании Cisco Systems), CISSP (Certified Information Systems Security Professional — сертифицированный специалист по безопасности информационных систем), (техническая редакция следующих глав: 2, 3, 5—8, 13—15 и 26), в настоящее время является старшим архитектором компьютерных сетей в корпорации Data Return, находящейся в городе Ирвинг (Irving, США, штат Техас). Он специалист по установке и безопасности информационных систем с более чем восьмилетним опытом в области информационных технологий. Специализируется на разработке и строительстве безопасных, крупномасштабных компьютерных сетей, использующих интернет-протокол. Связаться с Ричардом можно по электронной почте: **rcarrara@hotmail.com**.

Соавторы

Л. Дж. Закер (L. J. Zacker) (глава 2) начал заниматься большими ЭВМ и персональными компьютерами в середине 1980-х годов, и с тех пор поработал в качестве сетевого администратора, программиста, консультанта по безопасности больших компьютерных систем и локальных сетей. В настоящее время сотрудничает с разными издательствами, в том числе Microsoft Press и Windows 2000 Magazine, где в качестве автора и редактора участвовал в создании множества книг и статей.

Глен Карти (Glen Carty), CCIE, (глава 3), является автором книги "Организация широкополосных сетей" ("Broadband Networking"), выпущенной в издательстве McGraw-Hill/Osborne. С начала 1980-х годов занимается разработкой и строительством локальных и глобальных компьютерных сетей. Работал в качестве старшего менеджера и занимался глобальной разработкой и стандартами разработки для сетевых решений, предлагаемых компанией IBM Global Network.

Тоуби Дж. Велте (Toby J. Velte), доктор философии, CCNA (Cisco Certified Network Associate — консультант по компьютерным сетям), CCDA (Cisco Certified Design Associate — консультант по дизайну, сертификат компании Cisco Systems), MCSE+I (Microsoft Certified Systems + Installation Engineer — системный инженер и инженер по установке, сертификат компании Microsoft), (главы 5 и 26), является общепризнанным лидером в области сетевой передачи данных. Д-р Велте основал четыре высокотехнологичных компании и является соавтором восьми книг, вышедших в издательстве McGraw-Hill/Osborne.

Роберт К. Элсенпитер (Robert C. Elsenpeter) (главы 5 и 26), является автором книг и разработчиком Web-контента и имеет различные награды за работу в области журналистики. В качестве соавтора участвовал в создании таких книг, как "Электронный бизнес: руководство для начинающих" ("eBusiness: A Beginner's Guide"), "Волоконно-оптические компьютерные сети: руководство для начинающих" ("Optical Networking: A Beginner's Guide") и "Сетевое администрирование на основе операционной системы Windows XP Professional" ("Windows XP Professional Network Administration"), вышедших в издательстве McGraw-Hill/Osborne.

Гилберт Хелд (Gilbert Held) (глава 6) — автор и лектор, лауреат многих премий. Гил является автором более чем 50 книг и 450 статей по технике. Кроме того, он представлял Соединенные Штаты на конференциях, проходивших в Москве и Иерусалиме. Связаться с Гилом можно через электронную почту по адресу: **gil_held@yahoo.com**.

Кормак Лонг (Cormac Long), CCSI (Cisco Certified Systems Instructor — инструктор по сетям с правом преподавания, сертификат компании Cisco Systems), (глава 7), является независимым консультантом с более чем четырнадцатилетним инженерным опытом в области организации взаимодействия между локальными и глобальными сетями. Разработал и установил несколько крупных локальных и глобальных сетей для заказчиков из Соединенных Штатов и Европы. Получил степень бакалавра по электронной технике и степень магистра по телекоммуникациям. Является автором двух книг, посвященных теме объединения сетей, обе вышли в издательстве McGraw-Hill/Osborne: "Организация межсетевого взаимодействия и выявление неисправностей в компьютерных сетях при помощи оборудования фирмы Cisco" ("Cisco Internetworking and Troubleshooting") и "Разработка компьютерных сетей с использованием Интернет-протокола" ("IP Netwrok Design"). Будучи всемирно признанным экспертом по передаче данных и телекоммуникациям, Кормак Лонг часто выступает на конференциях и участвовал в живых Web-трансляциях, посвященных темам объединения компьютерных сетей, построенных на основе интернет-протокола.

Джэрд М. Насбом (Jared M. Nussbaum) (главы 8, 13 и 14) работает в сфере разработки сетей передачи данных и телекоммуникаций в течение последних 14 лет и специализируется на разработке, управлении и обеспечении безопасности системных архитектур и сетей передачи данных. Имеет степень бакалавра по управлению частными предприятиями и компаниями, полученную в Университете Хофстра (Hofstra University). В апреле 1997 г. мистер Насбом выступил в качестве одного из основателей компании OnSiteAccess, Inc. — провайдера телекоммуникаций для зданий. В ней он был ключевым специалистом по разработке сетевой инфраструктуры, что является основой информационных услуг, предоставляемых корпорацией OnSiteAccess. Кроме того, мистер Насбом отвечал за разработку и управление информационными продуктами, а также руководил группами по системной архитектуре и администрированию. В мае 1995 г. мистер Насбом основал компанию American DataNet, Inc., которая специализировалась на предоставлении высокоскоростного доступа в Интернет и разработке глобальных компьютерных сетей для академических и корпоративных сообществ.

Кейт Страсберг (Keith Strassberg) (глава 15) является опытным консультантом в области обеспечения безопасности информационных систем. Имеет степень бакалавра по бухгалтерскому делу Бингемтонского университета (Binghamton University). Мистер Страсберг получил свой диплом бухгалтера (CPA, certified public accountant — дипломированный бухгалтер, имеет право выступать в качестве независимого аудитора, бухгалтера-ревизора) во время работы в компании "Группа по компьютерному управлению рисками Артура Андерсена" (Computer Risk Management Group of Arthur Andersen, LLP (Limited Liability Partnership — товарищество с ограниченной ответственностью)), в которой он помогал клиентам выявлять и минимизировать производственные, технологические и коммерческие риски в своих информационных системах. В июне 1999 г. мистер Страсберг присоединился к "Гринвичским Технологическим Партнерам" (Greenwich Technology Partners, GTP). Работая в этой компании в

области компьютерной безопасности, мистер Страсберг помог множеству клиентов улучшить уровень своей сетевой безопасности посредством создания наилучшей конфигурации средств межсетевой защиты. Является автором книги "Полное руководство по аппаратно-программным средствам межсетевой защиты" ("Firewalls: The Complete Reference"), а также автором одной из глав книги "Безопасность: архитектура, разработка, развертывание и операции" ("Security Architecture, Design, Deployment, and Operations), вышедшей в издательстве RSA Press. Связаться с Кейтом можно через электронную почту по адресу: **kstrassberg@yahoo.com**.

Предупреждения

ВАЖНО, чтобы вы прочитали и поняли нижеследующую информацию. Пожалуйста, прочтите ее внимательно!

Личный риск и ограничение ответственности

Ремонт персональных компьютеров, периферийных устройств и компьютерных сетей предполагает некоторую долю личного риска. Соблюдайте крайнюю осторожность при работе с источниками переменного тока и высокого напряжения. Мы приложили все усилия, чтобы определить и уменьшить возможности личного риска. Настоятельно рекомендуем вам внимательно прочитать данную книгу *до* выполнения описанных в ней процедур. Если вы не уверены в том, что понимаете какие-либо из описанных процедур, НЕ выполняйте их и обратитесь к квалифицированным специалистам.

НИ АВТОР, НИ ИЗДАТЕЛЬ, НИ КТО-ЛИБО ЕЩЕ, ПРЯМО ИЛИ КОСВЕННО СВЯЗАННЫЙ С ИЗДАНИЕМ ДАННОЙ КНИГИ, НЕ ДАЕТ НИКАКОЙ ЯВНОЙ ИЛИ ПОДРАЗУМЕВАЕМОЙ ГАРАНТИИ ОТНОСИТЕЛЬНО ДАННОГО МАТЕРИАЛА, ВКЛЮЧАЯ, В ТОМ ЧИСЛЕ, ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ КАЧЕСТВА И ГОДНОСТИ ДЛЯ ПРОДАЖИ ИЛИ КАКОЙ-ЛИБО ДРУГОЙ ЦЕЛИ. Кроме того, ни автор, ни издатель, ни кто-либо еще, прямо или косвенно связанный с изданием этой книги, не несет ответственности за какие-либо ошибки в данном материале или за случайный или косвенный вред, ущерб или финансовые и имущественные убытки в результате использования (или невозможности использования) материала и программного обеспечения, содержащегося в настоящем издании. Данный материал и программное обеспечение поставляются "КАК ЕСТЬ", и читатель несет всю ответственность и риски, связанные с их использованием.

Предупреждение о поставщиках

Названия Web-сайтов, продуктов, материалов, оборудования, производителей, поставщиков услуг и торговых компаний, перечисленные в данной книге, используют-

ся только для ссылок. Упоминание и использование этих названий в данной книге не означает поддержки тех или иных лиц или организаций и не является свидетельством качества производимых ими продуктов или оказываемых ими услуг, а также не служит для подтверждения их деловой или профессиональной честности. Автор, издатель, а также любые другие лица, прямо или косвенно связанные с изданием данной книги, не несут никакой ответственности за любые финансовые и имущественные убытки или случайный и косвенный вред, который может возникнуть при контактах или деловом сотрудничестве с любыми упомянутыми организациями или лицами.

Благодарности

Такую книгу, как эта, невозможно создать без щедрой помощи, искренней поддержки и одобрения других людей. Я хотел бы поблагодарить тех, кто помог мне в работе над этим изданием.

- Прежде всего, хочу поблагодарить Трейси Данкелбергер, Эмму Экер, Марка Карменди, Мишель Галишиа, Джин Баттерфилд и всех остальных сотрудников издательства McGraw-Hill/Osborne за их неизменное терпение и настойчивость.
- Благодарю также Гэри Кеслера за его беспощадно честные комментарии и критику. Надеюсь, что в конце концов я создал книгу, которая достойна потраченного им времени и усилий.
- Спасибо Диане Гандерсон из компании Network Instruments за анализатор протоколов Observer Suite (*см. сайт компании по адресу:* **www.networkinstruments.com**).
- Спасибо Джону Туру из компании Maxtor за сетевое запоминающее устройство NAS 3000 (*см. сайт компании по адресу:* **www.maxtor.com**).
- Спасибо Диане Йинг из компании Linksys за возможность использования их беспроводного IP-маршрутизатора, беспроводной сетевой карты спецификации USB, беспроводной сетевой карты спецификации PCMCIA, KVM-переключателя, сервера GigaCD, голосовых устройств для кабельных линий и DSL, а также сетевых карт и переключателей для Gigabit Ethernet (*см. всю линейку сетевых устройств на сайте* **www.linksys.com**).
- Спасибо Рэймонду Джонсу из компании SonicWall за возможность использования их устройства межсетевой защиты SOHO2 (*см. сайт компании по адресу:* **www.sonicwall.com**).
- Спасибо Джули Декстер из компании APCC за возможность использования их устройства SmartUPS 700 (*см. сайт компании по адресу:* **www.apcc.com**).
- И моя особая благодарность Элу Кертсу из компании Gateway за возможность крайне широкого использования их серверной платформы 7400, что помогло существенным образом расширить содержание этой книги и сделать его более подробным (*см. сайт компании по адресу:* **www.gateway.com**).

И, наконец, хочу выразить свою особую благодарность моей замечательной жене, которая самоотверженно перенесла те одинокие вечера, которых оказалось больше, чем должно было выпасть на ее долю, пока я трудился над этим сложным проектом. Без ее преданного терпения и поддержки эта книга не стоила бы вложенных в нее усилий.

Введение: книга эпохи перемен

Многие годы тому назад персональные компьютеры (ПК) использовались независимо — словно небольшие островки вычислительной мощности, населяющие столы в домах и офисах. И сам факт того, что на каждом ПК зачастую выполнялась отличная от других версия какой-либо операционной системы или приложения, воспринимался не больше чем досадная неприятность. Знание того, что Билл из бухгалтерского отдела все еще пользуется DOS-овской электронной таблицей, которая несовместима с установленной у вас ранней Windows-версией программы Excel, было всего лишь фактом жизни. Вам просто приходилось заново сохранять ваш файл Excel в том формате, который был доступен для Билла, а потом переносить его на дискете в бухгалтерию. Конечно, это было неудобно, но что поделаешь?

Прошли годы, и начали происходить странные вещи. Сетевая технология принялась за персональные компьютеры, а пользователи стали понимать, что могут работать вместе. Наделение персональных компьютеров способностью взаимодействовать друг с другом открыло огромные возможности для сотрудничества и совместной деятельности. Например, одну-единственную версию вашего Excel-файла можно сделать доступной для чтения целой группе авторизованных пользователей, а для изменения — только ограниченному кругу пользователей, что обеспечивает быстрый доступ к самым свежим данным. Сегодня компьютерные сети жизненно необходимы для функционирования всех типов бизнеса и встречаются даже в домашних условиях, объединяя несколько ПК. При грамотной инструментовке и конфигурировании компьютерные сети могут быть весьма быстрыми и надежными в работе.

Однако сети могут выходить из строя, причем таким образом, что утомляют даже самый настойчивый ум. Когда случаются неполадки, необходимо выполнить решительные действия по обнаружению и исправлению возникшей проблемы. И если учитывать, что кроме кабелей, концентраторов, маршрутизаторов, коммутаторов и других сетевых устройств многие компьютерные сети могут включать в себя сотни или даже тысячи ПК, становится понятным, что для *эффективного* устранения неисправностей требуется нечто большее, чем просто замена персональных компьютеров и других сетевых устройств. Для эффективного и экономного устранения неисправностей сейчас больше чем когда-либо требуется знание сетевого оборудования и сетевых операционных систем, а также глубокое понимание симптомов и диагностики неполадок в сетях. Установка, оптимизация и модернизация компьютерных сетей — это еще три важных области, которые требуют внимания современного технического специалиста.

В этом издании

Эта книга предназначена для энтузиастов, интересующихся современными компьютерными сетями, а также для технических специалистов, в задачи которых входит построение и обслуживание компьютерной сети. В книге нет подробного изложения теории компьютерных сетей — уже существует множество других теоретических книг на эту тему. Наоборот, книга создавалась как настольное (или стендовое) руководство по ремонту, обслуживанию и модернизации компьютерных сетей. Содержание данной книги охватывает симптомы и проблемы, возникающие в любой области функционирования современных ПК, а также вопросы их правильной диагностики. Почти в каждой главе приводятся ссылки на онлайновые ресурсы, что делает эту книгу идеальным пособием для изучения как в классе, так и дома. Книга предназначена стать своеобразной "горячей линией" или ресурсом, с помощью которого вы сможете отремонтировать свою сеть в случае неполадок, следить за ее правильной работой и сделать ее функционирование максимально эффективным. Здесь вы найдете сотни подробных описаний проблем с необходимыми объяснениями. Также приводятся ссылки на сотни POST-кодов (Power On Self Test — самотестирование, выполняемое при включении питания) и диагностических кодов, которые помогут вам выявить даже самые непонятные проблемы компьютерной сети.

Подпишитесь на информационный бюллетень "The PC Toolbox"

Многие читатели жалуются, что книги по компьютерной тематике подвержены быстрому устареванию содержания. Очень часто книгу можно считать устаревшей уже в тот момент, когда она появилась на полках книжных магазинов. Чтобы избежать этого, вы можете подписаться на наш информационный бюллетень — "The PC Toolbox". С его помощью вы сможете ознакомиться с самыми последними статьями по практическому обслуживанию компьютерных сетей и методами их оптимизации и найдете в нем ответы на ваши вопросы о компьютерах. Даже если вы не занимаетесь обслуживанием компьютерных сетей профессионально, эта подписка поможет вам сэкономить сотни долларов в ваших покупках. Чтобы узнать подробности об информационном бюллетене "The PC Toolbox" и подписаться на него, зайдите на сайт по адресу: **www.dlspubs.com**.

Я заинтересован в вашем успехе

Мне пришлось потратить много сил и времени, чтобы эта книга, посвященная устранению проблем в компьютерных сетях, стала наиболее полным и понятным изданием из всех существующих сегодня. Если у вас есть какие-нибудь вопросы или комментарии по поводу этой книги, пожалуйста, свяжитесь со мной через компанию Dynamic Learning Systems по адресу: **www.dlspubs.com**.

Стивен Дж. Бигелоу

Краткий перечень симптомов неисправностей

(продолжение)

Симптом	Описание	Глава	Стр.
8.1	Периодически пропадает соединение	8	289
8.2	Отказал целый кабельный сегмент	8	289
8.3	Вы обнаружили необычайно высокое число коллизий	8	289
8.4	Ошибки контрольной суммы кадра возникают часто или периодически	8	289
8.5	После установки новой рабочей станции соединение отсутствует или характеризуется прерывистостью	8	290
8.6	Производительность сети понижена	8	296
8.7	Фиксируется большое количество коллизий или фрагментированных пакетов	8	296
8.8	При установке новой рабочей станции соединение отсутствует или является неустойчивым	8	296
8.9	Рабочая станция полностью выходит из строя	8	297
8.10	Отсутствует соединение в пределах сегмента оптоволоконного кабеля	8	302
8.11	Соединение отсутствует или является нестабильным	8	302
8.12	После установки новой рабочей станции соединение отсутствует	8	302
9.1	В многопроцессорном компьютере один процессор всегда обозначается как "занятый"	9	383
9.2	Светодиод питания не светится	9	383
9.3	Во время запуска система не подает звуковые сигналы	9	384
9.4	Система подает звуковой код ошибки	9	384
9.5	Система выводит сообщение об ошибке POST	9	384
9.6	Вы испытываете затруднения при использовании различных процессоров на серверной материнской плате	9	384
9.7	Данные SPD перезаписаны	9	385
9.8	В журнале системных событий зарегистрированы события сбоя напряжения	9	385
9.9	Область настройки PCI на сервере не обновляется должным образом	9	385
9.10	При нахождении сервера в режиме ожидания происходит отказ включения питания	9	386
9.11	При проверке точности часов реального времени серверные диагностические средства блокируются	9	386
9.12	При наличии переменного тока на сервер не подается питание	9	386

(продолжение)

Симптом	Описание	Глава	Стр.
9.13	Система загружается после установки адаптера PCI	9	387
9.14	Система автоматически загружается после подачи напряжения на шину питания	9	387
9.15	Сервер слишком долго загружается	9	387
9.16	При наличии одного процессора система не загружается	9	388
9.17	Механизм фиксации не подходит к вашему процессору с картриджем	9	388
9.18	При извлечении процессора из механизма фиксации его можно повредить	9	388
9.19	Ваша материнская плата не поддерживает быстрые процессоры Pentium III	9	388
9.20	При установке плат расширения в слоты PCI 5 или 6 серверная материнская плата может быть заблокирована	9	389
9.21	При обновлении микропрограммного обеспечения контроллера BMC происходит сбой в его работе	9	389
9.22	Сервер с резервным энергоснабжением не загружается в сочетании с данной материнской платой	9	389
10.1	Сетевой адаптер конфликтует с установленным на шине PCI адаптером SCSI	10	431
10.2	Сетевой адаптер успешно прошел диагностические тесты, но установить сетевое соединение не удается	10	431
10.3	При загрузке драйверов компьютер зависает	10	431
10.4	Драйвер сетевого адаптера не загружается или не опознает плату NIC	10	431
10.5	При установке драйверов сетевого адаптера процедура Setup сообщает о том, что адаптер "Не разрешен BIOS" ("Not enabled by BIOS")	10	431
10.6	Вы постоянно сталкиваетесь с проблемами при назначении прерывания IRQ 15 сетевому адаптеру	10	432
10.7	Система зависает при загрузке	10	432
10.8	При выполнении автосогласования с помощью диагностической утилиты сетевого адаптера светодиод этой платы не светится	10	432
10.9	Светодиод связи (LNK) сетевого адаптера не светится	10	432
10.10	Светодиод активности (ACT) сетевого адаптера не светится	10	432
10.11	Сетевой адаптер прекратил работать после установки на компьютер другой платы этого типа	10	433

(продолжение)

Симптом	Описание	Глава	Стр.
10.12	В среде Windows 2000 не обнаруживается BNC-соединение	10	433
10.13	Сетевой адаптер сначала работал, а потом прекратил работу без видимых причин	10	433
10.14	Вы сталкиваетесь с неполадками при использовании сетевого адаптера Xircom CE3 в среде Windows 2000	10	434
10.15	Вы получаете сообщение типа "Конфигурация адаптера не была сохранена. Для определения текущих настроек проверьте конфигурацию"	10	434
10.16	Связь между сетевым адаптером и эхо-сервером (echo server) установить не удалось	10	434
10.17	Появляется ошибка, указывающая на сбой адресного программируемого ПЗУ (address PROM)	10	434
10.18	Появляется сообщение о сбое теста прерываний	10	435
10.19	Вы наблюдаете ошибку типа "Сбой при тестировании микросхемы сетевого сопроцессора"	10	435
10.20	Появляется сообщение о сбое при прохождении теста ОЗУ NIC	10	435
10.21	Вы наблюдаете ошибку типа "Сбой теста простой передачи (simple transmit test)"	10	435
10.22	Вы наблюдаете ошибку типа "Невозможно обнаружить эхо-сервер"	10	435
10.23	Вы наблюдаете ошибку типа "Ваша система выполняет кэширование в верхней области памяти (high memory) — вы должны отключить кэширование в базовой области адресов ОЗУ 64 Кбайт"	10	436
10.24	Появляется ошибка вида "Размер ОЗУ слишком велик для базового адреса ОЗУ 0d8000. Определите ОЗУ в размере 16 или 32 Кбайт"	10	436
10.25	Появляется ошибка вида "Для базового адреса ОЗУ F00000 или выше размер ОЗУ должен составлять 64 Кбайт"	10	436
10.26	Появляется ошибка вида "Все каналы DMA не функционируют — нет возможности обнаружить другой канал"	10	436
10.27	Появляется ошибка о сбое тестирования ASIC	10	436
10.28	Появляется ошибка "DMA-канал <x> поврежден — попробуйте использовать DMA-канал <y>"	10	437
10.29	Обнаруживается, что рабочие станции не могут подключиться к серверу NetWare	10	437
10.30	Во время установки драйвера NetWare появляются сообщения об ошибках	10	437

(продолжение)

Симптом	Описание	Глава	Стр.
10.31	Сервер NetWare возвращает ошибку "Обнаружена ошибка конфигурации маршрутизатора"	10	437
10.32	Сервер NetWare создает сообщение: "Буферы приема недостаточны. Установите максимальный размер буфера приема пакетов в файле STARTUP.NCF равным 1536"	10	438
10.33	Сервер NetWare сообщает, что "Загрузчик не может найти общедоступный символ *<имя символа>*"	10	438
10.34	Сервер NetWare сообщает, что "NetWare не поддерживает обращения к BIOS в защищенном режиме. В отсутствие заплаты загрузчика драйверы PCI могут дать сбой"	10	438
11.1	Система зависает во время поиска устройств SCSI RAID	11	504
11.2	После установки RAID-контроллера система не загружается	11	504
11.3	Система не может обеспечить одновременное вращение всех дисков RAID	11	505
11.4	При установке RAID-контроллера появляется сообщение об ошибке типа "Система BIOS не установлена"	11	505
11.5	Возникают сбои при работе с RAID-контроллером IDE	11	505
11.6	В массиве, созданном с помощью утилиты настройки RAID, задействовано слишком много дисков	11	505
11.7	Загрузочное устройство RAID SCSI не найдено	11	506
11.8	Невозможна загрузка с RAID-контроллера типа IDE	11	506
11.9	Один из жестких дисков постоянно инициирует перекомпоновку массива или его работу в неоперативном режиме	11	506
11.10	Не удается обнаружить все диски, подключенные к RAID-контроллеру	11	506
11.11	Обнаруживается, что диски UDMA случайным образом выпадают из массива	11	507
11.12	Диски в массиве слишком часто выходят из строя	11	507
11.13	Видеокарта работает некорректно, несмотря на то, что разделяет ресурсы с RAID-контроллером	11	507
11.14	Сервер не загружается с сопроводительного компакт-диска	11	507
11.15	Емкость дискового массива, о которой сообщает RAID-контроллер, значительно меньше фактической	11	508
11.16	При работе с RAID-контроллером скорость передачи данных оказывается ниже запланированной	11	508
11.17	Сбои появляются, когда система пытается воспользоваться диском "горячего резерва" (hot spare) или "горячей замены" (hot swap)	11	508

(продолжение)

(продолжение)

Симптом	Описание	Глава	Стр.
12.15	Выводится код ошибки 113xxxx	12	546
12.16	Выводится код ошибки 210xxxx	12	546
12.17	Устройство SCSI отказывается взаимодействовать с адаптером SCSI, хотя по отдельности они работают нормально	12	546
12.18	Появляется сообщение об ошибке, в соответствии с которым "контроллер SCSI отсутствует"	12	546
12.19	Хост-адаптер SCSI на шине PCI не обнаруживается, а заголовок SCSI BIOS не отображается	12	547
12.20	Во время загрузки появляется сообщение об "ошибке конфигурации хост-адаптера"	12	547
12.21	Появляется сообщение об ошибке типа "функции SCSI не используются"	12	547
12.22	Появляется сообщение об ошибке типа "загрузочная запись не обнаружена"	12	547
12.23	Появляется сообщение об ошибке типа "устройство не отвечает — загрузка драйвера прервана"	12	548
12.24	Появляется сообщение об ошибке типа "неизвестное устройство SCSI" или "ожидание устройства SCSI"	12	548
12.25	Появляется сообщение об ошибке типа "ошибка CMD XX"	12	548
12.26	После появления заголовка системы BIOS адаптера SCSI выводится сообщение типа "идет поиск целевого устройства SCSI с LUN 0"	12	548
12.27	При появлении заголовка SCSI BIOS система зависает	12	549
12.28	Во время запуска системы выводится заголовок SCSI BIOS, но после этого появляется сообщение об "ошибке диагностики хост-адаптера"	12	549
12.29	В среде Windows 9x/ME программа Adaptec EasySCSI вызывает ошибку из-за недействительности страницы	12	549
12.30	Вы сталкиваетесь с трудностями при работе с контроллером SCSI BusLogic на шине PCI	12	549
12.31	Вы сталкиваетесь с трудностями при работе с контроллером SCSI Adaptec и приводом CD-RW	12	550
12.32	После обновления Windows 98 не может обнаружить привод CD-ROM SCSI	12	550
13.1	Соединение между коммутируемыми сегментами отсутствует	13	571
13.2	Наличие постоянных широковещательных штормов	13	571
13.3	Низкая пропускная способность коммутатора	13	571

(продолжение)

Симптом	Описание	Глава	Стр.
13.4	Невозможно установить связь с коммутатором с помощью Telnet, SNMP или Web-браузера	13	571
13.5	Невозможно получить доступ к коммутатору через его последовательный порт	13	572
14.1	Не удается получить доступ к кабельному/DSL-маршрутизатору	14	598
14.2	Диагностические светодиоды маршрутизатора не отражают корректную последовательность загрузки	14	598
14.3	Светодиод связи или активности маршрутизатора не работает	14	598
14.4	Ваш широкополосный маршрутизатор прекращает работу	14	598
14.5	Не удается установить связь с другими компьютерами через маршрутизатор	14	598
14.6	Не удается перемещаться по сети Интернет с помощью маршрутизатора	14	599
14.7	Ваша Web-страница зависает, а загруженные данные оказываются поврежденными	14	599
14.8	Не удается получить IP-адрес с использованием кабельного модема или DSL-маршрутизатора	14	599
14.9	Почтовая программа не получает электронную почту через маршрутизатор	14	599
14.10	Маршрутизатор отказывается работать с NetMeeting	14	599
14.11	Маршрутизатор отказывается подключаться к вашему поставщику интернет-услуг	14	600
14.12	Невозможно получить доступ к маршрутизатору через Web-страницу	14	600
15.1	Рабочая станция в локальной сети не может подключиться к сети Интернет	15	622
15.2	Сервер DMZ недоступен из сети Интернет	15	623
15.3	Сбои при отправке электронной почты из локальной сети на почтовый сервер поставщика интернет-услуг	15	623
15.4	Журнал регистрации брандмауэра сообщает о "переполнении диска"	15	623
15.5	Пароль администратора изменен или потерян	15	623
15.6	Выясняется, что соединения "auth" блокируются	15	623
15.7	Одна из подсетей не может подключиться к сети Интернет через брандмауэр	15	624

(продолжение)

Симптом	Описание	Глава	Стр.
16.1	Светодиоды сервера печати не сигнализируют	16	653
16.2	Светодиод состояния сервера печати сигнализирует беспрерывно	16	653
16.3	Светодиоды состояния и питания сервера печати сигнализируют беспрерывно	16	653
16.4	При использовании DHCP появляется конфликт IP-адресов с участием сервера печати	16	653
16.5	Возникают трудности при попытке применения WPCONFIG для настройки сервера печати в среде Windows 9x	16	653
16.6	Светодиод на трехпортовом сервере печати не сигнализирует	16	654
16.7	При использовании кабеля 10BaseT сервер печати не работает	16	654
16.8	Принтер, подключенный к серверу печати, не может печатать (или печатает с дефектами)	16	654
16.9	Не удается внести изменения в конфигурацию сервера печати	16	654
16.10	В среде NetWare сервер печати печатает с дефектами	16	654
16.11	В списке активных устройств (Active Device List) программы NetWare PSCONFIG сервер печати отсутствует	16	656
16.12	Сервер печати настроен на работу с NetWare, но не может зарегистрироваться на файловом сервере	16	656
16.13	Сервер печати настроен как удаленный принтер NetWare, но он не может зарегистрироваться на сервере печати NetWare	16	657
16.14	Сервер печати не выполняет задания, которые направляются в очередь печати NetWare	16	658
16.15	Для выполнения задания на печать использовалась команда *capture* NetWare, но задание было разделено на две части	16	658
16.16	Утилита PSCONFIG или программа администрирования выводит сообщение "нет ответа"	16	658
16.17	При проверке регистрации сервера печати на файловом сервере команда *quickset* блокируется по превышению лимита времени	16	659
16.18	В среде NetWare 4.x сообщения с уведомлениями не поступают	16	659
16.19	Установить состояние принтера не удается, или он определяется как "нефункционирующий"	16	659
16.20	Настройки "String Before Job" и/или "String After Job" в разделе логических принтеров (Logical Printers) работают некорректно	16	659
16.21	Появляются трудности при обслуживании дополнительных файловых серверов NetWare Bindery	16	659

(продолжение)

Симптом	Описание	Глава	Стр.
16.22	Появляются трудности при подключении к нескольким серверам печати NetWare	16	660
16.23	Документы приложений Windows распечатываются некорректно	16	660
16.24	При подключении нового принтера в среде Windows 9x появляется сообщение о том, что принтер не найден	16	660
16.25	Вы подключили и настроили принтер WPS (система печати Windows), но выполнить на нем задание печати не удается	16	661
16.26	В среде Windows текст распечатывается хорошо, а графика — с дефектами	16	661
16.27	Появляется сообщение об ошибке соединения SPX	16	662
16.28	Некоторые DOS-программы не работают в одноранговой среде Windows 9x	16	662
17.1	После отключения поддержки ACPI появляется сообщение об ошибке	17	672
17.2	Система не может перейти в спящий режим	17	673
17.3	Невозможно отключить монитор средствами Power Options	17	673
17.4	Компьютер игнорирует настройки таймера ожидания в Windows 2000	17	674
17.5	Хранители экрана OpenGL препятствуют переходу системы в ждущий режим	17	674
17.6	Не удается отключить управление прерываниями на компьютере с ACPI	17	674
17.7	В среде Windows 2000 происходит сброс установок даты и времени при каждой загрузке	17	675
17.8	В Windows 2000 появляется ошибка STOP 0x9F	17	675
17.9	Появляются сбои при сохранении данных в системе Windows 2000, работающей от аккумулятора	17	676
17.10	В стандартном режиме VGA функции управления питанием недоступны	17	676
17.11	При использовании SYSPREP система зависает	17	677
17.12	Компьютер зависает при работе в режиме ACPI	17	677
17.13	Windows 2000 использует IRQ6 даже при отсутствии контроллеров гибких дисков	17	677
17.14	Не удается обнаружить немаскируемое прерывание в многопроцессорной системе с поддержкой ACPI	17	678
17.15	В системе Windows 2000 с поддержкой ACPI появляется ошибка STOP 0xA	17	678

(продолжение)

Симптом	Описание	Глава	Стр.
17.16	Происходит полный отказ системы с набором микросхем OSB4	17	679
17.17	ИБП не включается	17	697
17.18	ИБП не отключается	17	698
17.19	ИБП использует аккумулятор при наличии нормального напряжения переменного тока	17	698
17.20	ИБП не обеспечивает ожидаемого времени резервного питания	17	698
17.21	Все индикаторы ИБП светятся, а само устройство постоянно подает звуковые сигналы	17	698
17.22	Панельные индикаторы ИБП сигнализируют один за другим	17	699
17.23	ИБП подключен к штатному источнику питания, но ни один индикатор не работает	17	699
17.24	Горит светодиод замены батареи (Replace Battery)	17	699
17.25	ИБП указывает на ошибку местной электропроводки	17	699
17.26	На ИБП начинает сигнализировать предупредительный светодиод высокого напряжения	17	699
17.27	На ИБП начинает сигнализировать предупредительный светодиод пониженного напряжения	17	699
17.28	ИБП часто переключается со штатного питания на аккумуляторное	17	700
17.29	На ИБП начинает сигнализировать предупредительный светодиод нагрузки	17	700
17.30	Вкладка *UPS* диалогового окна *Power Options* недоступна	17	700
17.31	Во время установки Windows 2000 ИБП входит в аккумуляторный режим	17	701
17.32	Во время установки Windows 2000 ИБП входит в режим аттестации аккумулятора	17	701
17.33	ИБП с "простым сигнализированием" не отключается после отключения системы	17	702
17.34	ИБП не может обратиться к своему COM-порту	17	702
17.35	Отключение Windows происходит сразу после сбоя энергоснабжения	17	702
17.36	Неисправность связана с последовательным подключением ИБП	17	703
18.1	Невозможно администрирование устройства NAS	18	721
18.2	Устройство NAS не удается обнаружить в сети	18	722
18.3	Программа администрирования выводится на экран некорректно	18	723

(продолжение)

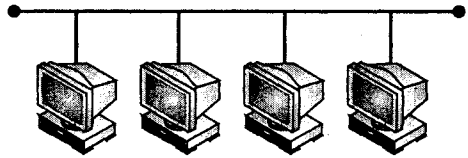
Симптом	Описание	Глава	Стр.
18.4	Пароль администратора утерян	18	723
18.5	Появляется сообщение об ошибке, в соответствии с которым "дисковое зеркало" находится в вырожденном состоянии	18	723
18.6	Появляется сообщение об ошибке, в соответствии с которым дублированный диск неисправен	18	723
18.7	Появляется сообщение об ошибке, в соответствии с которым том диска заполнен	18	724
18.8	Появляется сообщение об ошибке, в соответствии с которым фиксируется большое количество ошибок дисков	18	724
18.9	Появляется сообщение об ошибке, в соответствии с которым на диске осталось мало места	18	724
18.10	Появляется сообщение об ошибке, в соответствии с которым пользователь с указанным IP-адресом осуществил 5 неудачных попыток введения пароля	18	724
18.11	Предупреждения от NAS не приходят на ваш почтовый ящик	18	725
18.12	Пользователь просматривает содержимое NAS, но ему не удается сохранить файлы в определенном каталоге	18	725
18.13	Не удается обновить операционную систему NAS	18	725
18.14	Не удается подключиться к серверу компакт-дисков с целью его администрирования	18	739
18.15	При обзоре сети с вашей рабочей станции не удается обнаружить сервер компакт-дисков	18	740
18.16	Не удается изменить имя дисковода сервера компакт-дисков в Windows 2000	18	740
18.17	Появляется сообщение об ошибке, в соответствии с которым на диске недостаточно места	18	740
18.18	Предупреждения от сервера компакт-дисков не приходят на ваш почтовый ящик	18	741
19.1	Невозможно одновременно запустить несколько антивирусных программ	19	777
19.2	Ваше антивирусное средство не работает или приводит к некорректной работе других драйверов	19	777
19.3	Вы замечаете, что антивирусная программа значительно замедляет операции обращения к диску или при работе в Windows блокируется	19	777
19.4	Антивирусная программа выдает ложные аварийные сигналы	19	777
19.5	Вам не удается удалить резидентную антивирусную программу	19	778

(продолжение)

Симптом	Описание	Глава	Стр.
19.6	Механизм поиска вирусов выполняет операции поиска очень медленно	19	778
19.7	Во время проведения операций поиска механизм поиска вирусов конфликтует с загрузочным сектором	19	778
19.8	При установке антивирусной программы на сервер NetWare 4.x вы сталкиваетесь с ошибками NDS	19	778
19.9	Вы сталкиваетесь с ошибкой "свертывание постороннего процесса"	19	779
19.10	Вы сталкиваетесь с ошибкой невозможности загрузить <имя_файла>	19	779
19.11	После установки антивирусной программы вы сталкиваетесь с трудностями при запуске системы	19	779
19.12	После установки антивирусной программы вы сталкиваетесь с трудностями при отключении системы	19	780
19.13	После обновления 16-битовый клиент дважды упоминается в управляющем программном обеспечении	19	781
19.14	Вы сталкиваетесь с трудностями при загрузке антивирусного программного обеспечения для NetWare	19	781
20.1	Накопитель на магнитной ленте не работает	20	811
20.2	Операции считывания и записи на кассету не производятся, но лента и головка движутся	20	812
20.3	Накопитель на магнитной ленте осуществляет запись на кассету с защитой от записи	20	812
20.4	Программа резервирования указывает на "слишком большое количество дефектных секторов" на кассете	20	813
20.5	Программа резервирования на магнитных лентах генерирует ошибку XX накопителя на магнитной ленте	20	813
20.6	Накопитель на магнитной ленте работает в DOS, но отказывается работать в Windows 9x и более поздних версиях	20	813
20.7	Программа резервирования генерирует ошибку оверлея типа "не удалось открыть файл: QBACKUP.OVL"	20	813
20.8	Вы сталкиваетесь с ошибками носителей, ошибками дефектных участков, системными ошибками или блокировками	20	814
20.9	Во время инициализации в среде DOS или Windows драйвер накопителя на магнитной ленте SCSI (например, BPASPI.SYS) сообщает об ошибке, в соответствии с которой "устройство ASPI не найдено"	20	814

(окончание)

Симптом	Описание	Глава	Стр.
20.10	При использовании накопителя на магнитной ленте Colorado Trakker вам не удается заставить его надежно сохранять или восстанавливать файлы	20	814
20.11	На проведение операции резервирования уходит намного больше времени, чем вы ожидали	20	815
20.12	Во время выполнения операций резервирования фиксируются избыточные движения ленты	20	816
26.1	У меня неприятности с политиками паролей	26	1021
26.2	Пользователь забыл свой пароль	26	1023
26.3	Снятие блокировки с пользовательской учетной записи	26	1023
26.4	Предоставьте управление пользователю	26	1023
26.5	Пользователю не удается зарегистрироваться в домене из-за различий во времени	26	1024
26.6	Домен не идентифицирует клиентский компьютер после его переименования	26	1024
26.7	Пользователю не удается зарегистрироваться или воспользоваться командой *rlogin* в другом домене	26	1026
26.8	Новый пароль пользователя не функционирует	26	1027
26.9	Пользователю не удается зарегистрироваться в удаленном домене	26	1027
26.10	Пользователю не удается изменить свой пароль	26	1027
26.11	У пользователя нет необходимых полномочий	26	1028
26.12	У пользователя нет подходящего сертификата	26	1028
26.13	Имя пользователя идентично имени компьютера	26	1028
26.14	У меня неприятности со сценариями регистрации	26	1038
26.15	В смешанной среде появились проблемы	26	1038
26.16	Трудности с командой *Net Use*	26	1038



ГЛАВА 1

Введение в организацию сетей

Хотя автономные компьютеры и могут быть довольно мощными, они все же работают независимо друг от друга. При этом для совместного использования файлов и ресурсов обычно нужно скопировать файл на дискету (или CD-RW-диск) и затем физически переносить эту дискету на другие системы, — например, вы можете после работы внести какие-то изменения в свой документ, а на следующий день вернуть этот обновленный документ на работу, чтобы распечатать его. Очевидно, что такой порядок неудобен и отнимает много времени. Если бы было возможно "связать" между собой два или более компьютеров, вы смогли бы получить доступ к своей работе из другого места (например, с вашего домашнего компьютера), закончить свою работу за этот вечер и потом отправить ее назад на принтер, расположенный в вашем офисе. В этом состоит суть идеи построения *компьютерных сетей* — два или более компьютеров соединяются друг с другом для того, чтобы получить возможность одновременного доступа к файлам, ресурсам или даже приложениям. В этой главе вы сможете познакомиться с основными понятиями и терминами, необходимыми для понимания наиболее важных элементов обычных компьютерных сетей и серверов, с описанием основ сетевой документации, а также с основными правилами поиска и устранения неполадок в компьютерных сетях.

Начальные сведения о компьютерных сетях

Сетевой компьютер, выполняющий функцию предоставления ресурсов, называется *сервером* (server). Компьютер, использующий эти ресурсы, называется *рабочей станцией* (workstation) или *клиентом* (client). В качестве серверов обычно используются самые мощные компьютеры, соединенные с сетью, поскольку им требуются дополнительные обрабатывающие мощности для обслуживания множества поступающих от других компьютеров запросов на доступ к общим ресурсам. По сравнению с серверами рабочие станции или клиенты — это обычно менее дорогие и менее мощные персональные компьютеры (ПК). Как правило, компьютер выполняет роль *либо* сервера, *либо* рабочей станции, но редко может совмещать обе эти функции. Такое разделение значительно упрощает обслуживание и администрирование компьютерной сети. Малые компьютерные сети, включающие относительно небольшое количество пользователей, могут иметь *одноранговую* (peer-to-peer) архитектуру, в которой каждый ПК может иметь доступ к общим ресурсам, однако в этой книге мы будем го-

ворить в основном о компьютерных сетях с архитектурой "клиент-сервер". Конечно, все компьютеры, входящие в состав сети, должны иметь с ней физическое соединение. Такие соединения обычно устанавливаются при помощи сетевой интерфейсной платы (Network Interface Card, NIC) и медных кабелей (либо других средств соединения, таких, как оптоволоконная или беспроводная связь).

Преимущества компьютерных сетей

Если компьютеры работают независимо друг от друга, то приложения и ресурсы (например, принтеры или сканеры) придется дублировать для каждого из них. Например, если два аналитика хотят работать с таблицей Excel и ежедневно распечатывать результаты своей работы на принтере, оба используемых ими компьютера должны иметь свою копию программы Excel и принтер. Если бы пользователям понадобилось совместно применять свои данные, то эти данные пришлось бы непрерывно переносить между компьютерами при помощи дискет или CD-RW-дисков. А если бы пользователям понадобилось совместно применять свои компьютеры, то каждому из них пришлось бы приложить усилия, чтобы разобраться в другой системе — ведь в каждой из них имеется своя организация рабочего стола и приложений, своя структура папок и т. д. Короче говоря, это был бы весьма неудобный, неэкономный процесс, который приводил бы к большому количеству ошибок. И чем больше пользователей подключается к этому процессу, тем быстрее наступает момент, когда им становится уже невозможно управлять. Однако, если бы те два ПК из нашего примера были соединены между собой в сеть, оба пользователя смогли бы применять одно приложение Excel, иметь доступ к одним и тем же исходным данным и потом отправлять результаты своей работы на один "общий" принтер, присоединенный к сети (хотя, нужно сказать, что в современных сетях чаще всего каждая рабочая станция имеет свои приложения, например, Excel, а данные использует совместно). Если бы к этой сети добавилось больше пользователей, то все они смогли бы совместно применять Excel, данные и ресурсы одинаковым образом. Другими словами, компьютеры, входящие в сеть, могут совместно использовать:

- документы (записки, электронные таблицы, счета и т. д.);
- электронные почтовые сообщения;
- программное обеспечение по работе с текстом;
- программное обеспечение по сопровождению проектов;
- иллюстрации, фотографии, видео- и аудиофайлы;
- живые аудио- и видеотрансляции;
- принтеры;
- факсы;
- модемы;
- дисководы CD-ROM и другие сменные запоминающие устройства (как, например, Zip-дисководы и Jaz-дисководы);
- жесткие диски.

Поскольку в одной компьютерной сети работает множество компьютеров, более эффективно управлять всей сетью из центральной точки (*сетевой администратор*,

network administrator). Возьмем вышеприведенный пример и предположим, что нашим аналитикам дали новую версию программы Excel. Если их компьютеры не объединены в сеть, то каждую систему придется модернизировать и проверять по отдельности. Это не так уж и сложно сделать, если систем только две. Но если в компании есть десятки или даже сотни персональных компьютеров, проводить индивидуальную модернизацию каждого из них, естественно, становится дорогим и неэффективным занятием. При наличии компьютерной сети, для того чтобы модернизировать приложение, такую модернизацию достаточно выполнить только один раз на сервере, после чего все рабочие станции данной компьютерной сети смогут сразу же начать использовать обновленное программное обеспечение (ПО). Централизованное администрирование также позволяет из одного места управлять безопасностью компьютерной сети и следить за ее работой.

Но кроме возможности совместного доступа к информации, компьютерные сети дают и другие преимущества. Сеть позволяет сохранять и защищать информацию. Например, очень трудно координировать и управлять процессом резервирования информации при большом количестве независимых друг от друга персональных компьютеров. Системы, организованные в компьютерную сеть, могут автоматически создавать резервные копии файлов в одном центральном месте (например, накопителе на магнитной ленте, подключенном к сетевому серверу). Если информация на каком-либо компьютере оказывается утраченной, ее можно будет легко найти в центральной системе резервирования и восстановить. Кроме того, повышается уровень безопасности данных. Получение доступа к отдельному персональному компьютеру, как правило, означает доступ ко всей информации, содержащейся в этом компьютере. Однако возможности безопасности, которые предоставляет компьютерная сеть, не позволят неавторизованным пользователям получить доступ к важной информации или удалить ее. Например, каждый сетевой пользователь имеет свое регистрационное ("логинное") имя и пароль, которые дают доступ только лишь к ограниченному числу сетевых ресурсов. Наконец, компьютерные сети являются идеальными средами для общения между пользователями. Вместо того чтобы обмениваться бумажными напоминаниями и записками, электронная почта позволяет пользователям отправлять друг другу письма, отчеты, изображения — почти все типы файлов. Это также позволяет сэкономить на распечатывании материалов и уменьшить задержки, связанные с доставкой переписки между отделами компании. Электронная почта — это такой мощный инструмент, что он позволяет пользователям сети Интернет почти мгновенно обмениваться сообщениями, практически независимо от своего местоположения в мире.

Размеры компьютерных сетей

Компьютерные сети обычно можно отнести к одной из трех групп, в зависимости от их размера и функций. *Локальная сеть* (ЛС, Local Area Network, LAN) — это основной класс компьютерных сетей. Архитектура ЛС может варьироваться между простой (два компьютера, соединенных кабелем) и сложной (сотни компьютеров и периферийных устройств, объединенных в сеть в какой-либо крупной организации). Отличительной особенностью ЛС является то, что она существует в ограниченной географической области, такой как здание или отдел компании (как правило, не превышает 5 км в диаметре). Если компьютеры, объединенные в сеть, размещаются в нескольких зданиях на большой городской территории, то такая сеть иногда назы-

вается *региональной* или *городской сетью* (Metropolitan Area Network, MAN, обычно располагается в диаметре 5—50 км). В отличие от этих классов сетей, *глобальная сеть* (Wide Area Network, WAN) не имеет географических границ и может соединять между собой компьютеры и периферийные устройства, находящиеся на разных сторонах света. В большинстве случаев глобальная сеть состоит из нескольких взаимосвязанных ЛС. Вероятно, Интернет можно считать конечной глобальной сетью.

Когда компьютерная сеть необходима

Глядя на сегодняшнее весьма оживленное состояние бизнеса, кажется, что чуть ли не каждый торговец предлагает какое-то сетевое решение для повышения продаж, улучшения продуктивности и даже увеличения доходов. Во многих случаях компании просто уговаривают сделать вложения в построение компьютерной сети, без тщательного изучения затрат и предлагаемого качества. Если вы менеджер информационной службы или ответственный руководитель, то вас может интересовать, насколько будут оправданы материальные и технические затраты, связанные с созданием компьютерной сети. Описания следующих проблем помогут вам определить, сможет ли построение компьютерной сети принести вашей компании пользу.

- *Ваша компания или отдел тратит деньги на приобретение дополнительного аппаратного и программного обеспечения.* Компьютерные сети позволяют достичь чрезвычайно высокого уровня совместного использования информации и ресурсов, поэтому покупка дополнительного оборудования в виде принтеров, накопителей и программного обеспечения может оказаться (в конечном итоге) даже более затратной, чем построение сети для совместного использования этих ресурсов. Например, покупка или модернизация десяти новых принтеров может стоить больше, чем установка одного сетевого принтера. Преимущество этого решения не только в том, что установка и обслуживание одного сетевого принтера проходит проще и быстрее, но и в том, что таким принтером смогут пользоваться *множество* сетевых пользователей.
- *Из-за несоответствий программного обеспечения возникают ошибки и потери продуктивности.* Это часто случается, когда разные пользователи используют разные версии программного обеспечения. Файлы, созданные в старой версии приложения, могут быть прочитаны в его более поздних версиях, но не наоборот. Например, документ, созданный в программе Word 6, можно легко открыть в Word 2000, но не наоборот — и уж тем более не в Word для DOS. Все это ограничивает круг пользователей, которые могут использовать каждый документ. Это также может происходить в тех случаях, когда разные пользователи применяют приложения, созданные разными производителями (как, например, Word и WordPerfect). В системе объединенных в сеть ПК сотрудники могут использовать одну и ту же версию приложения, что обеспечивает совместимость файлов. Кроме того, специалисту, который занимается компьютерной сетью, достаточно будет только один раз обновить сетевое приложение, чтобы им могли пользоваться все, вместо того, чтобы множество раз обновлять его на каждом отдельном компьютере.
- *Расходы на обучение и поддержку слишком высоки.* Затраты на обучение постоянно растут, и даже те производители, которые раньше делали это бесплатно, теперь назначают плату за обучение и поддержку. Если же используется множество раз-

ных версий аппаратного и программного обеспечения, расходы вообще становятся непомерно высокими. Применение в компьютерной сети "стандартизированных" версий программного обеспечения позволяет сократить число используемых в организации приложений, а это, в свою очередь, позволит сократить диапазон услуг по поддержке, которые нужны вашим пользователям. Если для применения какого-либо приложения требуется пройти обучение, то такое обучение сможет пройти большее число пользователей (что также сократит расходы в расчете на каждого пользователя).

- *Производительность снижается из-за простоев в ожидании ресурсов.* Производительность может в значительной мере падать, если пользователи вынуждены ждать, пока они смогут получить доступ к тому или иному ресурсу. Например, один пользователь должен завершить текущий сеанс работы на компьютере, чтобы другой работник смог загрузить в него свои данные и распечатать какой-нибудь документ или отчет. Другой пример: сотрудники из отдела по работе с клиентами не могут со своего персонального компьютера получить доступ к истории обслуживания того или иного клиента, информации о счетах, тенденциях в заказах и другой информации, расположенной в других системах внутри данной организации. Поэтому клиентам приходится ждать, пока выполняется запрос в другие отделы. В компьютерной сети любой отдел компании может получить всю информацию о клиенте. Если же предусмотрена возможность обращения через Интернет, клиенты могут еще более продуктивно обращаться за нужной им информацией, делать заказы и получать помощь.

Конечно, есть и много других признаков, по которым можно понять, что необходимо использовать компьютерную сеть. Например, данные теряются из-за того, что некоторые пользователи не делают регулярно резервных копий файлов (если вообще делают). Потери времени и производительности из-за ручного переноса файлов (также известного под названием "сеть транспортировки информации на своих двоих", "sneaker-net") при помощи дискет или компакт-дисков также можно уменьшить, используя компьютерную сеть. Компьютерные сети могут заменить записки в блокнотах или кипы бумаг, а также делать такие сообщения, которые невозможно проигнорировать или не заметить. Компьютерная сеть может использоваться как сама по себе внутри компании, так и быть соединенной с другими компьютерными сетями (или даже с Интернетом), обеспечивая обмен данными и взаимодействие в глобальном масштабе.

Типы компьютерных сетей

Компьютерные сети обычно делят на две категории: *одноранговые сети* (peer-to-peer network) и *сети на основе сервера* (server-based network). Указанное различие между компьютерными сетями довольно важно, поскольку эти две категории существенно отличаются друг от друга и дают разные возможности своим пользователям. Одноранговые сети являются более простыми и менее дорогими и встречаются в небольших организациях — например, при создании небольших офисов или домашних офисов (Small Office/Home Office, SOHO), или небольших рабочих групп. Сети на основе сервера можно встретить в средних или крупных организациях, в которых важны безопасность, централизация администрирования и высокий уровень трафика. Рассмотрим немного подробнее эти типы компьютерных сетей.

Одноранговые сети

Этот подход к построению компьютерных сетей является довольно простым. Компьютеры просто соединяются между собой для получения основных возможностей обмена данными. Здесь нет специальной серверной машины и нет иерархии между компьютерами. Так как все компьютеры являются равноправными, их называют *одноранговыми* (peer). Каждый компьютер выступает в качестве как клиента, так и сервера, и здесь нет администратора, отвечающего за всю сеть в целом, — пользователь каждого компьютера сам определяет, какие данные на его ПК могут быть предоставлены для совместного доступа. Все остальные могут пользоваться любыми совместными ресурсами любым желаемым образом. В числе этих ресурсов могут быть совместно используемые каталоги, принтеры, факс-модемы и т. д. Одноранговые сети также еще называют *рабочими группами* (workgroup, небольшая группа людей), т. к. одноранговые сети, как правило, состоят не больше чем из десятка компьютеров. Подобная простота зачастую делает одноранговые сети менее дорогостоящими, чем серверные.

Программное обеспечение сетевого обмена в одноранговой сети не требует того же стандарта производительности и безопасности, какой требует сетевое программное обеспечение для системы с выделенным сервером (dedicated server system). На самом деле возможность создания одноранговой сети предусмотрена во многих популярных операционных системах (Windows 98/ME, MacOS и UNIX/Linux). Это означает, что построить одноранговую сеть можно без применения какой-либо дополнительной сетевой операционной системы.

Очевидным слабым местом одноранговых сетей является их безопасность. В целом, *безопасность* (т. е. защита компьютеров и хранящихся в них данных от ущерба или несанкционированного доступа) одноранговой сети обеспечивается установкой пароля на какой-либо совместно используемый ресурс (например, каталог). Все пользователи одноранговой сети сами регулируют уровень своей безопасности, и ресурсы общего применения могут находиться на любом компьютере, поэтому в такой сети очень сложно осуществлять централизованный контроль. Это оказывает огромное влияние на уровень безопасности сети, т. к. некоторые пользователи могут вообще не выполнять никаких правил безопасности. Таким образом, одноранговая сеть лучше всего подходит в следующих случаях:

- когда число пользователей невелико. Разработчики обычно устанавливают этот предел в десять пользователей, хотя, конечно, их может быть и больше;
- когда пользователи совместно используют ресурсы (например, файлы и принтеры), но для этого не применяются специальные серверы;
- когда вопросы безопасности не считаются главными;
- когда предполагается, что организация (а значит, и компьютерная сеть) будет расти только в ограниченных пределах.

Примечание

Поскольку каждый компьютер в одноранговой сети может выступать в роли как сервера, так и клиента, пользователям, как правило, необходимо получить дополнительное обучение для того, чтобы они могли действовать как в качестве пользователей, так и в качестве администраторов своих компьютеров.

Сети на основе сервера

В большинстве случаев возможности одноранговых сетей с двойственностью функций ПК являются просто-напросто не достаточными. Проблему ограниченного трафика и возможностей сетевой безопасности и управления часто можно решить при помощи выделенного сервера (такого, например, как Gateway 7400, который изображен на рис. 1.1). *Выделенный сервер* (dedicated server) — это компьютер, который работает только в качестве сервера, предоставляя файлы и управляя ресурсами, и *не* используется в качестве клиента или рабочей станции. Серверы предназначены специально для того, чтобы быстро обрабатывать запросы, поступающие от множества сетевых клиентов, и обеспечивать безопасность файлов и каталогов. Поэтому серверные компьютерные сети стали стандартной архитектурой для современных коммерческих компьютерных сетей. Серверные компьютерные сети еще называют сетями с архитектурой *"клиент-сервер"* (которую иногда обозначают как *двухзвенная* архитектура, two-tier architecture). Следует иметь в виду, что категория сетевой архитектуры ("клиент-сервер" или одноранговая) определяется именно операционной системой и другим программным обеспечением сети — аппаратное обеспечение и физическая конфигурация соединений между компьютерами и в том и в другом виде компьютерных сетей являются идентичными.

Примечание

Серверы обеспечивают особые ресурсы и функции для компьютерной сети. В сети данного типа их может быть несколько (или даже много).

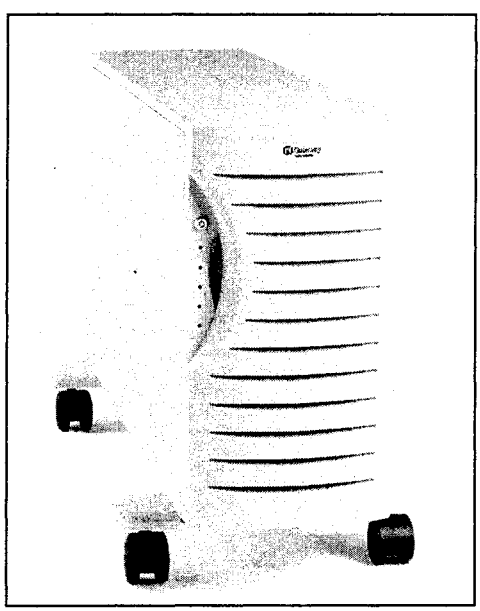


Рис. 1.1. Gateway 7400 – универсальный сервер уровня отдела компании или рабочей группы

Типы серверов

По мере увеличения размеров компьютерной сети (т. е. по мере того, как число взаимосвязанных компьютеров растет, а физическое расстояние и трафик между ними увеличивается), обычно возникает необходимость в увеличении количества серверов. Распределение сетевых задач между несколькими серверами обеспечивает максимальную эффективность выполнения каждой задачи. Серверы должны выполнять разнообразные и сложные задачи, а в больших компьютерных сетях серверы стали специализировать, чтобы удовлетворять расширяющиеся потребности пользователей. Ниже приводятся некоторые примеры различных типов серверов, используемых во многих больших компьютерных сетях.

Серверы доступа к файлам и принтерам

Этот тип серверов служит для управления всем доступом к файлам и принтерам. Например, когда вы используете текстовый процессор (допустим, Microsoft Word), это приложение работает на вашей рабочей станции. Документ, хранящийся на сервере доступа к файлам и принтерам, загружается в память вашей рабочей станции, и далее вы можете редактировать и использовать его. Другими словами, серверы доступа к файлам и принтерам используются для хранения файлов и данных. Если вы хотите распечатать документ, сервер доступа к файлам и принтерам осуществляет передачу этого файла на сетевой принтер.

Серверы базы данных

В большинстве случаев, сервер базы данных представляет собой сервер, на котором установлена система управления базой данных (СУБД, Database management system, DBMS) на основе языка SQL (Structured Query Language — язык структурированных запросов). Клиентский компьютер посылает свой SQL-запрос на сервер базы данных, который, в свою очередь, обращается в имеющуюся базу данных для обработки этого запроса, а затем возвращает результаты обработки на клиентский компьютер. В обозначении "сервер базы данных" термин "сервер" может относиться как к самому компьютеру, используемому в качестве этого сервера, так и к программному обеспечению СУБД, как, например, пакет Microsoft SQL Server.

Серверы приложений

Если серверы доступа к файлам и принтерам пересылают какой-то файл на ту клиентскую машину, которая сделала этот запрос, то серверы приложений отправляют только результаты обработки запроса. Например, вам нужно найти в базе данных по персоналу всех работников, у кого день рождения в ноябре. Вместо пересылки на ваш компьютер всей базы данных для того, чтобы вы могли выполнить поиск, этот поиск проводится на самом сервере приложений, а потом на ваш компьютер отправляется только результат сделанного вами запроса. Это небольшое, но значительное различие делает серверы приложений (такие, например, как Lotus Domino) идеальными инструментами для обслуживания огромных объемов данных и для предоставления этих данных клиентам.

Почтовые серверы

Электронная почта является важной частью современных коммуникаций. Почтовые серверы (такие, например, как Microsoft Exchange Server и Sendmail) управляют по-

током электронных сообщений, пересылаемых между пользователями компьютерных сетей. В большинстве случаев почтовые серверы похожи на серверы приложений, т. к. электронное письмо, как правило, сохраняется на сервере. Когда вы проверяете свою электронную почту, вы видите только те сообщения, которые относятся к вашему регистрационному имени. Сохранение электронных сообщений некоторым централизованным образом, как, например, на почтовом сервере, позволяет повысить безопасность и улучшить управление электронной корреспонденцией (например, старые электронные письма могут удаляться по прошествии некоторого количества дней во всей почтовой системе).

Разновидностью почтового сервера является *сервер почтовой рассылки*, который используется для создания, управления и обслуживания адресных списков рассылки. Серверы почтовой рассылки (например, Majordomo) обычно обладают большими возможностями и имеют более высокую производительность, чем почтовые серверы. Серверы почтовой рассылки могут использоваться для распространения электронных журналов, информационных бюллетеней, обновлений продуктов, документов технической поддержки, расписаний учебных занятий, рекламных проспектов, а также дискуссионных форумов для клубов и групп, электронных напоминаний и т. д.

Факс-серверы и коммуникационные серверы

Компьютерные сети редко существуют в вакууме, и, как правило, существует несколько путей доступа в компьютерную сеть извне. Факсы и коммутируемые телефонные соединения (dial-up) являются двумя распространенными способами внешнего соединения с компьютерной сетью. Факс-сервер (например, FaxMaker) управляет исходящим и входящим факсимильным трафиком при помощи одной или нескольких факс-модемных карт, позволяя пользователям компьютерной сети отправлять и получать факсимильные сообщения без использования собственных факсимильных устройств. Коммуникационные серверы (communication servers) управляют передачей массивов данных и электронных сообщений между вашей компьютерной сетью и другими компьютерными сетями, большими ЭВМ или удаленными пользователями, которые устанавливают соединение с этими серверами посредством модема и телефонной линии. Например, при помощи коммуникационного сервера пользователь компьютерной сети может получать доступ в Интернет.

Аудио- и видеосерверы

Аудио- и видеосерверы создают мультимедийные возможности для Web-сайтов, позволяя пользователям слушать звуки и музыку и смотреть видеоклипы через сменные модули Web-браузеров. Хотя для использования таких традиционных форматов, как **wav**, **midi**, **mov** или **avi**, на Web-сайтах не требуется применение специального сервера, недавнее появление технологий потоковой передачи звуковой и видеоинформации во многих случаях сделало необходимым применение аудио- и видеосерверов (вместе с использованием таких инструментов, как, например, RealServer Plus). Появление новых потоковых технологий отмечает важный этап в развитии мультимедийных средств во Всемирной паутине, и, несомненно, эти технологии станут одними из самых интересных в истории Интернета.

Чат-серверы

Обмен сообщениями в реальном времени между двумя или более пользователями — довольно обычная практика. Такой обмен называется *чатом* (Chat — беседа), и чат-

серверы (использующие такие инструменты, как, например, MeetingPoint) позволяют управлять дискуссиями, проходящими в реальном времени с участием большого числа пользователей. Потенциальные области применения чат-серверов включают в себя проведение телеконференций, организацию закрытых зон для проведения совещаний, создание справочных форумов и форумов поддержки и проведение неформальных собраний сотрудников компаний. Среди трех основных типов серверов связи можно перечислить следующие: серверы с использованием системы Internet Relay Chat (IRC — общение с передачей через Интернет), серверы проведения конференций (conferencing servers) и серверы сообществ (community servers). В самых современных чат-серверах недавно появилась возможность дополнять обычную текстовую среду общения динамической голосовой (и даже видео) поддержкой. Нередко для чата, основанного на системе IRC, используется выделенный IRC-сервер (с применением такого программного обеспечения, как, например, IRCPlus).

FTP-серверы

Значительная доля интернет-трафика состоит из передачи файлов для самых различных целей — от получения нового программного обеспечения и до пересылки корпоративных документов. Серверы, использующие протокол передачи файлов (File Transfer Protocol, FTP), позволяют перемещать один или более файлов между компьютерами через Интернет с соответствующим уровнем безопасности и контролем целостности данных (с использованием таких инструментов, как, например, ZBServer Pro). Протокол FTP основан на типичной схеме "клиент-сервер". FTP-сервер выполняет основную работу по обеспечению безопасности передачи файлов, по организации их структуры и по управлению процессом их передачи. Клиент (иногда в его роли выступает компонент браузера или специальная программа, например, FTP Voyager) получает файлы и размещает их на локальном жестком диске.

Новостные серверы

Новостные серверы функционируют в качестве источников распространения и доставки новостей для более чем 20 000 новостных конференций общего пользования, доступ к которым в настоящее время можно получить через пользовательскую сеть Usenet (самая крупная в сети Интернет система рассылки новостей и организации дискуссионных форумов, упорядоченная по группам новостей этой сети). Новостные серверы основаны на инструментах (таких, например, как INN News Server), которые используют сетевой протокол передачи новостей (Network News Transfer Protocol, NNTP) для взаимодействия с другими новостными серверами USENET и распространения новостей любым пользователям, использующим программы с возможностями получения новостей (например, Agent или Outlook Express). Новостные серверы также позволяют создавать в Интернете или в локальной сети свои собственные группы новостей и дискуссий.

Серверы межсетевого обмена (шлюзы)

Шлюз (gateway) — это транслятор, который дает возможность разным сетям взаимодействовать между собой. Один из распространенных вариантов применения шлюзов заключается в том, чтобы использовать их в качестве трансляторов между персональными компьютерами и мини-компьютерами или большими ЭВМ. Например, шлюз электронной почты может служить для трансляции информации между GroupWise и SMTP-системами (Simple Mail Transfer Protocol — простой протокол

электронной почты, протокол SMTP). В локальной сети один из компьютеров обычно назначается в качестве шлюзового. Специальные прикладные программы в настольных компьютерах обращаются к более глобальной компьютерной системе посредством шлюзового компьютера, и пользователи могут получать доступ к ресурсам большой ЭВМ, как если бы эти ресурсы находились в настольном компьютере.

Брандмауэры и прокси-серверы

Говоря простыми словами, *брандмауэр* (firewall) — это механизм, который предназначен для защиты от несанкционированного доступа *из* или *в* частную компьютерную сеть (например, локальную сеть какой-либо корпорации) и обычно используется в качестве первой линии обороны при защите частной информации. Брандмауэры могут быть реализованы как аппаратно, так и программно (а чаще и тем, и другим образом). При грамотном использовании эти средства позволяют предотвратить попытки неавторизованных пользователей получить доступ к соединенной с Интернетом частной сети — в особенности внутренней сети. В больших корпоративных компьютерных сетях брандмауэры также используются для защиты от попыток несанкционированного доступа внутри локальной или внутренней сети. Все сообщения, исходящие *из* или входящие *во* внутреннюю сеть, проходят через брандмауэр, который проверяет каждое сообщение и блокирует те из них, которые не отвечают установленным критериям безопасности. Существует множество методов межсетевой защиты, включая пакетную фильтрацию (packet filters), сетевые межпрограммные конверторы (application gateways), аппаратные шлюзы и прокси-серверы. *Прокси-серверы*, наверное, являются самыми распространенными формами межсетевой защиты. На практике прокси-сервер размещается между клиентской программой (например, Web-браузером) и каким-либо внешним сервером (обычно это сервер, находящийся во Всемирной паутине). Прокси-сервер эффективно скрывает истинный сетевой адрес, затем отслеживает и перехватывает любые направляемые на внешний сервер или поступающие из Интернета запросы. Это позволяет производить фильтрацию сообщений, повысить производительность и совместно использовать межсетевые соединения.

Web-серверы

Web-серверы позволяют предоставлять информацию через Интернет посредством языка гипертекстовой разметки (HyperText Markup Language, HTML). При помощи такого программного обеспечения, как, например, Microsoft IIS (Internet Information Server — информационный сервер Интернет) или Apache, Web-сервер принимает запросы от браузеров (например, Netscape или Internet Explorer) и затем отправляет соответствующий(-ие) HTML-документ(-ы) обратно на тот компьютер, с которого поступил запрос. Для повышения мощности сервера может быть использован ряд серверных технологий, которые позволяют не только доставлять стандартные HTML-страницы, но и применять CGI-сценарии (common gateway interface — общий шлюзовой интерфейс), протокол безопасности SSL (Secure Sockets Layer — протокол защищенных сокетов), а также Active Server Pages (ASP — активные серверные страницы).

Telnet- и WAIS-серверы

Telnet-серверы позволяют пользователям подключаться к главному компьютеру и работать с ним так, как будто все задачи выполняются на самом удаленном компью-

тере. Пользователи могут подключаться к главной системе посредством Telnet-сервера из любой точки мира при помощи клиентского приложения Telnet. До появления всемирной сети серверы глобальной информационной системы WAIS (Wide Area Information Server) были единственным средством, позволяющим пользователям осуществлять поиск в содержании файлов по ключевым словам. Хотя сегодня система WAIS уже не так популярна, разработчики компьютерных сетей, которые хотят расширить набор интернет-служб, могут включить поддержку таких служб, как Telnet и WAIS.

Программное обеспечение серверов

Главное отличие серверов от одноранговых компьютеров заключается в их программном обеспечении. Независимо от того, насколько мощным может быть сервер, для него нужна операционная система (типа Windows NT/2000 Server, Novell NetWare или UNIX/Linux), которая позволит задействовать его ресурсы. Для серверов также необходимы специальные приложения, позволяющие им взаимодействовать с компьютерной сетью. Например, на Web-сервере могут использоваться Windows NT и Microsoft IIS. На данном этапе изложения читателю не обязательно иметь полное понимание программного обеспечения для серверов. В последующих главах будет дано более подробное рассмотрение сетевых протоколов и сетевых операционных систем.

Преимущества архитектуры "клиент-сервер"

Несомненно, компьютерные сети на основе серверов являются более сложными с точки зрения их создания и конфигурации, но они имеют ряд значительных преимуществ по сравнению с одноранговыми сетями.

- *Совместное использование.* Серверы позволяют более эффективно организовать ресурсы и совместно их использовать. Сервер предназначен для предоставления доступа ко множеству файлов и принтеров, сохраняя при этом высокую производительность и обеспечивая безопасность для пользователя. Сервер позволяет осуществлять централизованное администрирование и контроль над имеющимися в его распоряжении данными и ресурсами. Такой централизованный подход делает поиск файлов и ресурсов поддержки более простым, чем это было бы возможно при помощи независимого компьютера.
- *Безопасность.* В сети, основанной на сервере, один администратор может управлять безопасностью всей сети, устанавливая соответствующие сетевые политики и применяя их в отношении каждого пользователя и ресурса.
- *Резервирование.* Выполнение процедур резервирования также упрощается, поскольку эти процедуры необходимо применять только для серверов (применять резервирование для клиентских компьютеров/рабочих станций становится необязательно, хотя, конечно, возможно). Резервирование серверов может осуществляться автоматически по заранее установленному расписанию, даже если эти серверы физически находятся в разных частях компьютерной сети.
- *Отказоустойчивость.* Так как данные содержатся в основном на серверах, в них можно использовать систему отказоустойчивого хранения данных (т. е. RAID, Redundant Array of Independent Disks — матрица независимых дисковых накопи-

телей с избыточностью) для того, чтобы избежать потери данных из-за поломок дисковых накопителей или системных отказов. Это позволяет сделать сервер более надежным и снизить вероятность его простоя.

- *Пользователи.* Серверная сеть способна обеспечивать работу тысяч пользователей. Такой огромной компьютерной сетью невозможно было бы управлять при одноранговой архитектуре, однако существующие сегодня средства сетевого контроля и управления позволяют создавать компьютерные сети, включающие большое число пользователей.

Надежность серверов

Надежность в основном связана с понятиями устойчивости и безотказности работы и означает вероятность того, что какой-то компонент или система будут выполнять свою задачу в течение какого-то конкретного периода времени, — это может быть отнесено, в том числе, и к серверу, и к сети. Надежность часто измеряют как функцию времени, проходящего между сбоями, и обозначают термином "среднее время безотказной работы" (Mean Time Between Failure, MTBF). Целостность данных и возможность предупреждения об ожидаемых аппаратных сбоях являются двумя другими аспектами надежности. Серверы часто оснащаются такими средствами повышения надежности, как резервные источники питания и вентиляторы, анализ с прогнозированием возможных сбоев накопителей на жестких дисках (называемый технологией самоконтроля, анализа и предупреждения — SMART, Self-Monitoring, Analysis and Reporting Technology) и системы RAID для того, чтобы обеспечить непрерывность работы сервера и сохранность данных даже в случае возникновения неполадок. В числе других средств повышения надежности можно упомянуть самотестирование памяти при загрузке, во время которого система может выявлять и отключать дефектные блоки памяти, а также средства обнаружения и исправления ошибок (error checking and correction, ECC) памяти, позволяющие улучшить целостность данных.

Примечание

Надежность имеет критическое значение с точки зрения работы сервера и является абсолютно необходимой для долговременного функционирования компьютерной сети. Большие компьютерные сети обычно стремятся достичь 99,999% надежности или даже выше.

Высокий уровень доступности серверов

Сервер должен быть постоянно "в строю" и находиться в готовности к непосредственному применению, чтобы пользователи могли в реальном времени получать доступ к необходимым ресурсам. Короче, речь идет о *высоком уровне доступности* (high availability). С другой стороны, высокий уровень доступности означает для сервера возможность быстро восстанавливаться после системных сбоев (например, возможность "горячего переключения" на RAID-диск для восстановления данных, хранившихся на отказавшем дисковом накопителе). Независимо от того, используются ли в системе с высоким уровнем доступности какие-либо резервные компоненты (например, резервные источники питания), эти системы должны поддерживать возможность горячей замены ключевых компонентов. *Горячая замена* (hot swapping) —

это возможность извлечь из системы отказавший компонент и поставить вместо него новый при включенном питании с сохранением функциональности системы. Система с высоким уровнем доступности также обладает способностью выявлять потенциальные сбои и явным образом перенаправлять или переключать сомнительные процессы на другие устройства или подсистемы. Например, некоторые SCSI-накопители (Small Computer Systems Interface — интерфейс малых компьютерных систем) могут автоматически перемещать данные из крайних секторов (т. е. секторов, в которых иногда могут происходить ошибки чтения) в запасные секторы без уведомления об этом операционной системы или пользователя.

В общем, параметр доступности измеряется как процент того времени, в течение которого система остается функционирующей и доступной к использованию. Например, система, которая обеспечивает 99% доступность при круглосуточном доступе, в действительности будет давать потерю 88 часов работы в год, что является неприемлемым для многих пользователей. А вот 99,999% уровень доступности означает приблизительно 5,25 минут незапланированного простоя в год, однако достижение такого уровня может быть довольно дорогостоящим.

Расширяемость серверов

Компьютерные пользователи прошлых времен при покупке базового блока системы часто выбирали его размером в два раза больше, чем было необходимо, — с учетом будущего расширения, машину выбирали "на вырост". Сегодня можно сразу выбрать компьютер, подходящий под нужную задачу, а потом добавлять оборудование по мере необходимости. Это называется *расширяемостью* (scalability). Расширяемый персональный компьютер может быть увеличен по размерам (объема) и скорости. Некоторые машины имеют конструктивные ограничения для расширения, тогда как другие могут быть расширены до любого нужного размера. Расширяемость также подразумевает возможность увеличивать объем оперативной памяти (Random-Access Memory, RAM), добавлять дополнительные процессоры (для многопроцессорных платформ), добавлять запоминающие устройства (накопители на жестких дисках), при этом сохраняя функциональность машины в рамках сетевой операционной системы.

Между расширяемостью и модернизацией (upgrading) есть небольшое различие. Модернизация — это замена существующего компонента на другой, более быстрый и совершенный. Расширение персонального компьютера — это добавление новых компонентов с целью увеличения его производительности. Например, обычный ПК имеет один процессор. Этот процессор можно заменить на более быструю модель (модернизация), но увеличить процессорные мощности ПК за счет добавления новых процессоров (расширение) невозможно — для этого нужно, чтобы в нем была установлена многопроцессорная материнская плата. В отличие от процессора, практически во всех персональных компьютерах можно расширить память (RAM), просто добавив в систему новые модули DIMM (Dual In-line Memory Module — модуль памяти с двухрядным расположением выводов). Все это распространяется и на дисковые накопители, — вы можете произвести модернизацию и установить диск с большим объемом памяти и с большей скоростью работы, или расширить объемы физической памяти системы, добавив в нее дополнительные жесткие диски.

Симметричная многопроцессорная обработка и параллельная обработка

Поскольку процессоры являются ключевыми элементами производительности и расширяемости сервера, имеет смысл рассмотреть несколько подробнее мультиобработку. Машина с симметричной мультиобработкой (Symmetric multiprocessing, SMP) представляет собой компьютер, в котором применяются два или более процессоров. Эти процессоры совместно используют общую память и работают под управлением одной операционной системы. SMP-машины могут быть расширены добавлением новых процессоров по мере роста потребностей предприятия и увеличения количества приложений. Помимо процессоров, такие компьютеры, как правило, допускают возможность расширения памяти, кэша и дисковых накопителей. На сегодняшний день SMP-машины могут быть расширены с 2 до не более чем 32 процессоров.

При использовании SMP следует учитывать некоторые ограничивающие факторы. Хотя может показаться, что количество процессоров в этих системах возможно расширить до более чем 32, это на самом деле не так. Если вы к двум процессорам добавите еще два, в результате вы получите почти 100%-ное повышение производительности, однако поскольку на все эти процессоры приходится только одна операционная система и только одна совместная память, с увеличением числа процессоров производительность будет снижаться. Для большинства SMP-систем заметного повышения производительности можно достичь, если увеличить число процессоров не более чем до 8 (эффект снижения производительности от роста числа процессоров также зависит от того, какая операционная система и приложения используются). Сегодня не так уж редко можно встретить системы на основе UNIX с 16 и более процессорами, тогда как системы на основе Windows NT, как считается, можно расширить приблизительно только до 4 процессоров. Кроме того, нужно учесть, что многие операционные системы и приложения при работе с базами данных могут использовать только первые 2 Гбайт памяти.

Некоторые из крупнейших в мире систем, обладающих наибольшими возможностями расширения, используют технологию параллельной обработки. *Параллельная обработка* (parallel processing) является шагом вперед в области симметричной многопроцессорной обработки, т. к. в ней сочетаются сразу несколько SMP-узлов. Эти узлы могут работать параллельно с одним и тем же приложением — обычно это база данных с возможностью параллельной передачи данных. Так как каждый узел имеет свою копию операционной системы, и все узлы взаимодействуют между собой посредством специальной межпроцессорной схемы, добавление новых узлов не слишком снижает производительность работы операционной системы. Это позволяет расширять параллельную обработку до большего числа уровней, чем это было бы возможно при использовании только лишь симметричной обработки.

Кластеризация серверов

Несколько лет тому назад для работы сервера и использования всех его приложений нужен был только один процессор. С появлением многопроцессорной обработки, при которой два и более процессоров совместно используют одну память, сервер получил возможность работать как с более крупными приложениями, так и с большим числом этих приложений. Через некоторое время множество серверов стали организовывать в группы, в которых каждый сервер предназначался для выполнения

какой-то конкретной задачи (т. е. появились файловые серверы, серверы приложений и т. д.). Сегодня многие компьютерные сети высшего класса используют *серверные кластеры* (server clusters), в которых два или более серверных компьютера действуют как один сервер, за счет чего обеспечивается больший уровень доступности и производительности по сравнению с одной машиной. Приложения могут перемещаться с одного сервера на другой или запускаться на нескольких серверах одновременно, и все такие групповые операции происходят незаметно для пользователя.

Кластеризация позволяет достичь большего уровня доступности и расширяемости, чем это возможно при независимой работе компьютеров. Каждый узел в кластере, как правило, имеет свои собственные ресурсы (процессоры, устройства ввода/вывода, память, операционную систему, запоминающие устройства и т. д.) и контролирует свой круг пользователей. Высокий уровень доступности серверного кластера обеспечивается возможностью так называемого автоматического восстановления в случае отказа (failover). Когда один узел выходит из строя, его ресурсы могут быть переключены на один или несколько других узлов, входящих в кластер. Как только узел возобновляет свою работу в нормальном режиме, его ресурсы могут быть вручную (или автоматически) переключены обратно. Серверные кластеры также легко расширяемы, при этом нет необходимости прерывать их работу. Для выполнения модернизации компонентов одного сервера его функции нужно принудительно передать другим серверам кластера, после чего отключить сервер и добавить нужные компоненты. Затем сервер снова присоединяют к кластеру и переключают на него с других серверов прежние функции.

Кластеризация — на самом деле, не новая идея, но, как правило, всякий раз она реализуется каким-нибудь особым набором аппаратного и программного обеспечения. Теперь менеджеры информационных систем смотрят на кластеризацию серьезнее, поскольку она становится более доступной за счет применения серийного, стандартного оборудования (например, системы RAID или системы симметричной мультипроцессорной обработки, сетевых адаптеров и адаптеров ввода/вывода и других периферийных устройств). Хотя в будущем методы кластеризации станут еще более сложными, и формальные стандарты кластеризации продолжают разрабатываться, уже сегодня существует возможность применения многих из них.

Оборудование компьютерных сетей

Теперь, когда вы немного познакомились с видами компьютерных сетей и типами серверов, будет полезно узнать подробнее о различных аппаратных элементах, которые используются для построения компьютерных сетей. Сетевое оборудование имеет огромное значение с точки зрения скорости, качества и общей производительности компьютерной сети. В данной книге мы рассмотрим следующие виды *сетевого аппаратного обеспечения*: концентраторы, повторители, мосты, маршрутизаторы, шлюзы, сетевые платы и кабели.

Повторители

При прохождении электрических сигналов по кабелю происходит их ослабление и искажение. Этот эффект называется *затуханием* (attenuation). По мере увеличения длины кабеля эффект затухания усугубляется. По достижении некоторой длины ка-

беля эффект затухания делает сигнал окончательно неузнаваемым, что приводит к ошибкам передачи данных по сети. Специальное устройство, *повторитель* (repeater), позволяет увеличить путь прохождения сигнала посредством его усиления и передачи на следующий сегмент кабельной линии. Повторитель принимает слабый сигнал с одного кабеля, регенерирует его и передает на следующий кабель. В качестве повторителей часто используются активные концентраторы, однако повторители как самостоятельные устройства могут понадобиться для обслуживания очень длинных кабелей.

Важно понимать, что повторители являются всего лишь усилителями (или регенераторами сигнала) и не производят трансляцию или фильтрацию сетевых сигналов. Для нормальной работы повторителя необходимо, чтобы оба соединенных посредством него кабеля использовали одинаковые кадры (frames), логические протоколы и методы доступа. Наиболее распространенными методами доступа к среде передачи являются: CSMA/CD (Carrier Sense Multiple Access with Collision Detection — множественный доступ с контролем несущей и обнаружением коллизий) и эстафетная передача маркера (token passing). Повторитель не может соединить сегмент кабеля, использующий метод CSMA/CD, с сегментом, использующим метод эстафетной передачи маркера. Таким образом, повторитель не дает возможности установить соединение между сетью типа Ethernet и сетью типа Token Ring (локальной сетью на основе маркерного кольца) — для подобного рода трансляции используют более сложные устройства. Однако повторители *могут* перемещать пакеты из одной физической среды в другую. Например, повторитель может принять Ethernet-кадр, поступивший с тонкого коаксиального кабеля, и передать его на оптоволоконный кабель (при том условии, что этот повторитель имеет соответствующие физические разъемы).

Следует понимать, что поскольку повторители только лишь передают данные от одного кабеля к другому, ошибочные данные (например, деформированные пакеты) тоже будут переданы. Они не будут отфильтрованы, соответственно порождая излишний сетевой трафик. Как правило, следует избегать использования повторителей при большом сетевом трафике или в случаях, когда необходима фильтрация данных.

Концентраторы

Говоря простым языком, *концентратор* (hub) — это главное соединительное устройство, которое связывает компьютеры в сети звездообразной топологии. Разновидностью концентратора является модуль множественного доступа (Multistation Access Unit, MAU), который используется для соединения персональных компьютеров в кольцеобразной локальной сети. Концентраторы сейчас являются стандартным видом оборудования для современных компьютерных сетей и обычно разделяются на два класса: *активные* и *пассивные*. Пассивные концентраторы не обрабатывают данные, и выполняют только коммутацию. В отличие от них, активные концентраторы (иногда называемые повторителями) регенерируют данные для поддержания достаточного уровня мощности сигнала. Некоторые концентраторы могут выполнять дополнительные функции, например, установление сопряжения, маршрутизацию или переключение. Сети с концентраторами обладают широкими возможностями и имеют преимущества по сравнению с системами без них. Например, в обычной шинной топологии разрыв кабеля приводит к сбою всей сети. Однако, если разрыв

происходит в каком-либо из кабелей, присоединенных к концентратору, нарушается только работа данного ограниченного сегмента компьютерной сети.

Большинство концентраторов являются активными, т. е. регенерируют и передают сигналы таким же образом, как и повторители. Поскольку концентраторы обычно имеют от восьми до двенадцати портов для присоединения компьютеров, их иногда называют *многопортовыми повторителями* (multiport repeaters). Активные концентраторы всегда требуют для своей работы источника электрического питания. Некоторые концентраторы являются пассивными (среди них можно упомянуть коммутационные платы и стековые блоки (punch-down blocks)). Они служат только в качестве соединительных устройств и не выполняют регенерации или усиления сигнала. Сигнал только проходит через концентратор. Для работы пассивного концентратора не требуется электрического питания. Новое поколение концентраторов позволяет одновременно использовать несколько разных типов кабелей. Этот вид концентраторов называется *гибридными концентраторами* (hybrid hubs).

Мосты

Мост (bridge) открывает другие возможности для интенсивно используемой компьютерной сети. Мост может действовать как повторитель для увеличения полезной длины сетевого кабеля. Однако мост — более "умное" устройство. Он может разделять компьютерную сеть на части для того, чтобы изолировать области повышенного трафика или данные с ошибками. Например, если трафик, исходящий от одного-двух компьютеров (или отделов), переполняет сеть и замедляет всю ее работу, мост может изолировать эти компьютеры (или отделы), переключив их на их собственный кабельный сегмент. Мосты не определяют виды протоколов, а просто пропускают по сети все из них. Поскольку по мостам проходят все протоколы, каждый компьютер должен самостоятельно определять доступный для него протокол. Мосты также позволяют связывать между собой разные физические среды передачи — например, кабель на основе витой пары и тонкий коаксиальный кабель.

Маршрутизация данных

Мост имеет и другие возможности по обработке данных, которых нет у концентраторов и повторителей. Мосты могут "прослушивать" весь трафик, выявлять адреса отправления и назначения каждого кадра и строить таблицу маршрутов (по мере поступления информации), что позволяет им эффективно распределять данные по разным частям компьютерной сети. Мосты обладают способностью "учиться" продвижению данных. По мере прохождения трафика через мост, в его памяти накапливается информация об адресах компьютерного оборудования. Эту информацию мост использует для построения таблицы маршрутов на основе исходных адресов. Изначально память моста пуста, так же как и его таблица маршрутов. При передаче пакетов информации выполняется копирование исходных адресов в таблицу маршрутов. Запоминая эти адреса, мост, в конце концов, "узнает" о том, какие компьютеры находятся в том или ином сегменте сети.

Когда мост получает кадр, исходный адрес сверяется с таблицей маршрутов. Если адрес отправления отсутствует в таблице, он добавляется в нее. После этого мост сверяет адрес назначения со своей базой данных. Если адрес уже имеется в таблице маршрутов и находится в том же сегменте сети, к которому относится и исходный адрес, тогда кадр не обрабатывается (поскольку предполагается, что данные будут

получены другим компьютером в той же части сети). Такая процедура фильтрации позволяет уменьшить трафик и отделить друг от друга разные части сети. Если же адрес назначения содержится в таблице маршрутов, но относится к другому сегменту сети (в отличие от исходного адреса), мост перенаправляет кадр из соответствующего порта по адресу назначения. Если адрес назначения не обнаружен в таблице маршрутов, мост направляет кадр по всем своим портам за исключением того, откуда он поступил.

Уменьшение трафика

Нужно иметь в виду, что хотя отправлять данные могут многие персональные компьютеры, входящие в сеть, не всем ПК эти данные могут понадобиться. Чтобы определить, для какой рабочей станции предназначена какая-то информация, все компьютеры должны ее принять, а затем каждый компьютер должен ждать возможности отправить свои данные. В большой сети такой порядок может значительно снизить общую производительность работы. Однако в больших компьютерных сетях рабочие станции часто группируются в отделы, и объем данных, пересылаемых между отделами, часто намного меньше того трафика, который порождается при пересылке данных между компьютерами внутри одного отдела. Разделив при помощи мостов всю сеть компании на несколько небольших подсетей, связанных с ее отделами, можно достичь уменьшения трафика в целом по сети, и таким образом улучшить ее общую производительность.

Для примера возьмем компанию, в которой существуют пять основных отделов: отдел продаж, бухгалтерия, экспедиторский отдел, отдел производства и отдел разработки. В "открытой" сети трафик, исходящий из персонального компьютера в отделе продаж, будет, в конце концов, доходить до каждой другой машины сети (т. е. до бухгалтерии, экспедиторского отдела и т. д.). Чаще всего трафик из одного ПК отдела предназначен для других ПК того же отдела, поэтому всем остальным компьютерам сети не имеет смысла тратить время на проверку этого трафика. Если использовать мост для разделения сети на пять разных областей, то трафик, исходящий от компьютера из отдела разработки и предназначенный для другого компьютера этого же отдела, не будет выходить в другие области сети. Это позволит уменьшить трафик, т. к. всем остальным ПК не нужно будет его проверять, чтобы определить, не предназначен ли он для них. Если с машины из отдела разработки отправляются данные на машину из отдела продаж, мост будет "знать" (посредством таблицы маршрутов), на какой сегмент сети передать этот трафик, и тогда остальным сегментам не придется обрабатывать его. Такой контроль (или ограничение) движения сетевого трафика называется *сегментированием* сетевого трафика. Большая сеть не ограничивается только одним мостом. Множество мостов может использоваться для связывания нескольких малых сетей в одну большую.

Удаленные соединения

Мосты часто используются для соединения между собой малых компьютерных сетей, которые разделяют большие физические пространства. Например, когда две отдельные локальные сети расположены на большом расстоянии друг от друга, их можно объединить в одну сеть при помощи двух удаленных мостов, связанных посредством синхронных модемов с выделенной телефонной линией для передачи данных.

Маршрутизаторы и мосты-маршрутизаторы

В более сложной сетевой среде, состоящей из нескольких сегментов с различными протоколами и архитектурой, зачастую недостаточно использовать мосты для обеспечения быстрого и эффективного взаимодействия между этими сегментами. Такая сеть требует применения более сложного устройства, способного знать адрес каждого сегмента, определять наилучшие пути для пересылки данных и отфильтровывать широковещательный трафик в локальном сегменте. Этот тип сетевых устройств называется *маршрутизаторами* (routers). Как и мост, маршрутизатор способен фильтровать и отделять сетевой трафик, а также соединять между собой сегменты сети. Кроме того, маршрутизаторы могут переключать и направлять пакеты данных по различным сетям посредством выполнения обмена особой протокольной информацией между разными сетями. Маршрутизаторы могут получать больше информации о пакетах данных, чем мосты, используя эту дополнительную информацию для улучшения передачи данных. Маршрутизаторы используются в сложных сетях, т. к. они дают возможность более эффективно управлять трафиком. Например, маршрутизаторы могут обмениваться между собой информацией о состоянии и маршруте данных и использовать эту информацию для того, чтобы обходить медленные или неисправные участки линий передач.

Есть два основных протокола для маршрутизаторов: статичный и динамичный. "Статичный маршрутизатор" иногда еще называется "ручным маршрутизатором", т. к. он должен настраиваться сетевым администратором вручную. Таблицы маршрутов в статичном маршрутизаторе являются фиксированными, поэтому в нем всегда используется один и тот же маршрут (даже если сетевая активность изменяется). Это означает, что маршрут, используемый маршрутизатором, не обязательно будет самым коротким. В отличие от него, "динамичный маршрутизатор" может иметь начальную настройку, но потом он будет автоматически адаптироваться к изменяющимся сетевым условиям, находя более короткие маршруты или же маршруты с менее интенсивным трафиком.

Маршрутизация данных

Маршрутизаторы ведут свои собственные таблицы маршрутов, которые обычно состоят из сетевых адресов (хотя при необходимости могут включать в себя и адреса хостов). Для определения адреса назначения поступающих данных в таблицу маршрутов включаются все известные сетевые адреса, логические инструкции для соединения с другими сетями, информацию о возможных путях между маршрутизаторами, и даже затраты на пересылку данных по каждому из путей. Таким образом, маршрутизатор использует свою таблицу маршрутов для того, чтобы выбрать *наилучший* маршрут для передачи данных с учетом возможных затрат и имеющихся путей. Следует понимать, что таблицы маршрутов, используемые в мостах, *отличаются* от тех, которые используются в маршрутизаторах.

Когда маршрутизатор получает пакет данных, предназначенный для пересылки на удаленную сеть, он отправляет этот пакет на маршрутизатор, обслуживающий сеть назначения. Использование маршрутизаторов позволяет разработчикам разделить крупные сети на небольшие сегменты и ввести элемент безопасности между ними. К сожалению, маршрутизаторы должны выполнять сложные функции при обработке каждого пакета, поэтому они работают медленнее, чем большинство мостов. На-

пример, по мере прохождения пакета данных от одного маршрутизатора к другому, исходный адрес и адрес назначения изменяются. Это позволяет направлять пакеты данных с Ethernet, находящейся под управлением протокола TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/протокол Интернета) на сервер, входящий в кольцевую локальную сеть, которая также использует протокол TCP/IP, — что недостижимо при помощи моста.

Уменьшение трафика

Маршрутизатор проверяет адрес назначения, содержащийся в пакете данных, и направляет этот пакет в соответствии с указанным адресом. Если сетевой адрес неизвестен, тогда пакеты передаются на шлюз, используемый по умолчанию. Никакой маршрутизатор не может знать адреса всех сетей, поэтому для неизвестных сетей все они используют маршрут, принятый по умолчанию. Маршрутизаторы не допустят передачи данных с ошибками в сеть. Способность маршрутизатора контролировать проходящие через него данные позволяет уменьшить объем трафика между сетями и использовать связи между ними более эффективно, чем это делают мосты. Поэтому маршрутизаторы могут значительно снизить объем трафика в сети, а также уменьшить время ожидания для пользователей. Однако следует помнить, что не все протоколы позволяют выполнять маршрутизацию *(более подробно о протоколах речь пойдет в гл. 2)*. Среди типичных протоколов, допускающих маршрутизацию, можно перечислить следующие: DECnet, протокол IP и протокол межсетевого пакетного обмена (Internetwork Packet Exchange, IPX), в то время как локально-сетевой транспортный протокол (Local Area Transport Protocol, LATP) или расширенный пользовательский интерфейс сетевой базовой системы ввода/вывода (NetBIOS Extended User Interface, NetBEUI) не предусматривают маршрутизации. Существуют маршрутизаторы, которые могут работать с несколькими протоколами одновременно внутри одной компьютерной сети (например, IP и DECnet).

Выбор маршрута

Заметным преимуществом маршрутизаторов является то, что они могут поддерживать множество активных путей между сегментами локальной сети и даже при необходимости выбирать резервные пути. Поскольку маршрутизаторы способны связывать между собой сегменты, использующие совершенно разные схемы доступа к данным и их упаковки, обычно маршрутизатор может использовать несколько возможных путей. Например, если один из маршрутизаторов не функционирует, данные все же можно переслать при помощи других маршрутизаторов. Это также относится и к сетевому трафику. Если один из путей слишком загружен, маршрутизатор определяет альтернативный путь и пересылает данные через него. В маршрутизаторах применяются весьма мощные алгоритмы, например, первоочередное открытие кратчайших маршрутов (Open Shortest Path First, OSPF), протокол маршрутной информации (Routing Information Protocol, RIP) или протокол коммуникационных услуг NetWare (NetWare Link Services Protocol, NLSP), которые служат для определения наиболее подходящего пути передачи пакета данных.

Мост-маршрутизатор

По мере развития технологии функциональные различия между мостами и маршрутизаторами становится все более размытой. Некоторые мосты обладают особыми

возможностями, позволяющими им выполнять такие задачи, которые обычно требуют использования маршрутизатора. Такие более совершенные мосты называются *мостами-маршрутизаторами* (bridge router, brouter — брутер). Мост-маршрутизатор может выступать для одного протокола в качестве "маршрутизатора", а для всех остальных — в качестве "моста". Мост-маршрутизатор может трассировать отдельные маршрутизируемые протоколы, сопрягать немаршрутизируемые протоколы и обеспечивать более эффективные и более контролируемые межсетевые взаимосвязи, чем это могут делать мосты и маршрутизаторы сами по себе.

Шлюзы

Шлюз (gateway) действует в качестве мощного преобразователя, предназначенного для создания связи между совершенно разными сетями. Хотя шлюз работает медленнее, чем мост или маршрутизатор, он может выполнять такие сложные функции, как, например, осуществление трансляции данных между сетями, использующими разные языки, при помощи таких методов, как преобразование протоколов и полосы пропускания (protocol and bandwidth conversion). Например, шлюз может преобразовать приложение cc:Mail в SMTP, и наоборот. Шлюзы позволяют устанавливать связь между сетями совершенно разных архитектур и типов. Они способны эффективно изменять способ сжатия данных и преобразовывать данные, исходящие из компьютерной сети одного типа и направленные в сеть другого типа, таким образом, обеспечивая взаимодействие между этими сетями. Шлюз изменяет способ сжатия данных в соответствии с требованиями системы назначения и изменяет формат сообщения в соответствии с тем приложением, которое работает на принимающем конце линии. В большинстве случаев шлюзы предназначены для выполнения какой-то конкретной задачи, т. е. для выполнения какого-то конкретного типа передачи данных. Часто их обозначают по той задаче, которую они выполняют (например, шлюз Windows NT/SNA).

Сетевая плата

Сетевая интерфейсная плата, также известна под названием "сетевого адаптера" (LAN adapter) функционирует в качестве устройства сопряжения между отдельным компьютером (сервером или клиентом) и кабельной системой сети (рис. 1.2). С точки зрения компьютера, она должна идентифицировать ПК в сети и выполнять буферизацию данных между компьютером и кабелем. При отправлении данных она должна преобразовывать байты параллельного кода в последовательные биты (и наоборот при получении данных). С точки зрения компьютерной сети, эта плата должна генерировать электрические сигналы, проходящие по сети, управлять доступом к сети и обеспечивать физический контакт с кабелем. Каждый компьютер сети должен иметь по крайней мере один порт сетевой платы. Современные сетевые адаптеры могут увеличивать производительность при помощи новых методов группирования адаптеров (например, метода обеспечения отказоустойчивости адаптера — Adapter Fault Tolerance, AFT), которые автоматически поддерживают средства резервирования для сетевой платы. Если первичный адаптер выходит из строя, его заменяет вторичный. Адаптивная балансировка нагрузки (Adaptive Load Balancing, ALB) позволяет распределять поток передаваемых данных между 2—4 сетевыми адаптерами. Более подробно сетевые интерфейсные платы будут рассматриваться далее в этой книге.

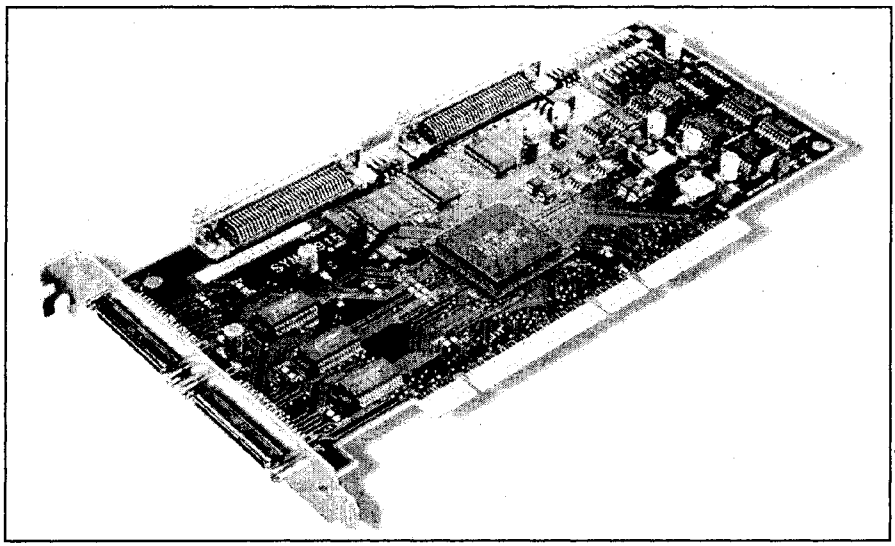


Рис. 1.2. Сетевая интерфейсная плата Symbios SYM22915 (с разрешения LSI Logic Corp.)

Кабели

И наконец, компьютерные сети любых размеров и конфигураций физически строятся при помощи кабелей, которые соединяют между собой персональные компьютеры и другое сетевое оборудование. Кабели, которые также называют *сетевой средой* (network media), имеют множество различных конфигураций, но для компьютерных сетей, как правило, используют следующие типы: кабель на основе неэкранированной витой пары, коаксиальный кабель, кабель на основе экранированной витой пары и оптоволоконный кабель. С технической точки зрения кабели, используемые для компьютерных сетей, должны обладать тремя следующими основными свойствами:

- защищенность от *перекрестных* (взаимных) *помех* (электрических токов, возникающих между проводниками внутри кабеля);
- защищенность от помех, наведенных внешними электрическими полями (создаваемыми электрическими моторами, линиями электропередачи, ретрансляторами и передатчиками);
- простота в монтаже.

Эти свойства являются довольно важными, т. к. кабели, имеющие защиту от перекрестных помех и помех от внешних электрических полей, можно прокладывать на большие расстояния, и они способны обеспечить более высокие скорости передачи данных. Например, коаксиальный кабель и кабель на основе экранированной витой пары имеют внешний слой в виде металлической фольги, который создает защиту от электрического шума, однако использование фольги делает кабель более толстым, что затрудняет его монтаж внутри кабельных трубопроводов и стен. Кабель на основе неэкранированной витой пары имеет меньший диаметр, и его легче монтировать,

но он в меньшей степени защищен от электрического шума. В отличие от электрических кабелей оптоволоконный кабель передает не электричество, а свет, поэтому он не подвержен воздействию электрических помех. Оптоволоконный кабель позволяет передавать сигналы быстрее и на большие расстояния, чем любой другой тип кабеля. К сожалению, такой кабель зачастую намного дороже других типов кабеля, и для его правильного монтажа требуются специальные инструменты и прошедшие специальную подготовку работники.

Персонал компьютерных сетей

При работе с автономным компьютером за его производительность следит, в конечном счете, каждый пользователь самостоятельно. Некоторые пользователи просто имеют в этом больше способностей или умения, чем другие, поэтому их часто просят помочь при возникновении каких-либо проблем в работе ПК. Низкая эффективность использования автономных ресурсов становится повседневным явлением в работе офисов. При наличии компьютерной сети обязанности по ее управлению и обслуживанию передаются группе специально подготовленных профессионалов. Если ранее вы не имели дела с компьютерными сетями в своей организации, то вам следует познакомиться с теми несколькими должностями, которые обеспечивают поддержку сетей.

Администратор компьютерной сети

Как бы они ни были нужны, компьютерные сети не материализуются просто из воздуха. Они создаются трудом талантливых и опытных людей, в том числе *сетевых администраторов* (network administrator). Сетевой администратор должен быть хорошо подготовлен и разбираться в каждом аспекте компьютерной сети, исходя из детальной информации о ней. Компьютерная сеть требует ежедневного обслуживания и наблюдения для того, чтобы она правильно функционировала и обеспечивала безопасность огромных объемов данных, хранящихся в ней. Сетевой администратор, безусловно, является ключевой фигурой в любой компьютерной сети и может добиться от нее максимальной производительности, даже если она не совсем современна.

Если вы создаете в своей организации компьютерную сеть взамен автономных ПК, лучше всего начать с назначения сетевого администратора. Администратор должен быть первым привлечен к созданию сети и иметь возможность вникать в каждый аспект системы в процессе ее разработки и построения. Как правило, поиск подходящего администратора производится целенаправленно. Проводите подробные интервью, тщательно проверяйте рекомендации и нанимайте только того кандидата, который имеет серьезные достижения и хорошие отзывы. Кроме того, можно инвестировать в подготовку уже существующего работника, который продемонстрировал соответствующие способности. Этот работник должен стремиться к достижению наилучших результатов, поиску способов извлечения максимума возможностей из существующих технологий и избежанию необдуманных затрат на приобретение новых технологий.

Другой персонал

Хотя сетевой администратор может в одиночку справиться с обслуживанием небольшой или средней по размеру сети, компьютерные сети более крупных размеров или имеющие специальное назначение могут потребовать дополнительного персонала для управления базами данных, обслуживания электротехнической части сети, разработки Web-страниц и т. д.

Администратор по сетевой безопасности

В очень больших организациях сетевой администратор может один не справиться со всеми важными вопросами сетевой безопасности, которые часто возникают в крупных сетях. Поэтому для работы над этими вопросами может быть назначен специальный человек — *администратор по сетевой безопасности* (security administrator), в обязанность которого входит ведение протоколов безопасности, управление паролями, контроль и расследование случаев сетевых атак и управление физическим доступом к сетевому оборудованию.

Администратор баз данных

Администратор баз данных (database administrator) в основном отвечает за программирование и обслуживание большой мультиреляционной базы данных, содержащейся в компьютерной сети, а также за обеспечение прямого доступа пользователей к этой базе данных.

Менеджер рабочих групп

Менеджер рабочих групп обычно отвечает за решение системных проблем, разработку стандартов и сетевых решений, слежение за производительностью компьютерной сети и оптимизацию производительности работы той или иной группы пользователей, которые коллективно (как группа) соединены с большим сетевым окружением.

Персонал сетевой поддержки

Как правило, работники из группы сетевой поддержки обеспечивают техническую помощь системному администратору в большой, сложной компьютерной сети. Персонал сетевой поддержки осуществляет текущую работу по устранению возникающих неисправностей, разрешению проблем и оказанию персональной помощи конечным пользователям сети.

Подрядчик по техническому обслуживанию сети

Фирма по техническому обслуживанию отвечает за ремонт и модернизацию сетевого оборудования (например, монтаж кабельных сетей в каком-либо здании или модернизацию дисковых накопителей на всех рабочих станциях компьютерной сетевой системы). Во многих случаях в качестве такого подрядчика выступает сторонняя обслуживающая компания или системный поставщик.

Web-мастер

Web-мастер отвечает за разработку и обслуживание содержания и оформления сайта компании в сети Интернет. Кроме того, Web-мастер следит за точностью информации и ее обновлением на Web-сайте, а также оформляет информацию таким образом, чтобы привлечь и заинтересовать пользователя.

Основы сетевой документации

Если вы собираетесь отправиться в путешествие в незнакомое вам место, то, скорее всего, вы возьмете с собой карту. Разумный человек не скажет вам, что карта бесполезна, и не станет убеждать вас в том, что карта не нужна, когда вы что-то ищите. И все же, от сетевых специалистов часто требуют, чтобы они работали без достаточной (или вообще без) документации по физической и логической установке компьютерной сети. Со временем даже простые сети могут развиться в сложное построение из серверов, рабочих станций и сетевой среды. В результате, хотя рабочие станции и серверы сами по себе могут быть вполне понятными, взаимосвязи и компоновка различных элементов аппаратного и программного обеспечения могут быть весьма запутанными. Причина вполне очевидна — ведение и обновление документации требует много времени, а когда его не хватает на неотложные проблемы установки, модернизации и устранения неисправностей, про документацию часто совсем забывают. К сожалению, схема и конфигурация компьютерной сети остается только в голове сетевого администратора или другого персонала, и многие опытные специалисты могут рассказать истории о страшных бедах, которые случались после того, как из компании уходил *последний* человек, хорошо знавший их сеть.

Для того чтобы избежать подобного рода проблем, все технические специалисты должны иметь доступ к полному собранию документации по сети. Набор этих документов может сильно различаться в зависимости от компании, но, по сути, современная документация должна давать информацию о том, как сеть должна выглядеть и работать, а также о том, где можно получить помощь в случае возникновения проблем. Документация дает те важные подробности, по которым вы можете понять, где следует искать решения возникающих проблем, и всегда будет полезна в тех случаях, когда вам нужно исправить или модернизировать компьютерную сеть. Сетевая документация, как правило, должна содержать следующую информацию.

- Физическую карту всей сети, включая расположение всех компонентов аппаратного оборудования и кабелей. Физическая карта может сопровождаться логической схемой компьютерной сети (например, "звездообразная топология"), хотя это не всегда обязательно.
- Полную информацию о каждом сервере (марка, модель, набор собственных устройств). Также сюда должно быть включено расписание выполнения резервирования информации, содержащейся в этих серверах, а также расположение выполненных резервных копий. Также имеет смысл собирать аналогичные сведения по каждой рабочей станции, но, в большинстве случаев, в менее подробной форме.
- Полную информацию о каждом повторителе, концентраторе, мосте и маршрутизаторе. Часто для этого достаточно указать их месторасположение на карте ком-

пьютерной сети и приложить копию руководства по эксплуатации каждого из устройств.

- Полную информацию о сетевой операционной системе и прикладном программном обеспечении, включая информацию о версиях, лицензиях и поддержке (а также о месторасположении всех инсталляционных CD-дисков).
- Полный список производителей, поставщиков, подрядчиков и других компаний, имеющих отношение к данной компьютерной сети. Если обслуживание какого-либо оборудования выполняет его производитель или сторонняя организация, в общий набор документации следует также включить копии действующих соглашений по такому обслуживанию.
- Подробный протокол с описанием всех возникших проблем, включая симптомы и решения, даты, контакты, примененные процедуры и достигнутые результаты.

Логические карты

Логические (или *функциональные*) карты обычно представляют собой документацию, которую вы будете составлять и использовать чаще всего (рис. 1.3). Они служат в качестве структурной схемы компьютерной сети и наглядно показывают, какое устройство (или сервер) отвечает за ту или иную основную функцию. Логические карты также показывают, какие устройства зависят в своей работе от других устройств. Здесь важны не детали, а общее описание потоков данных или взаимосвязей между устройствами. Логическая карта помогает разобраться в схеме взаимосвязей внутри

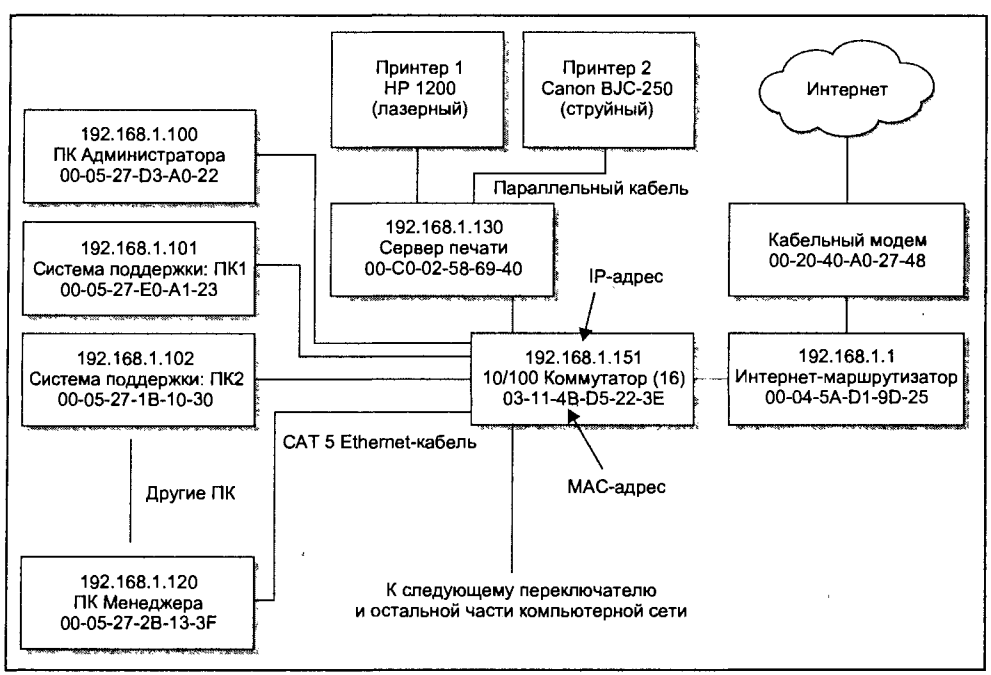


Рис. 1.3. Пример логической карты компьютерной сети

компьютерной сети (например, почему отдел А не может получить доступ к серверу, в отличие от отдела В).

Нет необходимости отображать в логической карте каждый персональный компьютер или принтер, но в ней *следует* указать каждое устройство, от которого зависит работа всей сети (как, например, серверы и маршрутизаторы). Концентраторы и переключатели часто отображают отдельно, однако в некоторых сетевых конфигурациях (например, когда переключатель связывает между собой две существенно отличающихся области компьютерной сети) лучше выделять их особым образом. Если сеть довольно большая или сложная, не бойтесь использовать несколько листов бумаги, чтобы не "впихивать" все в одну страницу. Для крупных компьютерных сетей обычно составляют "общий вид сверху" на одной странице, а потом делают подробное описание каждой области компьютерной сети на отдельном листе. Например, на общей схеме могут отображаться основные области компьютерной сети в виде прямоугольников, относящихся к отдельным более подробным картам.

Физические карты

Физические карты описывают физическую реализацию компьютерной сети, т. е. то, как элементы оборудования компьютерной сети физически взаимосвязаны между собой. Поскольку физические карты часто имеют намного более подробное содержание, чем логические карты, как правило, их удобнее составлять в виде небольших и наглядных рисунков (см. пример на рис. 1.4). Для некоторых небольших компьютерных сетей (обычно менее 50 ПК) можно обойтись только одной физической картой. При больших размерах компьютерных сетей обычно нужно составлять физическую карту для каждого этажа здания, в котором эта сеть расположена. Для большинства сетевых конфигураций эту карту довольно непросто составить, поскольку в ней необходимо отобразить буквально каждый провод, подходящий к буквально каждому ПК, принтеру, переключателю и маршрутизатору, что может сделать физическую карту довольно громоздкой. В случае более простых сетевых конфигураций можно взять архитектурный план здания и отобразить на нем местоположение сетевых проводов и электрических щитов. Для более сложной сети может также потребоваться дополнительная документация в виде карты физических сегментов компьютерной сети.

Примечание

В качестве физического *сегмента* компьютерной сети часто рассматривается группа концентраторов, соединенных между собой без применения маршрутизатора или переключателя. Любые концентраторы, которые соединены между собой посредством переключателя или маршрутизатора, всегда рассматриваются как отдельные физические сегменты и при больших размерах требуют составления отдельной карты.

Как правило, физическую карту следует делать как можно более подробной. Нельзя забывать об обновлении физических карт в соответствии с происходящими изменениями сети. Примите это в качестве стандартной процедуры, выполняемой персоналом по консультированию, сетевому обеспечению и поддержке персональных компьютеров, особенно если добавлениями и изменениями занимаетесь вы, а не персонал по консультированию или какой-либо другой сторонний персонал. Не

забывайте указывать на карте дату. По мере развития сети, в конце концов, появится множество карт для одной и той же ее области, и если на каждой карте будет указана дата ее создания, это поможет определить, какая из них является верной.

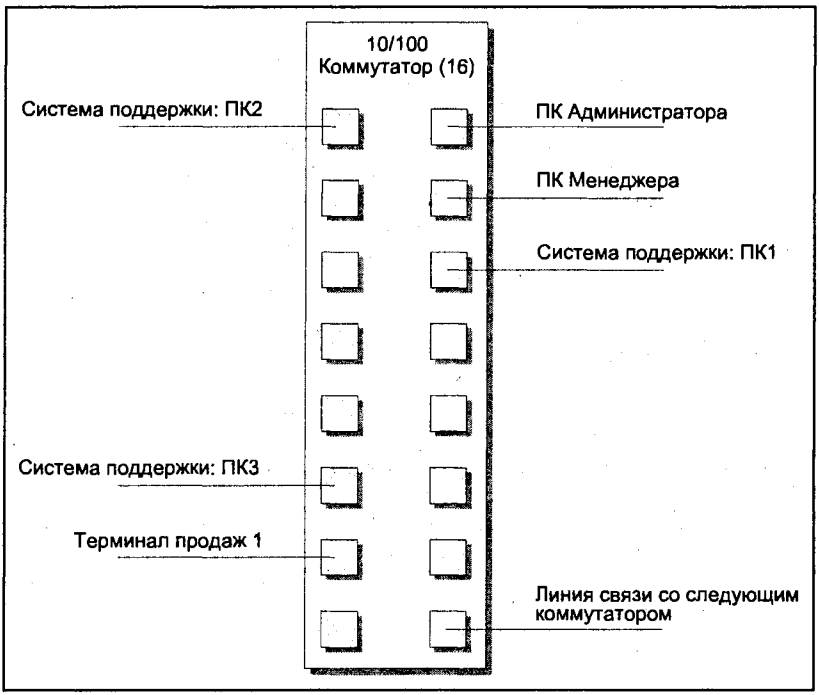


Рис. 1.4. Пример физической карты компьютерной сети

Примечание

Старайтесь не использовать цвета при составлении карт. Хотя цвета могут быть полезными, они легко теряются при копировании или пересылке по факсу. Вместо цветов используйте символы для выделения важной информации на физической карте.

Маркировочные знаки и обозначения

Конечно, карта оказывается совершенно бесполезной, если вы не можете найти устройства, отображенные на ней. Если вы управляете автомобилем, ориентируясь по дорожной карте, вы не сможете понять, по какой дороге едете, без помощи знаков, выставленных вдоль нее. Это же относится и к компьютерным сетям. Бывали случаи, когда люди не могли перезагрузить маршрутизатор, т. к. никто из них не знал, где именно он находится и как вообще выглядит. Хороший технический специалист имеет привычку заранее наносить ясную и короткую *маркировку* на каждое устройство. Неправильные или неполные обозначения могут значительно увеличить время простоя, несмотря на наличие подробной и новейшей документации.

Если вы обнаруживаете, что устройства и кабели, имеющиеся в вашей сети, не имеют маркировки, и вы уже не можете заставить вашего поставщика (-ов) вернуться и нанести эту маркировку, вам придется начать это дело самостоятельно. Например, каждый раз, когда вы находите какой-нибудь кабель или сетевое устройство, прикрепите к нему соответствующий ярлык. Это позволит вам избавиться от необходимости полагаться на свою память и даст возможность другим людям выполнять задачи по текущему обслуживанию сети, ее модернизации и исправлению без вашего непосредственного участия. Как правило, обычного маркировочного устройства типа Dymo вполне достаточно для выполнения большинства работ, связанных с нанесением маркировочных обозначений, тем более что тяжелые пластиковые ярлыки не рвутся, не пылятся и не пачкаются.

Примечание

Помещайте маркировку на расстоянии 30—45 см от коннектора. Это может показаться большим расстоянием, но нужно учитывать, что рядом друг с другом часто оказывается *множество* кабелей. Если поместить ярлыки непосредственно рядом с коннектором, то их трудно будет различить, т. к. будет мешать множество других кабелей. Кроме того, маркировку следует помещать на *обоих* концах кабеля.

И наконец, нельзя забывать о своевременном обновлении маркировки (как и документации) вместе с изменениями в компьютерной сети. Это потребует некоторой дополнительной работы, которая, однако, поможет избежать многочасовых потерь из-за простоя и путаницы. Предположим, что вы обозначили маршрутизатор IP-адресом, но позже этот адрес изменился. Если возникнет какая-то проблема, технический специалист, рискуя потерять собственный рассудок, может потерять много времени на то, чтобы найти маршрутизатор по обозначенному на нем старому IP-адресу. Одна такая мелочь может изменить время простоя с 10 минут до 2 часов.

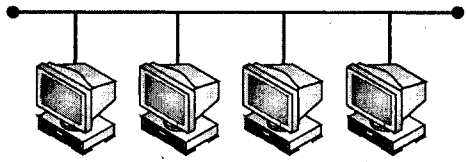
Дополнительные ресурсы

3Com Technology Information:
www.3com.com/solutions/en_US/technology.jsp?techid=0&solutiontype=1000003.

Google: **groups.google.com**.

Microsoft Knowledge Base (база знаний компании Microsoft):
search.support.microsoft.com/kb/c.asp.

Microsoft TechNet: **www.microsoft.com/technet/**.



ГЛАВА 2

Архитектура сетей и доступ к ним

В этой главе даются основные сведения о топологиях компьютерных сетей, кабелях и протоколах канала передачи данных. Сетевые топологии, сигналы и кабели являются тремя компонентами, составляющими физический уровень OSI-модели (модели взаимодействия открытых систем — Open Systems Interconnection). *Физический уровень* является первым уровнем OSI-модели и используется для определения характеристик аппаратных компонентов компьютерной сети, например, характеристики сигнала, используемого для передачи двоичных данных, типа сетевой платы, устанавливаемой на каждый компьютер сети, а также типа используемого концентратора. В число других элементов физического уровня входят различные типы медного и оптоволоконного кабеля, а также целый ряд различных средств беспроводной связи. В локальной сети характеристики физического уровня непосредственно связаны с протоколом *канального уровня*. Это значит, что от выбора протокола канала передачи данных зависит определение соответствующих характеристик физического уровня.

Протокол канального уровня связывает между собой сетевое оборудование каждого компьютера с его сетевым программным обеспечением. Протокол канала передачи данных, который был выбран при разработке локальной сети, является важнейшим фактором при определении и установке приобретаемого вами оборудования. Наиболее популярным протоколом канального уровня, используемым для локальных сетей, сегодня является Ethernet. Среди прочих локальносетевых протоколов стоит упомянуть маркерное кольцо (Token Ring) и распределенный интерфейс передачи по оптоволоконным каналам (Fiber Distributed Data Interface, FDDI). Настоящая глава начинается с описания одного из компонентов физического уровня — сетевых топологий.

Топологии компьютерных сетей

Термин "топология" выражает то, как компьютеры и другие устройства связаны между собой посредством кабелей. Тип используемого вами кабеля определяет топологию вашей компьютерной сети. Имея один из типов кабеля, невозможно построить компьютерную сеть с любой топологией. Для каждого типа кабеля следует использовать соответствующую топологию. Есть три основных вида топологии, применяемых для локальных компьютерных сетей: шинная, звездообразная и кольцевая. Все-

го в данной книге обсуждается семь видов топологии: шинная, звездообразная, шинно-звездообразная, иерархическая звездообразная, кольцеобразная, решетчатая и беспроводная.

Топология типа "Шина"

При шинной топологии компьютерной сети компьютеры и другие устройства соединены между собой последовательно посредством единого кабеля (шины). Такая конфигурация еще часто называется "гирляндной цепью". Все сигналы, передаваемые системами, входящими в сеть, проходят по шине в обоих направлениях через все другие системы, пока не достигнут пункта назначения. В шинной топологии всегда имеется два открытых конца (рис. 2.1), которые должны завершаться электрическим сопротивлением (оконечной нагрузкой) во избежание отражения сигналов и их последующего смешивания со вновь передаваемыми сигналами. При недостаточной оконечной нагрузке на одном или обоих концах шины компьютеры, которые подключены к ней, не могут правильно взаимодействовать.

В топологии типа "Шина" по стандарту Ethernet используется два вида кабельного соединения: толстый (thick) и тонкий (thin). В стандарте Thick Ethernet используется один сплошной коаксиальный кабель. Компьютеры, входящие в такую сеть, присоединяются к этому кабелю посредством небольших кабельных сегментов, называемых интерфейсными кабелями подключаемых устройств (Attachment Unit Interface cable, AUI) или кабелями трансивера (transceiver cables). В стандарте Thin Ethernet используется более тонкий коаксиальный кабель, разделенный на несколько сегментов. Каждый такой сегмент соединяет между собой два компьютера.

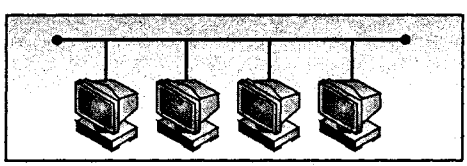


Рис. 2.1. Шинная топология

Каждый компьютер сети имеет приемопередающее устройство (трансивер), предназначенное для передачи и приема данных через сетевой кабель. Все стандарты физических уровней Ethernet-сетей, за исключением сетей типа Thick Ethernet, предусматривают интеграцию приемопередатчика в сетевую интерфейсную плату. Thick Ethernet является единственной формой Ethernet-сетей, в которой интерфейс используется отдельно от сетевой платы. Приемопередатчик присоединяется к коаксиальному кабелю при помощи прокалывающего ответвителя, а затем к сетевой плате компьютера при помощи AUI-кабеля (рис. 2.2).

Основной недостаток шинной топологии заключается в том, что при любом повреждении кабеля, оконечной нагрузки или коннектора нарушается работа всей компьютерной сети. Сеть оказывается разбитой на части, и поэтому взаимодействие между системами становится невозможным. Кроме того, при разрыве внутри компьютерной сети, вызванном нарушением в работе какого-либо ее компонента, каждая часть сети теряет оконечное сопротивление, что приводит к отражению сигнала и искажению данных.

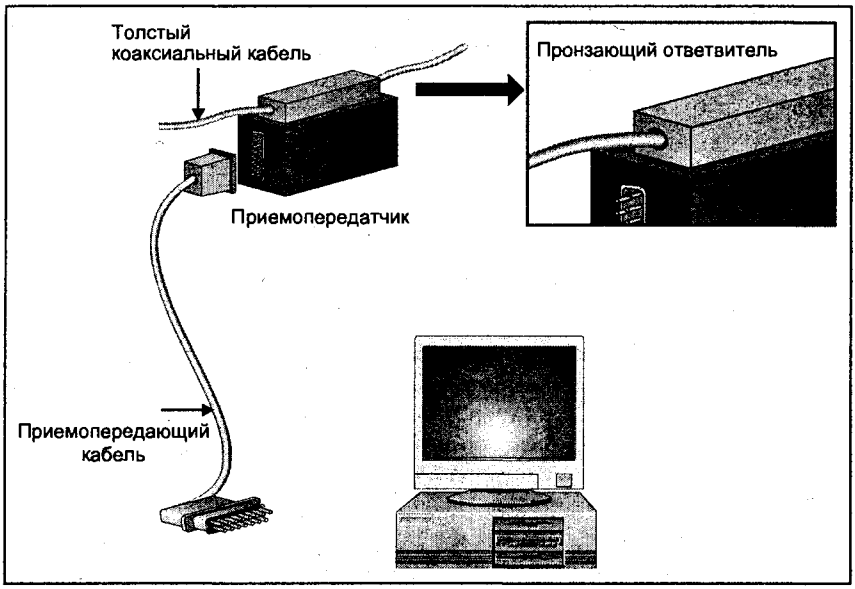


Рис. 2.2. Трансивер с ответвителем, применяемый для соединения AUI-кабеля с толстым коаксиальным кабелем

Топология типа "Звезда"

Топология типа "Звезда" (star topology) использует специальное коммутирующее устройство — концентратор (Hub). Каждый компьютер подключается к концентратору при помощи отдельного кабеля (рис. 2.3). В звездообразной топологии используется кабель на основе витой пары, подобный тем, которые описаны в спецификациях 10BaseT и 100BaseT. Большинство локальных сетей, использующих протокол Ethernet, а также многие компьютерные сети, использующие другие протоколы, строятся на основе звездообразной топологии.

Хотя каждый ПК не связан непосредственно с остальными компьютерами и подключен только к концентратору посредством отдельного кабеля, все сигналы, поступающие на любой из портов концентратора, передает на все остальные порты. Таким образом, все сигналы, передаваемые ПК в сеть, достигают всех остальных компьютеров.

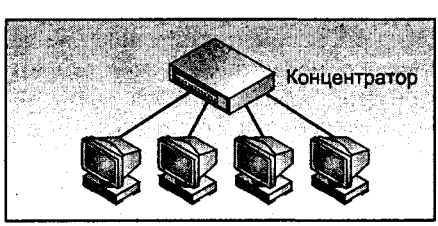


Рис. 2.3. Звездообразная топология

Благодаря тому, что каждый ПК имеет выделенное соединение с концентратором, топология типа "Звезда" обеспечивает более надежную работу сети, чем шинная, т. к. повреждение какого-либо кабеля затрагивает работу только одного компьютера, использующего этот кабель, и не влияет на работу остальной части сети. Недостатком звезды является то, что для нее требуется дополнительное устройство — концентратор. Выход из строя концентратора затрагивает всю сеть, — она вся целиком перестает работать.

Топология типа "Звезда — Шина"

Топология типа "Звезда — Шина" позволяет увеличить количество топологических звезд в локальной сети. При таком расширении несколько звездообразных структур связываются между собой при помощи специальной шины, соединяющей их концентраторы (рис. 2.4). Каждый концентратор передает поступающие в него данные через свой шинный порт на аналогичный порт концентратора другой звезды, что позволяет всем компьютерам локальной компьютерной сети взаимодействовать между собой. Данная топология изначально была разработана для расширения Ethernet-сетей спецификации 10BaseT, но из-за снижения производительности работы компьютерной сети, вызванного низкой пропускной способностью коаксиальной шины, сегодня она редко используется.

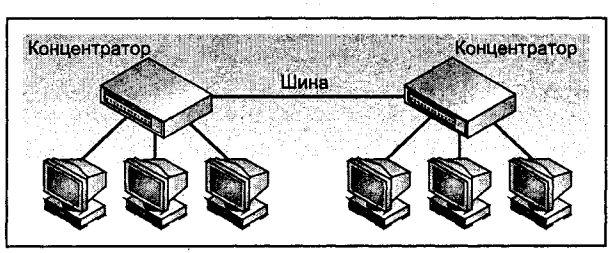


Рис. 2.4. Топология типа "Звезда — Шина"

Иерархическая звездообразная топология

Для увеличения производительности звездообразной компьютерной сети сверх тех возможностей, которые дает ее изначальный концентратор, можно воспользоваться иерархической звездообразной топологией (рис. 2.5), также называемой "разветвленной компьютерной сетью". Для расширения звездообразной сети ее концентратор подключается ко второму концентратору посредством стандартного кабеля, присоединенного к специально предназначенному для этого порту, называемому "связным" (uplink port), при этом трафик, поступающий на любой из этих концентраторов, передается и на другой концентратор, а также на присоединенные к нему компьютеры. Количество концентраторов, которое может поддерживать одна сеть, определяется используемым в ней протоколом. Например, компьютерные сети типа Fast Ethernet обычно могут поддерживать только два концентратора.

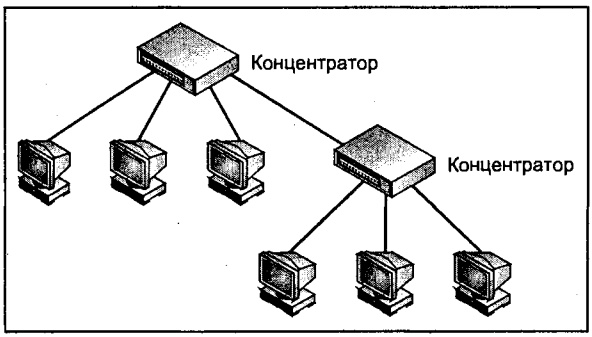


Рис. 2.5. Иерархическая звездообразная топология

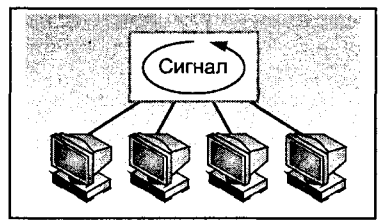


Рис. 2.6. Кольцеобразная топология

Топология типа "Кольцо"

Топология типа "Кольцо" похожа на шинную топологию тем, что каждый компьютер в ней соединен с другим компьютером. Однако концы шины не заделываются резисторами, а связываются друг с другом, образуя кольцо (рис. 2.6). При такой топологии сигналы перемещаются по кольцу от одного компьютера к другому и, в конце концов, возвращаются в исходную точку. В большинстве случаев кольцеобразная топология в строгом смысле реализуется логически, а не физически, поскольку кабели подводятся к концентратору и принимают форму звезды. В кольцеобразной топологии можно использовать несколько разных типов кабеля. В сетях с FDDI-интерфейсом применяется оптоволоконный кабель, а в сетях на основе маркерного кольца (token ring networks) — кабель на основе витой пары.

В компьютерных сетях типа Token Ring используется особый тип концентратора, называемый модулем множественного доступа (Multistation Access Unit, MAU). MAU-модуль принимает каждый входящий сигнал через один порт и передает его последовательно через все остальные порты. Этот процесс является не одновременным, как в концентраторе сети Ethernet, а последовательным. Например, когда компьютер, подключенный к порту 7 в 16-портовом MAU-модуле, передает пакет данных, MAU-модуль принимает этот пакет, а затем передает его только на порт 8. Когда компьютер, подключенный к порту 8, получает этот пакет данных, он сразу же возвращает его в MAU-модуль, который затем передает его на порт 9, и т. д. MAU-модуль продолжает этот процесс до тех пор, пока он не передаст пакет данных на каждый компьютер, входящий в данную сеть. Когда ПК, отправивший этот пакет, получает его обратно, он должен вывести его из кольца.

Структура этой топологии позволяет компьютерной сети сохранять свою работоспособность, даже если какой-то кабель или коннектор выходит из строя, поскольку MAU-модуль содержит специальную схему, которая исключает неисправный ПК из кольца. MAU-модуль в этом случае сохраняет логическую топологию, и компьютерная сеть продолжает функционировать без участия неисправной рабочей станции.

Топология типа "Решетка"

Применение топологии типа "Решетка" в локальной сети, по крайней мере, нерационально. При такой топологии каждый компьютер имеет выделенное соединение

с каждым другим компьютером, входящим в локальную сеть. Эта топология полезна только в том случае, когда сеть является двухузловой. Для построения решетчатой сети, объединяющей три или более компьютеров, потребовалось бы, чтобы каждый ПК имел отдельную сетевую плату для каждого другого компьютера. Например, в семиузловой решетчатой сети каждый компьютер должен был бы иметь по шесть сетевых плат. Хотя такая топология является непрактичной для ЛС, она обладает превосходной отказоустойчивостью. Повреждение сети в одной из точек может нарушить работу только одного компьютера, но не всей сети целиком.

Применение решетчатой топологии становится полезным в компьютерных сетевых комплексах. Существование множества маршрутов, связывающих любые две точки, позволяет применять резервные маршрутизаторы (рис. 2.7). Такая топология часто встречается в больших компьютерных сетях, т. к. она делает сети более устойчивыми к возможным отказам, вызванным неисправностями кабелей, концентраторов и маршрутизаторов.

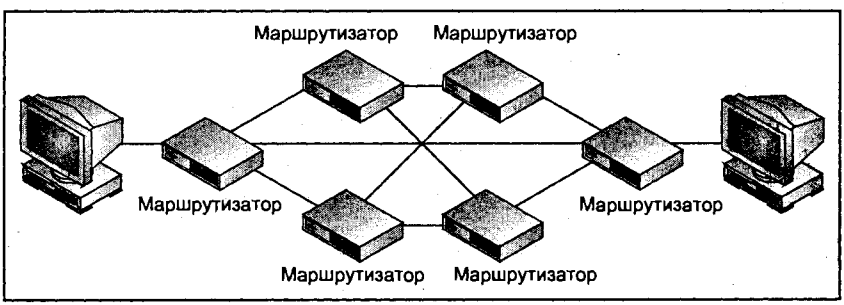


Рис. 2.7. Решетчатая топология

Беспроводная топология

Хотя термин "топология" обычно относится к схеме расположения кабелей в компьютерной сети, он означает не только это. В беспроводных сетях используются так называемые нестационарные средства в виде радио или световых волн, образующих особые схемы, посредством которых компьютеры могут взаимодействовать между собой. Есть два основных вида беспроводной топологии: инфраструктурная топология и специальная топология. Инфраструктурная топология состоит из компьютеров, оснащенных устройствами беспроводной связи и способных взаимодействовать с компьютерной сетью через беспроводные приемопередатчики (называемые точками доступа к сети, network access points), которые, в свою очередь, подключены к сети через стандартный кабель (рис. 2.8). В этой топологии компьютеры взаимодействуют не между собой, а с кабельной компьютерной сетью посредством беспроводных приемопередатчиков. Эта топология наиболее подходит для больших компьютерных сетей, содержащих всего несколько компьютеров с беспроводной связью, которым не нужно взаимодействовать с другими компьютерами, например, это может быть портативный компьютер торгового курьера. Как правило, таким пользователям не требуется обращаться к другим рабочим станциям сети, и они в основном пользуются беспроводным каналом связи для обращения к серверам и ресурсам компьютерной сети.

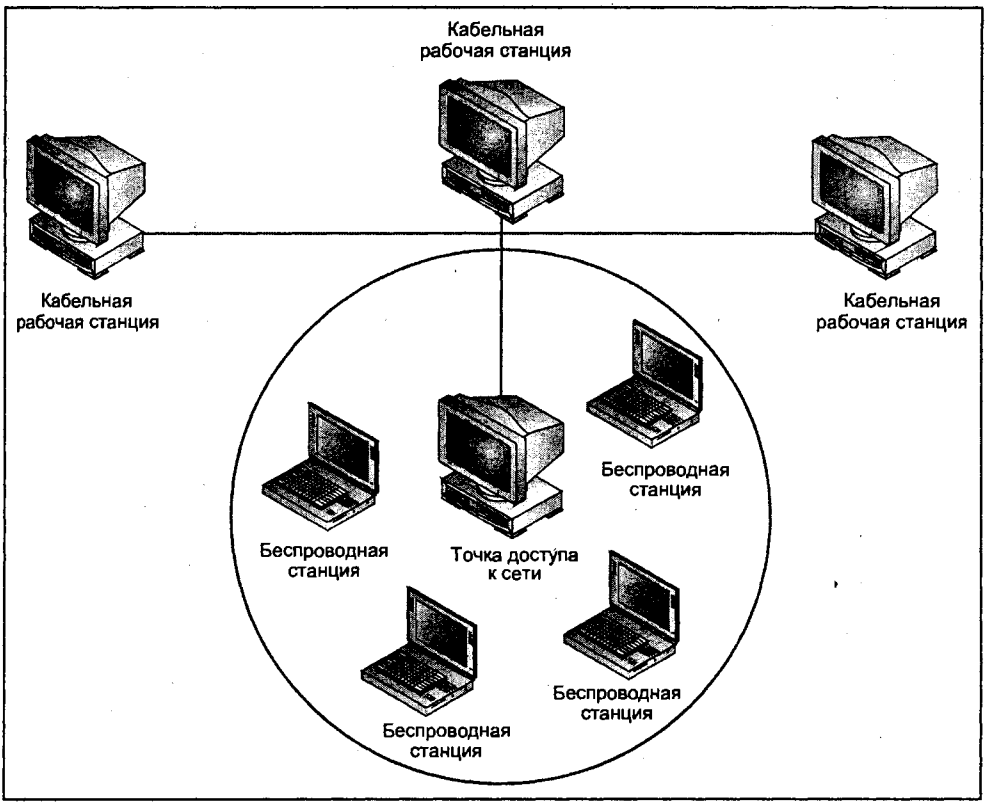


Рис. 2.8. Беспроводная топология

Специальная топология состоит из группы компьютеров, каждый из которых оснащён беспроводной сетевой платой и способен взаимодействовать с другими компьютерами. Недостатком этих двух видов беспроводной топологии является то, что компьютеры должны оставаться в пределах области действия такой топологии. Специальный вид беспроводной топологии наиболее подходит для домашних и небольших офисных компьютерных сетей, в которых использование кабелей может быть нерациональным.

Основы кабельных систем

На заре появления компьютерных сетей существовали проблемы совместимости между сетевыми продуктами разных производителей. Для решения этих проблем все согласились с необходимостью разработки стандарта для кабельных систем, которые могли бы использоваться в ряде различных сетевых технологий. Три организации объединились для решения этого вопроса: Американский национальный институт стандартизации (American National Standards Institute, ANSI), Ассоциация электронной промышленности (Electronic Industry Association, EIA) и Ассоциация телекоммуникационной промышленности (Telecommunications Industry Association, TIA), а

также группа телекоммуникационных компаний разработала "Стандарт телекоммуникационных кабельных систем коммерческих зданий ANSI/EIA/TIA-568-1991 (ANSI/EIA/TIA-568-1991 Commercial Building Telecommunications Cabling Standard). После нескольких редакций этот документ получил другое наименование — ANSI/TIA/EIA/-568-A, и в своей последней версии вышел в марте 2002 года (ANSI/TIA/EIA/-568-B). Стандарт номер 568 определяет требования для кабельных систем, устанавливаемых в США. Для кабельных систем, устанавливаемых в Европе, применяется отдельный стандарт, который был основан на стандарте номер 568 и разработан Международной организацией по стандартизации, получив наименование ISO 11801 1995.

Стандарт номер 568 определяет требования как для речевых кабельных систем, так и для кабельных систем передачи данных, которые совместимы с продуктами различных производителей и срок службы которых составляет не менее 10 лет. В частности, данный стандарт определяет требования по установке кабеля внутри здания, основные требования по топологии и по длине кабельных сегментов, требования для кабельных разъемов, характеристики кабелей, а также критерии, устанавливающие рабочие характеристики для каждого типа кабеля. Упоминаются следующие типы кабелей:

- одномодовое оптоволокно;
- многомодовое оптоволокно;
- неэкранированная витая пара;
- экранированная витая пара.

Кроме того, компания, занимающаяся установкой кабельных систем в зданиях, должна знать и несколько других стандартов:

- TIA/EIA-569 Commercial Building Standard for Telecommunications Pathways and Spaces — Стандарт прокладки телекоммуникационных каналов коммерческих зданий;
- TIA/EIA-606 Administration Standard for the Telecommunications Infrastructure of Commercial Building — Стандарт администрирования телекоммуникационной инфраструктуры коммерческих зданий;
- TIA/EIA-607 Grounding and Bonding Requirements for Telecommunications in Commercial Building — Требования по заземлению и электрическим соединениям телекоммуникационных систем коммерческих зданий.

Типы кабелей

Как уже говорилось выше, протоколы канального уровня связаны с соответствующими типами кабеля. Эти протоколы устанавливают, в том числе, и максимальную длину кабельного сегмента. При определении протокола, наиболее подходящего для вашей компьютерной сети, следует учитывать, какой соответствующий тип кабеля должен быть использован и насколько он подходит для того места, в котором вы строите сеть. Кроме того, необходимо учитывать стоимость этого типа кабеля и связанных с ним компонентов — сетевых плат, коннекторов, а также требуемый объем работ по установке всех этих компонентов. Также следует определить, какой сорт кабеля данного типа наиболее подходит для выбранного вами места. Сорт кабеля зависит от таких параметров, как категория, наличие экранировки и толщина про-

водника. При определении сорта кабеля для использования в компьютерной сети следует учитывать, что все облицовочные панели стен, коммутационные панели и коннекторы должны иметь ту же категорию, что и данный сорт кабеля, для того чтобы обеспечить более надежную сетевую среду.

Есть три основных типа кабеля: коаксиальный кабель, кабель на основе витой пары и оптоволоконный кабель. Коаксиальный кабель и кабель на основе витой пары переносят электрические сигналы и содержат медный проводник. Оптоволоконный кабель переносит световые сигналы и состоит из стеклянного и пластмассового волокна.

Коаксиальный кабель

Коаксиальный (соосный) кабель содержит внутри своей оболочки два проводника. В большинстве двухпроводниковых электрических кабелей проводники расположены рядом друг с другом внутри изолирующей оболочки, которая разделяет и защищает их. В отличие от них, коаксиальный кабель имеет круглую форму, и в нем один проводник расположен внутри другого (рис. 2.9). Первый проводник, находящийся в центре кабеля, представляет собой медный провод, который и переносит электрические сигналы. Провод может быть цельномедным или состоять из нескольких медных жил. Медный сердечник коаксиального кабеля окружен слоем диэлектрического пенного изолятора, предназначенного для того, чтобы защитить сердечник кабеля от второго проводника, который, как правило, представляет собой медную оплетку и действует в качестве "земли". Вся эта конструкция покрывается изолирующей оболочкой, сделанной из поливинилхлорида или тефлона.

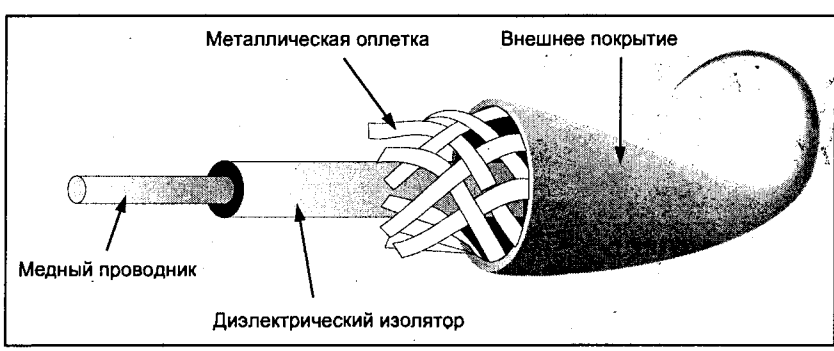


Рис. 2.9. Коаксиальный кабель

Здесь важно отметить, что внешняя изолирующая оболочка кабеля состоит из нескольких разных материалов, поэтому следует убедиться в том, что изоляция вашего кабеля подходит для того типа кабельной системы, которую вы хотите установить. Например, если вы хотите провести кабель через вентиляционную систему вашего здания, тогда этот кабель должен быть сделан из материала, который при горении не выделяет токсичный газ. Такой кабель, конечно, имеет более высокую стоимость, чем стандартный кабель с поливинилхлоридной оболочкой, однако его использование обязательно, если вы прокладываете кабель через вентиляционную систему здания.

В табл. 2.1 приводятся типы коаксиального кабеля и их характеристики. В компьютерных сетях используется два типа коаксиального кабеля: RG-58, известный под названием Thin Ethernet (или 10Base2), и RG-8, известный под названием Thick Ethernet (или 10Base5). Обозначения 10Base2 и 10Base5, используемые для этих типов электрического кабеля, показывают, что скорость передачи данных по этим кабелям ограничена 10 Мбит/с, что данные в них передаются без модуляции сигнала и что максимальная длина кабельного сегмента не может превышать приблизительно 200 и 500 м, соответственно.

Таблица 2.1. *Рабочие характеристики коаксиальных кабелей*

	RG-8/U	RG-58/U или RG-58A/U	RG-62A/U	RG-59/U
Диаметр	0,405 дюйма	0,195 дюйма	0,242 дюйма	0,242 дюйма
Импеданс	50 Ом	50 Ом	93 Ом	75 Ом
Затухание (дБ/100', частота 100 МГц)	1,9	4,5	2,7	3,4
Тип коннекторов	N	BNC	BNC	F
Поддерживаемые протоколы	Thick Ethernet	Thin Ethernet	ARCnet	Кабельное телевидение (CATV)

Оба этих типа коаксиального кабеля используются в сочетании с шинной топологией. Как видно из табл. 2.1, кабели отличаются друг от друга главным образом по толщине и по типу коннекторов. В кабеле RG-8 используются N-коннекторы (рис. 2.10), а в кабеле RG-58 — байонетные коннекторы Нейла-Конселмана (bayonet-Neill-Concelman, BNC) (рис. 2.11).

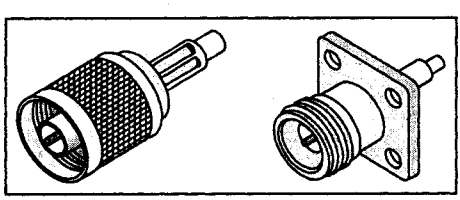


Рис. 2.10. N-коннекторы, применяемые в кабеле RG-8 (Thick Ethernet)

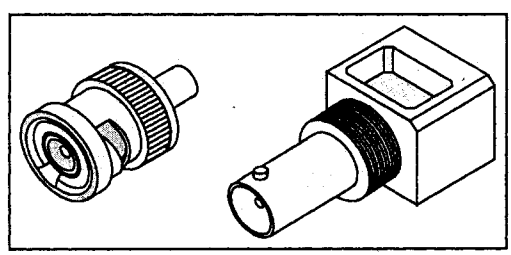


Рис. 2.11. BNC-коннекторы, применяемые в кабеле RG-58 (Thin Ethernet)

Коаксиальный кабель неэффективен для передачи данных, особенно в корпоративной среде, поскольку его пропускная способность ограничена 10 Мбит/с. Хотя этот тип кабеля сегодня еще используется для многих целей, в том числе для сетей кабельного телевидения, в компьютерных сетях он редко находит применение и не подходит для большинства новых Ethernet-сетей.

Кабель на основе витой пары

В настоящее время наиболее распространенным типом электрического кабеля, встречающимся в локальных компьютерных сетях звездообразной топологии, является кабель на основе витой пары. Есть два типа электрических кабелей на основе витой пары: неэкранированная витая пара, которая широко используется в большинстве новых локальных компьютерных сетей, и экранированная витая пара, которая используется в тех случаях, когда кабельная система подвержена электромагнитным помехам. Кабель на основе витой пары содержит восемь изолированных медных проводников в виде проволоки. Эти восемь жил составляют четыре витых пары, и каждая пара имеет свое цветовое обозначение в соответствии со стандартом номер 568 (табл. 2.2). Провода в витых парах скручены в разной степени для того, чтобы избежать перекрестных помех (паразитная передача сигнала от одного проводника к другому), а также для того, чтобы защитить сигнал от помех, вызванных внешними источниками. И наконец, эти четыре пары проводников покрыты общей экранировкой. На рис. 2.12 показано поперечное сечение кабеля на основе витой пары.

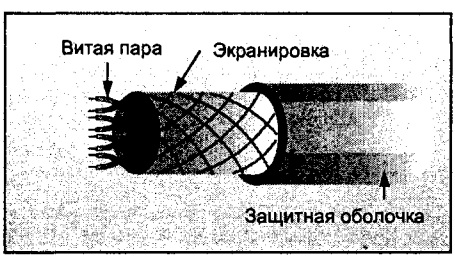


Рис. 2.12. Кабель на основе витой пары

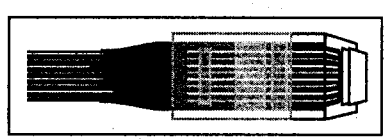


Рис. 2.13. Коннектор RJ-45

Таблица 2.2. *Цветовое кодирование электрических кабелей на основе витой пары*

Пара	Цвет
Пара 1	Сплошной синий и белый с синей полосой
Пара 2	Сплошной оранжевый и белый с оранжевой полосой
Пара 3	Сплошной зеленый и белый с зеленой полосой
Пара 4	Сплошной коричневый и белый с коричневой полосой

Примечание. Жила со сплошным цветом несет сигнал, а белая жила с цветной полосой — "земля".

Коннектор в кабеле на основе витой пары может показаться знакомым, т. к. модульный коннектор RJ-45 очень похож на коннектор RJ-11, который уже не один год используется в стандартных телефонных кабелях (RJ — это аббревиатура от англ. registered jack — зафиксированное гнездо коннектора). Различие между ними состоит в том, что коннектор RJ-45 имеет восемь электрических контактов (рис. 2.13), а коннектор RJ-11 — четыре или шесть контактов. Стандарт TIA/EIA-568-A определя-

ет схему расположения контактов (рис. 2.14) в кабельном коннекторе RJ-45 для кабеля на основе витой пары.

Кабель на основе витой пары имеет преимущества по сравнению с коаксиальным кабелем. Многие фирмы-подрядчики уже знакомы с процедурой установки кабеля на основе витой пары, т. к. этот тип кабеля многие годы используется в телефонии. Это обстоятельство позволяет фирмам-подрядчикам заниматься установкой как телефонного кабеля, так и кабеля для компьютерных сетей. Другим преимуществом электрического кабеля на основе витой пары является то, что он намного более гибок, чем коаксиальный кабель, что делает его более простым в установке.

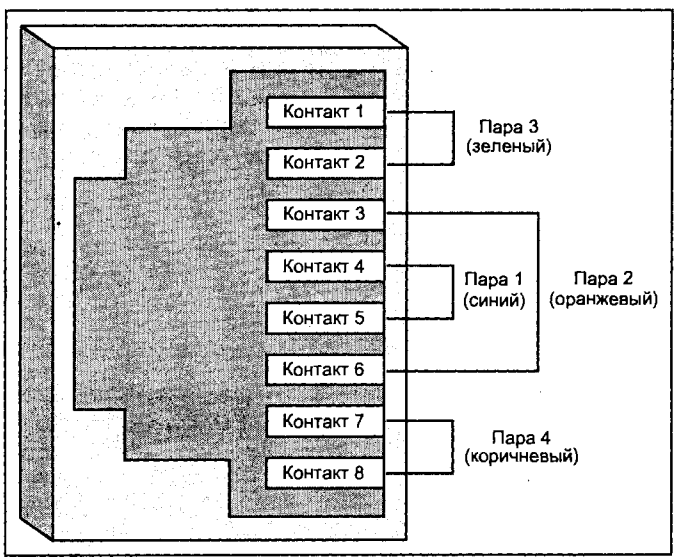


Рис. 2.14. Схема разводки в коннекторе для кабеля на основе витой пары (стандарт 568A)

Кабель на основе неэкранированной витой пары

Ассоциация телекоммуникационной промышленности (TIA) и Ассоциация электронной промышленности (EIA) разработали стандарт TIA/EIA-568, который определяет различные сорта (категории) кабеля на основе неэкранированной витой пары (Unshielded Twisted Pair, UTP). Чем выше категория кабеля, тем более он эффективен для передачи данных и тем выше его пропускная способность. Различие между категориями состоит в степени скрученности каждой пары проводников в кабеле. В Ethernet-сетях, за исключением протоколов 100BaseT4 и 100BaseVG-AnyLAN, как правило, используются только две из четырех пар проводников в UTP-кабеле — одна пара для приема данных, а другая — для передачи. Даже если не все пары задействованы, оставшиеся две пары не могут быть использованы для каких-то других целей, например, телефонной связи. Передача сигналов по двум неиспользованным парам проводников, вероятнее всего, приведет к увеличению перекрестных помех, что значительно увеличивает риск потери данных и искажения сигнала.

Для локальных компьютерных сетей, прежде всего, используются электрические кабели на основе неэкранированной витой пары категории 3 и категории 5 (также

называемой Cat5). В самых современных кабельных системах, применяемых для сетей, используются кабели не ниже 5 категории. UTP-кабель категории 3, как правило, не применяется для сетей типа Fast Ethernet, но подходит для Ethernet-сетей, работающих со скоростью 10 Мбит/с (спецификация 10BaseT). Протокол сетей типа Fast Ethernet по спецификации 100BaseT4 является исключением, т. к. в нем используется UTP-кабель категории 3, рассчитанный для работы на скорости 100 Мбит/с. Однако этот протокол может работать и на большей скорости, т. к. в спецификации 100BaseT4 используются все четыре пары жил кабеля вместо обычных двух. В табл. 2.3 приведены категории кабеля на основе витой пары.

UTP-кабель категории 5 подходит для Ethernet-сетей, работающих со скоростью 100 Мбит/с, а также для более медленных протоколов. UTP-кабель категории 5 также может работать по спецификации 1000BaseT, при условии что он отвечает требованиям стандарта TIA/EIA TSB-95. Стандарт для UTP-кабелей категории 5е устанавливает более высокие рабочие характеристики при использовании в сетях спецификации 1000BaseT (также называемой Gigabit Ethernet). Этот стандарт определяет использование сегментов UTP-кабеля на основе витой пары длиной 100 м и применение сигнала с частотой 100 МГц.

Таблица 2.3. *Категории кабеля на основе неэкранированной витой пары (стандарт TIA/EIA)*

Категория	Частота	Применение
1	= 100 кГц	Только речевые телефонные линии и системы сигнализации. Для передачи данных по компьютерным сетям не предназначена
2	< 4 МГц	Речевые телефонные линии, а также линии связи с терминалами ввода/вывода компании IBM в больших ЭВМ и мини-компьютерах, вычислительные сети с присоединенными ресурсами (ARCnet) и кабельные системы сети AppleTalk (LocalTalk)
3	до 16 МГц	Речевые телефонные линии, сети Ethernet со скоростью передачи 10 Мбит/с (спецификация 10BaseT), кольцевые сети на основе маркерного кольца со скоростью 4 Мбит/с, спецификация 100BaseT4 (Fast Ethernet) и спецификация 100BaseVG-AnyLAN (в этих двух спецификациях задействуются все четыре пары проводников вместо обычных двух). Также может использоваться в телекоммуникационных сетях
4	до 20 МГц	Сети на основе маркерного кольца со скоростью 16 Мбит/с. Может использоваться в сетях передачи данных
5	до 100 МГц (также может использоваться по спецификации 1000BaseT при условии соответствия стандарту TIA/EIA TSB-95)	Спецификация 100BaseTX (Fast Ethernet), синхронные оптические сети (SONET), сети с асинхронным режимом передачи данных (ATM) по оптическим носителям (OC-3). Может использоваться в телекоммуникационных сетях

Таблица 2.3 (окончание)

Категория	Частота	Применение
5e	до 100 МГц	Спецификация 1000BaseT (Gigabit Ethernet). Может использоваться в телекоммуникационных сетях

Кабель на основе экранированной витой пары

Компания IBM разработала сетевой протокол с маркерным доступом (Token Ring), в котором используется кабель на основе экранированной витой пары (Shielded Twisted Pair, STP), а также создала стандарты для различных типов этого кабеля (табл. 2.4). (В стандарте TIA/EIA-T568-A упомянуты только два из этих типов: 1A и 6A.) Кабель на основе экранированной витой пары (STP-кабель) до сих пор используется в основном в локальных сетях типа Token Ring, а также в кабельных системах, требующих дополнительного экранирования для защиты от электромагнитных помех, создаваемых находящимся поблизости электрическим оборудованием. STP-кабель по своей конструкции отличается от UTP-кабеля — в нем только две витых пары, каждую из которых окружает дополнительный слой фольги или оплетки. Дополнительный металлический экран также служит проводником, как и медный провод в витых парах. Если он хорошо заземлен, окружающий электромагнитный шум преобразуется в ток, который, в свою очередь, воздействует на расположенные внутри экрана провода. Поле тока экрана создает в витых парах равный по силе, но протекающий в противоположном направлении ток. В результате, оба тока компенсируют друг друга, тем самым устраняя искажающее влияние окружающего шума на сигналы, передаваемые по проводникам.

Таблица 2.4. Типы кабеля на основе экранированной витой пары

Тип кабеля	Проводники	Материал внешней оболочки
1A	Две пары одножильных проводов калибра 22 с фольговым экраном, а также с экранирующим слоем (фольговым или оплеточным) вокруг каждой пары. Применяется в магистральных линиях и горизонтальных защитных линиях	Поливинилхлорид или материал, подходящий для использования в вентиляционной системе
2A	Две пары одножильных проводов калибра 22 с фольговым экраном, а также с экранирующим слоем (фольговым или оплеточным) вокруг каждой пары, плюс четыре дополнительных пары одножильных проводов калибра 22, используемых для передачи речевых сигналов	Поливинилхлорид или материал, подходящий для использования в вентиляционной системе
6A	Две пары многожильных проводов калибра 26 с фольговым или сетчатым экраном вокруг каждой пары. Применяется во фрагментных кабелях (patch cables)	Поливинилхлорид или материал, подходящий для использования в вентиляционной системе

Таблица 2.4 (окончание)

Тип кабеля	Проводники	Материал внешней оболочки
9A	Две пары многожильных проводов калибра 26 с фольговым или сетчатым экраном вокруг каждой пары	Поливинилхлорид или материал, подходящий для использования в вентиляционной системе

Оптоволоконный кабель

Оптоволоконный кабель (fiber-optic cable) состоит из прозрачного стеклянного или пластикового сердечника, способного переносить световые импульсы. Сердечник окружен отражающим слоем (cladding). Отражающий слой, в свою очередь, покрыт буферным слоем из пластика. Далее следует защитный слой из переплетенных между собой волокон фирмы Kevlar. Наконец, все это покрыто наружной оболочкой из тефлона или поливинилхлорида (рис. 2.15).

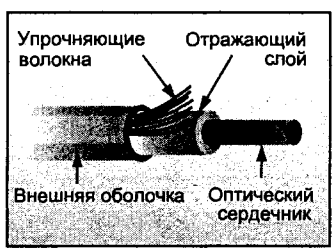


Рис. 2.15. Оптоволоконный кабель

Оптоволоконный кабель представляет собой такой тип кабеля, который совершенно отличается от коаксиального кабеля или кабеля на основе витой пары. В отличие от медных проводников, по которым сигналы передаются в виде электрических импульсов, оптоволоконный кабель переносит по стеклянному или пластиковому волокну импульсы света (фотоны), посредством которых передаются двоичные сигналы, генерируемые компьютером. Так как для передачи сигналов по оптоволоконному кабелю используется свет вместо электричества, кабель устойчив как к электромагнитным, так и к перекрестным помехам. Кроме того, в оптоволоконном кабеле уровень затухания сигнала (его ослабление по мере прохождения по проводнику) ниже, чем в медном кабеле. В некоторых видах оптоволоконного кабеля сигнал может без существенного ослабления проходить расстояние до 120 км, тогда как в традиционном медном кабеле сигнал становится уже практически нечитаемым при прохождении расстояния от 100 до 500 м в зависимости от типа кабеля. Поэтому оптоволоконный кабель является наилучшим средством передачи в тех случаях, когда необходимо установить связь между зданиями или когда сигнал нужно передать на большое расстояние. Дополнительным преимуществом оптоволоконного кабеля является то, что он дает большую степень безопасности, чем медный кабель, т. к. несанкционированное подключение к нему приводит к нарушению связи.

Существует два основных типа оптоволоконного кабеля: одномодовый и многомодовый. Главное различие между этими двумя типами состоит в толщине сердечника

и его отражающей оболочки. Определить тип оптоволоконного кабеля можно по размеру оптического волокна (общей толщине сердечника и отражающей оболочки). В одномодовом волокне обычно диаметр сердечника составляет 8,3 микрона, а общая толщина сердечника и отражающей оболочки — 125 микрон, поэтому одномодовый кабель обычно обозначают как "одномодовое волокно 8,3/125". В отличие от него, многомодовое волокно имеет сердечник диаметром 62,5 микрон, а общая толщина сердечника и отражающей оболочки — 125 микрон, поэтому многомодовое волокно обозначают как "многомодовое волокно 62,5/125".

Для передачи сигнала по одномодовому волокну в качестве источника света используется лазер, работающий на одной длине волны. В отличие от него в многомодовом волокне используется светоизлучающий диод (СИД) и оно может переносить сигналы на разной длине волны. Так как для передачи сигнала по одномодовому волокну используется одноволновый лазер, это волокно способно передавать сигналы на очень большие расстояния, и поэтому оно обычно используется для наружных кабельных линий (например, сетей кабельного телевидения). Этот тип кабеля значительно дороже, чем многомодовый, и имеет больший радиус изгиба, поэтому он не очень подходит для кабельных систем компьютерных сетей. Многомодовый кабель, наоборот, больше подходит для локальных сетей, т. к., хотя он и не может использоваться на таких больших расстояниях, как одномодовый, его стоимость не так высока, и он допускает большие изгибы. Для оптоволоконного кабеля чаще всего используют два типа коннекторов: коннектор типа SC (Subscriber Connector) и коннектор типа ST (Straight Tip connector) (рис. 2.16).

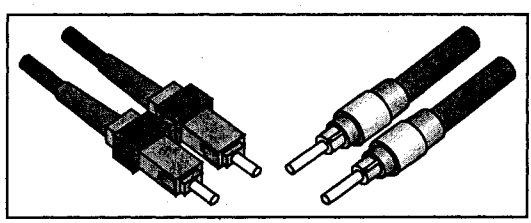


Рис. 2.16. Коннекторы оптоволоконных кабелей

Протоколы канального уровня

Протокол канального уровня (data link layer protocol) обеспечивает в компьютере связь между физическим уровнем и стеком протоколов (protocol stack). Как правило, он состоит из трех элементов:

- формата для кадра;
- механизма регуляции доступа к разделяемой сети;
- нормативов физического уровня сети.

Протокол Ethernet

Говоря о локальных сетях, главным образом имеют в виду сети типа Ethernet. Со времени своего создания стандарт Ethernet уже изменялся несколько раз в соответ-

ствии с новыми требованиями рынка. Ранние версии компьютерных сетей типа Ethernet работали со скоростью 10 Мбит/с. Сегодня же такие сети работают на скоростях 100 Мбит/с, 1000 Мбит/с и даже 10 Гбит/с, что позволяет их использовать как в качестве самых небольших домашних компьютерных сетей, так и в качестве магистральных сетей с высокой пропускной способностью.

Основные сведения о стандарте Ethernet

Стандарт Ethernet впервые был разработан в 1970-х годах и впоследствии стал известен под названием Thick ("толстый") Ethernet из-за размера используемого в нем кабеля (около 1 см в диаметре). Первый из двух стандартов был впервые опубликован в 1980 году под названием "Локальная компьютерная сеть типа Ethernet: спецификации канального и физического уровней" ("The Ethernet: a Local Area Network: Data Link Layer and Physical Layer Specifications"). Он был разработан компаниями Digital Equipment Corporation, Intel и Xerox и стал известен как стандарт DIX Ethernet. В этом стандарте описывалась компьютерная сеть, построенная по шинной топологии с использованием коаксиального кабеля RG-8 и работающая со скоростью 10 Мбит/с. Такая компьютерная сеть стала называться Thick ("толстый") Ethernet, thicknet или 10Base5. В 1982 году этот стандарт обновили, и он стал называться DIX Ethernet II. В обновленном стандарте к протоколу был добавлен второй физический уровень на основе более тонкого коаксиального кабеля типа RG-58, и такая компьютерная сеть стала называться "тонкий" Ethernet, thinnet или 10Base5.

В то же время, международная организация по разработке стандартов, Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers, IEEE), начала работу по созданию международного стандарта для компьютерных сетей общего пользования, схожих с Ethernet-сетями. Для этого организация IEEE создала рабочую группу под названием IEEE 802.3. Компания Xerox сделала название Ethernet своей собственной торговой маркой, поэтому рабочая группа не могла назвать свою компьютерную сеть Ethernet. В результате, в 1985 году был опубликован следующий документ: "Метод множественного доступа с контролем несущей и обнаружением коллизий и спецификации физического уровня" ("IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications"). В дополнение к двум возможностям использования коаксиального кабеля, имеющимся в стандарте DIX Ethernet, рабочая группа IEEE 802.3 ввела стандарт для кабеля на основе неэкранированной витой пары, известный как спецификация 10BaseT. Кроме того, в 1995 году рабочая группа IEEE 802.3 опубликовала дополнительные документы: "IEEE 802.3u", в которых определяется спецификация компьютерной сети Fast Ethernet, работающая со скоростью 100 Мбит/с, а также "IEEE 802.3z" и "IEEE 802.ab", в которых описаны стандарты для сетей типа Gigabit Ethernet, работающих со скоростью 1000 Мбит/с.

Основное отличие стандарта IEEE 802.3 от стандарта DIX Ethernet заключается в том, что в нем появились дополнительные возможности физического уровня, упомянутые выше, а также некоторые изменения в формате кадра. Несмотря на то, что название Ethernet продолжает использоваться для обозначения этого стандарта, на самом деле в современных компьютерных сетях применяется именно протокол IEEE 802.3, т. к. в нем имеется дополнительный физический уровень, а также описаны стандарты для сетей типа Fast Ethernet и Gigabit Ethernet. Единственный элемент стандарта DIX Ethernet, который продолжает сегодня использоваться, — это

формат кадра из Ethernet II. В этом формате имеется поле, обозначающее, в каком протоколе сетевого уровня были созданы данные, содержащиеся в каждом пакете. В табл. 2.5 приводятся основные различия между стандартом DIX Ethernet II и стандартом IEEE 802.3.

Оба этих стандарта состоят из следующих компонентов:

- спецификации физического уровня, в которых определяются ограничения по прокладке кабеля, тип кабеля и методы передачи служебных сигналов;
- формата кадра, в котором определяются назначение и порядок битов, передаваемых в пакете;
- механизма управления доступом к передающей среде (Media Access Control), который называется "управлением множественным доступом с контролем несущей и обнаружением коллизий " (CSMA/CD) и который позволяет компьютерам, входящим в компьютерную сеть, получать доступ к сетевой среде.

Таблица 2.5. *Основные различия между стандартом DIX Ethernet II и стандартом IEEE 802.3*

Стандарт	Возможности физического уровня	Биты 13-14 в заголовке кадра	Тип теста внешнего приемопередатчика
DIX Ethernet II	Только коаксиальный кабель	Как в стандарте Ethernet	Выявление конфликтов
IEEE 802.3	Коаксиальный кабель, кабель на основе неэкранированной витой пары, оптоволоконный кабель	Длина поля данных	SQE-тест

Типы стандартов Ethernet и физический уровень

В спецификациях физического уровня, содержащихся в стандарте Ethernet, описаны такие параметры, как топология, максимальная длина кабельного сегмента и типы кабеля, которые можно использовать для построения данной компьютерной сети. Основные спецификации физического уровня сетей типа Ethernet приведены в табл. 2.6. Эти спецификации необходимо соблюдать для того, чтобы избежать таких проблем, как перекрестные помехи и затухание сигнала. Следует также учитывать спецификации производителя при использовании той или иной технологии, т. к. точные значения параметров могут различаться в зависимости от производителя.

Таблица 2.6. *Спецификации стандарта Ethernet*

Обозначение	Скорость	Топология	Тип кабеля	Максимальная длина кабельного сегмента	Тип стандарта
10Base5	10 Мбит/с	Шина	Коаксиальный RG-8	500 м	Ethernet

Таблица 2.6 (продолжение)

Обозначение	Скорость	Топология	Тип кабеля	Максимальная длина кабельного сегмента	Тип стандарта
10Base2	10 Мбит/с	Шина	Коаксиальный RG-58	185 м	Ethernet
10BaseT	10 Мбит/с	Звезда	На основе неэкранированной витой пары, категория 3	100 м	Ethernet
Звено оптоволоконной связи между повторителями (Fiber-Optic Inter-Repeater Link, FOIRL)	10 Мбит/с	Звезда	Многомодовое оптоволокно 62,5/125	1000 м	Ethernet
10BaseFL	10 Мбит/с	Звезда	Многомодовое оптоволокно 62,5/125	2000 м	Ethernet
10BaseFB	10 Мбит/с	Звезда	Многомодовое оптоволокно 62,5/125	2000 м	Ethernet
10BaseFP	10 Мбит/с	Звезда	Многомодовое оптоволокно 62,5/125	500 м	Ethernet
100BaseTX	100 Мбит/с	Звезда	На основе неэкранированной витой пары, категория 5	100 м	Fast Ethernet
100BaseT4	100 Мбит/с	Звезда	На основе неэкранированной витой пары, категория 3	100 м	Fast Ethernet
100BaseFX	100 Мбит/с	Звезда	Многомодовое оптоволокно 62,5/125	412 м при полудуплексном канале и/или 2000 м при полнодуплексном канале	Fast Ethernet

Таблица 2.6 (продолжение)

Обозначение	Скорость	Топология	Тип кабеля	Максимальная длина кабельного сегмента	Тип стандарта
1000BaseLX	1000 Мбит/с	Звезда	Одномодовое оптоволокно 9/125	5000 м	Gigabit Ethernet
1000BaseLX	1000 Мбит/с	Звезда	Многомодовое оптоволокно 50/125 или 62,5/125	550 м	Gigabit Ethernet
1000BaseSX	1000 Мбит/с	Звезда	Многомодовое оптоволокно 50/125 (частота 400 МГц)	500 м	Gigabit Ethernet
1000BaseSX	1000 Мбит/с	Звезда	Многомодовое оптоволокно 50/125 (частота 500 МГц)	550 м	Gigabit Ethernet
1000BaseSX	1000 Мбит/с	Звезда	Многомодовое оптоволокно 62,5/125 (частота 160 МГц)	220 м	Gigabit Ethernet
1000BaseSX	1000 Мбит/с	Звезда	Многомодовое оптоволокно 62,5/125 (частота 200 МГц)	275 м	Gigabit Ethernet
1000BaseLH	1000 Мбит/с	Звезда	Одномодовое оптоволокно 9/125	10 км	Gigabit Ethernet
1000BaseZX	1000 Мбит/с	Звезда	Одномодовое оптоволокно 9/125	100 км	Gigabit Ethernet
1000BaseCX	1000 Мбит/с	Звезда	Экранированный медный кабель (сопротивление 150 Ом)	25 м	Gigabit Ethernet

Таблица 2.6 (окончание)

Обозначение	Скорость	Топология	Тип кабеля	Максимальная длина кабельного сегмента	Тип стандарта
1000BaseT	1000 Мбит/с	Звезда	На основе неэкранированной витой пары, категория 5 (или 5E)	100 м	Gigabit Ethernet

Стандарт Ethernet

Стандарт IEEE 802.3 включает в себя четыре спецификации для кабелей, которые приведены в табл. 2.7. Скорость передачи данных в компьютерной сети типа Thick Ethernet ограничивается 10 Мбит/с, поэтому такая сеть непригодна в качестве магистральной среды. Однако она все еще неплохо иллюстрирует те компоненты, которые входят в состав физического уровня Ethernet-сетей.

Таблица 2.7. Спецификации кабелей, используемых в компьютерных сетях типа Ethernet

	Обозначение	Максимальная длина кабельного сегмента	Максимальное количество узлов на кабельный сегмент	Тип кабеля	Тип коннекторов
Thick Ethernet	10Base5	500 м	100	Коаксиальный RG-8	N
Thin Ethernet	10Base2	185 м	30	Коаксиальный RG-58	BNC
Кабель на основе витой пары	10BaseT	100 м	2	На основе неэкранированной витой пары, категория 3	RJ-45
Оптоволоконный	100BaseFL	1000/2000 м	2	Многомодовое оптоволокно 62,5/125	ST

Прежде всего, сегмент коаксиального кабеля более эффективен в работе, если он является цельным, не состоящим из сегментов. Если это невозможно, то лучше всего соединять отрезки из одной бобины или партии. При этом кабель следует составлять из как можно меньшего количества сегментов, используя N-коннекторы на каждом конце кабеля и цилиндрические N-коннекторы между сегментами кабеля.

Если же вы используете кабельные отрезки из разных партий, то их длина должна быть равна 23,4 м, 70,2 м или 117 м. При таких длинах, отражения сигналов будут минимальны. Наконец, следует завершать оба конца шины при помощи сопротивления на 50 Ом, которое встроено в N-оконечную нагрузку, и заземлить только один конец при помощи заземляющего коннектора, подключенного к N-оконечной нагрузке.

Thin ("тонкий") Ethernet отличается от "толстого" только лишь тем, что в нем используется более гибкий и тонкий (5 мм) коаксиальный кабель RG-58. Кроме того, в сетях типа Thin Ethernet используются BNC-коннекторы вместе с Т-образными коннекторами (рис. 2.17). Т-коннектор применяется для подсоединения коаксиального кабеля, с одной стороны, к компьютеру, а с другой — к следующей системе. Кабель Thin Ethernet тоже нужно завершать резистором и заземлять. Для завершения шины два компьютера на обоих концах сети должны иметь оконечную нагрузку с сопротивлением 50 Ом на одном из концов Т-коннектора. Один конец шины (т. е. только один из двух крайних компьютеров) должен быть заземлен.

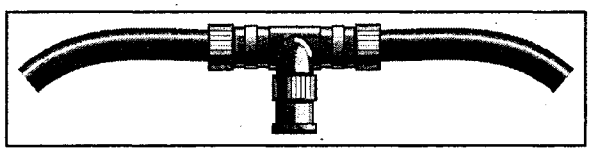


Рис. 2.17. Т-коннектор, используемый в сети типа Thin Ethernet

При использовании в сети Ethernet кабеля на основе витой пары вместо коаксиального кабеля требуется концентратор (в этих условиях он не требуется только в одном случае). При этом концентратор служит в качестве как повторителя сигнала, так и в качестве коммутационного звена. Хотя максимальная длина каждого кабельного сегмента не может быть больше 100 м, при использовании промежуточного концентратора в качестве повторителя сигнала общее расстояние между двумя узлами может быть увеличено до 200 м. Для соединения двух компьютеров без помощи концентратора можно воспользоваться кроссоверным кабелем (crossover cable).

Сети Ethernet с использованием оптоволоконного кабеля работают со скоростью 10 Мбит/с. Сетевая среда в этих сетях строится на основе двухжильного многомодового оптоволоконного кабеля 62,5/125. Одна жила служит для приема сигналов, а другая — для передачи. Для Ethernet-сетей, работающих со скоростью 10 Мбит/с существует два основных стандарта оптоволоконного кабеля: FOIRL и 10BaseF. Стандарт 10BaseF определяет три конфигурации: 10BaseFB, 10BaseFP и 10BaseFL, причем последняя из них — наиболее распространенная. Сейчас, когда существуют протоколы Fast Ethernet и FDDI, тоже работающие с использованием оптоволоконных кабелей, очевидно, что стандарт Ethernet имеет слишком низкую в сравнении с ними пропускную способность.

Стандарт Fast Ethernet

Стандарт Fast Ethernet (IEEE 802.3u) включает в себя две кабельных спецификации: 100BaseTX и 100BaseT4. В обеих сохраняется то же ограничение на длину кабельного отрезка — 100 м. В спецификации 100BaseTX применяется кабель 5 категории. Так как категория 5 является высшей, спецификация 100BaseTX обеспечивает более высокое качество передачи сигнала, чем спецификация 100BaseT4. Так же, как и в

спецификации 10BaseT, в спецификации 100BaseTX используются только две пары проводников кабеля. В спецификации 100BaseT4, как и в старых компьютерных сетях типа Ethernet, применяется кабель 3 категории, что упрощает модернизацию. Кроме того, в этой спецификации используются все четыре пары проводников кабеля для передачи и приема сигналов.

Стандарт Gigabit Ethernet

В стандарте Gigabit Ethernet предусмотрено две спецификации: IEEE 802.3z для оптоволоконного кабеля и IEEE 802.3ab для кабеля на основе витой пары с использованием стандарта 1000BaseT. В стандарте 1000BaseT используется кабель категории 5 или 5E (Enhanced Category). Этот стандарт разработан для модернизации существующих сетей на основе стометровых сегментов UTP-кабеля (неэкранированная витая пара). Он обеспечивает более высокую пропускную способность кабеля благодаря тому, что в нем задействованы все четыре пары проводников, а также благодаря использованию особой схемы передачи служебных сигналов — амплитудно-импульсная модуляция-5 (pulse amplitude modulation-5, PAM). Пропускная способность кабелей категории 5 или 5E одинакова (1000 Мбит/с) при условии того, что кабельная система отвечает дополнительным требованиям, изложенным в стандарте TIA/EIA TSB-95. Модернизация кабельной системы категории 5 до уровня категории 5E осуществляется главным образом при помощи усиления защиты против перекрестных помех.

Кадр протокола Ethernet

Данные, полученные от протокола сетевого уровня, протокол Ethernet инкапсулирует в кадры (frames). Кадр представляет собой определенную последовательность битов, которая начинает и завершает каждый пакет передаваемых по кабелю данных. Кадр состоит из заголовка и завершителя. Как заголовок, так и завершитель разделены на поля, которые содержат служебную информацию, необходимую для передачи каждого пакета по месту назначения. Во всех типах стандарта Ethernet (обычный Ethernet, Fast Ethernet и Gigabit Ethernet) используется один и тот же вид кадра (рис. 2.18).

Ethernet-кадр имеет следующие поля.

- Преамбула (7 байт). Поле преамбулы (preamble) состоит из семи байтов чередующихся 0 и 1, которые используются в системах коммуникации для синхронизации, а затем сбрасываются. В кадре протокола DIX Ethernet длина преамбулы составляет 8 байт.
- Начальный ограничитель кадра (1 байт). Поле начального ограничителя кадра (Start of Frame Delimeter, SFD) содержит 6 битов чередующихся 0 и 1, за которыми следуют две единицы подряд, и служит сигналом того, что начинается передача кадра как такового, а также того, что любые последующие данные являются частью пакета данных, который должен быть помещен в буферную память сетевой платы. В отличие от кадра протокола IEEE 802.3, кадр протокола DIX Ethernet не имеет отдельного поля ограничителя. Однако последние два бита заголовка кадра являются последовательностью из двух единиц аналогично ограничителю кадра, что сигнализирует о начале передачи кадра как такового.
- Адрес назначения (6 байт). Поле адреса назначения (Destination Address) содержит 6 байт информации о шестнадцатеричном адресе сетевой платы в той локальной сети, в которую направляется пакет.

- Адрес источника (6 байт). Поле адреса источника (Source Address) содержит 6 байт информации о шестнадцатеричном адресе сетевой платы того компьютера, который отправил пакет.
- Тип протокола или длина поля данных (2 байт). В кадре протокола DIX Ethernet поле типа протокола (Ethertype) указывает код, определяющий протокол сетевого уровня, для которого предназначены данные, содержащиеся в передаваемом пакете. В кадре протокола IEEE 802.3 поле длины (Length) определяет длину поля данных (исключая заполнитель, о котором сказано ниже).
- Данные и заполнение (от 46 до 1500 байт). Поле данных и заполнения (Data and Pad) содержит данные, полученные от протокола сетевого уровня в передающей системе. Эти данные отсылаются для аналогичного протокола в системе назначения. Если данные, полученные от протокола сетевого уровня, имеют слишком маленький размер (менее 46 байт), Ethernet-адаптер добавляет в поле заполнения последовательность незначащих битов, чтобы довести длину поля данных до своего минимального значения (46 байт).
- Контрольная последовательность кадра (4 байт). Поле контрольной последовательности кадра (Frame Check Sequence, FCS) служит в качестве завершителя кадра и содержит 4-байтовое значение контрольной суммы, вычисленной передающим компьютером и помещенной им в это поле. Принимающая система использует это значение для определения правильности передачи пакета данных.

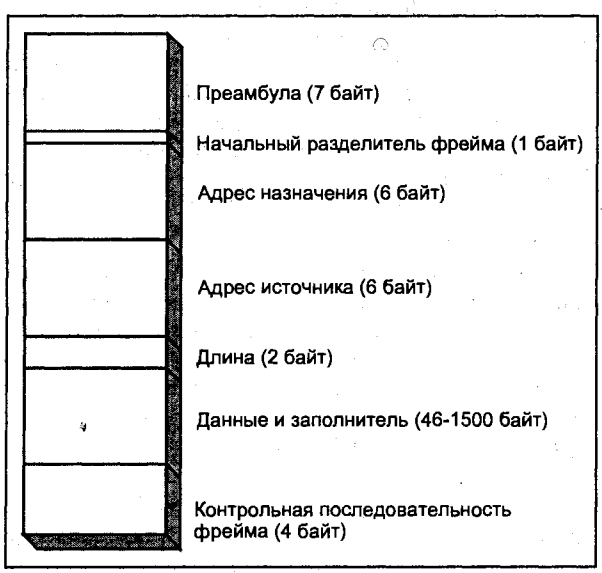


Рис. 2.18. Кадр протокола Ethernet

Механизм CSMA/CD

Механизм управления доступом к передающей среде (Media Access Control, MAC), который называется "управлением множественным доступом с контролем несущей и

обнаружением коллизий" (CSMA/CD), является главным и самым определяющим элементом стандарта Ethernet. Он работает следующим образом. Когда какой-либо компьютер, входящий в компьютерную сеть типа Ethernet, собирается отправить данные, он делает запрос в сеть, чтобы определить, не используется ли она какой-либо другой системой. Эта фаза называется "фазой контроля несущей" (carrier sense phase). Если сеть занята, компьютер ждет некоторое время и затем проверяет состояние сети еще раз. Если компьютер определяет, что сеть свободна, он отправляет пакет данных. Эта фаза называется "фазой множественного доступа" (multiple access phase). Такое название обусловлено тем, что все устройства, входящие в компьютерную сеть, конкурируют за доступ к общей среде передачи.

Хотя фаза контроля несущей как раз и служит в качестве средства защиты против ошибок, конфликты все же могут происходить. Коллизия возникает в том случае, когда две или более систем, входящих в компьютерную сеть, начинают одновременно передавать данные, что приводит к "конфликту" между их сигналами. Также коллизия может возникнуть в том случае, когда сигнал от передающего компьютера еще не достиг принимающего компьютера. Принимающий компьютер, который еще не получил идущий к нему сигнал, может начать передачу своих данных. В результате, два пакета данных смешиваются на каком-то участке кабеля. При возникновении такой коллизии оба пакета сбрасываются, и поэтому обоим компьютерам приходится передавать свои пакеты заново. В сети типа Ethernet подобные конфликты вполне обычны и, как правило, не составляют проблемы, если компьютеры могут выявлять их или если они случаются не слишком часто.

Фаза обнаружения коллизий (collision detection phase) является очень важной, т. к. если компьютеры не могут выявлять возникновение конфликтов, возможно использование искаженных данных. Компьютер может выявлять коллизии сети в процессе передачи данных. Если ПК регистрирует какой-либо скачок напряжения в сети на основе коаксиального кабеля, он считает, что произошла коллизия. Если же в качестве сетевого носителя используется полудуплексная линия с применением оптоволоконного кабеля или кабеля на основе неэкранированной витой пары, то коллизией считается ситуация, когда компьютер регистрирует сигнал одновременно на канале передачи и на канале приема.

Если пакет данных имеет слишком малый размер (менее 64 байт) или если сетевой кабель имеет слишком большую длину, может возникнуть ситуация, когда коллизия случается уже после того, как ПК закончил передачу данных. Когда коллизия возникает после того, как последний бит данных ушел из передающей системы, она называется "запаздывающей" (late collision), и такая ситуация уже не часто встречается в сетях типа Ethernet. Возникновение запаздывающей коллизии указывает на более серьезные проблемы (например, неисправность сетевой платы), требующие немедленного решения.

Если компьютер обнаруживает коллизию, он сразу же останавливает передачу данных и выдает специальную последовательность битов так называемой беспорядочной последовательности (jam pattern). Она служит для предупреждения каждого ПК сети о том, что произошел конфликт и что все компьютеры должны прекратить прием текущих пакетов и не начинать передачу каких-либо данных до тех пор, пока сетевой носитель не освободится. После передачи последовательности компьютер делает на некоторое время паузу, а затем снова пытается передать свои данные. Эта фаза называется "фазой отсрочки" (backoff period). Для того чтобы вычислить продолжительность собственной фазы отсрочки, оба компьютера, вызвавшие коллизию,

используют рандомизированный алгоритм, называемый "усеченным двоичным экспоненциальным алгоритмом вычисления продолжительности фазы отсрочки" (truncated binary exponential backoff). Подобные вычисления необходимы для того, чтобы сделать продолжительность фазы отсрочки разной и тем самым избежать повторного конфликта после выхода из фазы.

Основы Token Ring

Протокол Token Ring, разработанный компанией IBM, является протоколом уровня канала передачи данных и принципиально отличается почти во всех отношениях от протокола Ethernet. В компьютерных сетях на основе маркерного кольца применяется совершенно другая спецификация физического уровня, другой механизм управления доступом к передающей среде (MAC-механизм) и другие форматы кадра. Первоначальный стандарт Token Ring был разработан компанией IBM для собственных нужд. Впоследствии этот протокол был признан Институтом инженеров по электротехнике и электронике (IEEE) в качестве стандарта (стандарт 802.5). Хотя ранние версии компьютерных сетей типа Token Ring работали со скоростью 4 Мбит/с, сегодня почти все системы этого типа работают со скоростью 16 Мбит/с.

Спецификация физического уровня

В компьютерных сетях типа Token Ring изначально использовалась разновидность кабеля на основе экранированной витой пары под названием "кабельная система IBM тип 1" (IBM Type 1 cabling system) со специальными коннекторами для передачи данных IBM Data Connectors (IDC). Эти кабели используются для соединения компьютеров с особым типом концентратора, называемого "модулем множественного доступа" (Multistation Access Unit, MAU). Модуль MAU — это компонент, который логически организует внутри себя кольцеобразную топологию из подключаемых к нему станций, хотя физически эти станции организованы в звездообразную топологию.

Примечание

За более подробными сведениями о звездообразной топологии обращайтесь к *разд. "Топология типа "Звезда".*

Сегодня практически все компьютерные сети типа Token Ring строятся с использованием кабелей на основе неэкранированной витой пары, которые в терминологии, принятой в компании IBM, называются кабелями типа 3 (Type 3 cabling). Однако соединения с модулем MAU в них те же самые. В табл. 2.8 приводится список некоторых требований по использованию кабеля в сетях типа Token Ring.

***Таблица 2.8.** Основные требования по использованию кабеля в компьютерных сетях типа Token Ring*

	Кабель 1-го типа	Кабель 3-го типа
Максимальное количество рабочих станций	260	72
Максимальная длина абонентского кабеля	300 м	150 м

Таблица 2.8 (окончание)

	Кабель 1-го типа	Кабель 3-го типа
Максимальное количество 8-портовых MAU-модулей	32	9
Максимальная длина кольца (при скорости 4 Мбит/с)	360 м	150 м
Максимальная длина кольца (при скорости 16 Мбит/с)	160 м	60 м

Эстафетная передача маркера

Главное различие между компьютерной сетью типа Token Ring и компьютерной сетью типа Ethernet заключается в механизме управления доступом к передающей среде (Media Access Control, MAC). Эстафетная передача маркера в компьютерных сетях типа Token Ring — это такой метод управления доступом к передающей среде, который позволяет устранить конфликты и эффективно управлять большим объемом трафика. В сетях с эстафетной передачей маркера используется специальный кадр — маркер (token). С помощью маркера обозначается тот компьютер, которому в данный момент разрешена передача данных. Маркер циклически передается по компьютерной сети от одного компьютера к другому, и только тот ПК, в котором маркер находится в данный момент, может осуществлять передачу данных. Как только компьютер завершает передачу, он формирует новый маркер и передает его следующему по порядку ПК, входящему в сетевое кольцо. После того, как данные обойдут все сетевое кольцо и будут получены всеми компьютерами, система, отправившая эти данные, должна изъять их из кольца. Так как в каждый момент времени в сети существует только один маркерный кадр, два компьютера не могут передать данные одновременно. В результате, в компьютерной сети типа Token Ring таких конфликтов, как в сети типа Ethernet, не возникает совсем.

Эстафетная передача маркера — это очень эффективный механизм управления доступом к передающей среде, который используется и в некоторых других протоколах, в том числе в протоколе FDDI.

Кадры протокола Token Ring

В компьютерных сетях типа Token Ring используются три разных типа кадра в отличие от компьютерных сетей типа Ethernet, в которых используется только один тип кадра. Как было сказано выше, маркерный кадр служит исключительно для управления доступом к среде передачи и его размер составляет только 3 байта.

Кадр маркера

Формат маркерного кадра (Token Frame) изображен на рис. 2.19. Поля, входящие в маркерный кадр, выполняют следующие функции.

- Начальный ограничитель (1 байт). Поле начального ограничителя (Start Delimiter) служит для обозначения начала кадра.
- Управление доступом (1 байт). Поле управления доступом (Access Control) содержит биты, которые используются для обозначения приоритета передаваемой информации.

- Конечный ограничитель (1 байт). Поле конечного ограничителя (End Delimiter) служит для обозначения конца кадра аналогично полю начального ограничителя.

Рис. 2.19. Кадр маркера

Кадр данных

Кадр данных (Data Frame) в компьютерной сети типа Token Ring служит для передачи прикладных данных, генерируемых компьютерами сети. Этот кадр больше всего похож на тот, что используется в сетях типа Ethernet. Формат кадра показан на рис. 2.20. Поля, входящие в кадр данных, выполняют следующие функции.

- Начальный ограничитель (1 байт). Поле начального ограничителя (Start Delimiter) служит для обозначения начала кадра.
- Управление доступом (1 байт). Поле управления доступом (Access Control) содержит биты, которые используются для обозначения приоритета передаваемой информации.
- Управление кадром (1 байт). Поле управления кадром (Frame Control) служит для сообщения о том, что содержит пакет: данные или команды (command frame).
- Адрес назначения (6 байт). В поле адреса назначения (Destination Address) сообщается аппаратный адрес (hardware address), по которому пакет направлен. Эти стандартные адреса аппаратно "зашиты" в сетевые платы.
- Адрес источника (6 байт). В поле адреса источника (Source Address) сообщается стандартный аппаратный адрес компьютера, отправившего пакет. Этот адрес закодирован в сетевой плате компьютера.
- Информация (до 4500 байт). Поле информации содержит прикладные данные, переданные из протокола сетевого уровня.
- Контрольная последовательность кадра (4 байт). Поле контрольной последовательности кадра (Frame Check Sequence) содержит значение контрольной суммы, которое было определено передающим компьютером. Это значение сравнивается со значением, вычисленным принимающим компьютером, для управления доступом. Если указанные значения не совпадают, пакет информации сбрасывается.
- Конечный ограничитель (1 байт). Поле конечного ограничителя (End Delimiter) служит для обозначения конца кадра аналогично полю начального ограничителя.
- Состояние кадра (1 байт). Поле состояния кадра (Frame Status) содержит информацию о том, смог ли компьютер назначения успешно принять кадр.

Управляющий кадр

В управляющем кадре протокола Token Ring используется тот же формат, что и в кадре данных. Единственное отличие заключается в значении поля управления кадра и содержании поля информации. Управляющие кадры не несут прикладных

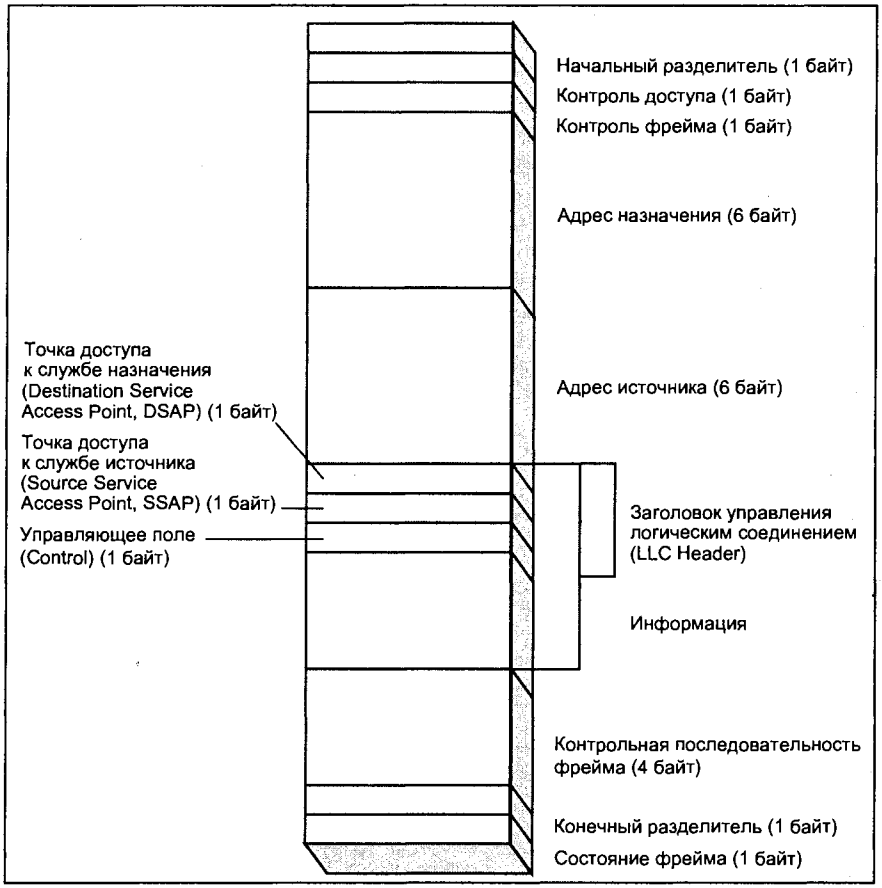


Рис. 2.20. Кадр данных протокола Token Ring

данных и используются только для функций управления, в частности управления кольцом. Они никогда не передаются в другие сегменты сети через такие устройства сопряжения, как мосты, коммутаторы или маршрутизаторы.

Прерывающая последовательность

Прерывающая последовательность (Abort Delimiter Frame) составляет всего 2 байта и содержит в себе только два поля: начальный и конечный ограничители, аналогичные тем, что используются в других типах кадра. Этот кадр применяется только в особых случаях, когда необходимо очистить кольцо от данных, оставшихся после возникновения какой-либо проблемы (например, после незавершенной передачи пакета).

Основы FDDI

Распределенный интерфейс передачи данных по оптоволоконным каналам (Fiber Distributed Data Interface, FDDI) был первым коммерческим протоколом для переда-

чи данных по оптоволоконному каналу со скоростью 100 Мбит/с. Сегодня протокол FDDI используется редко, т. к. он был вытеснен стандартами Fast Ethernet и Gigabit Ethernet с применением оптоволоконных линий, однако в свое время протокол FDDI часто использовался для высокоскоростных сетевых магистралей.

Компьютерные сети типа FDDI, как правило, строятся на основе топологии с двойным кольцом и с использованием многомодового оптоволоконного кабеля типа 62,5/125. В отличие от компьютерных сетей типа Token Ring, сети типа FDDI могут физически строиться по кольцевой топологии, в которой каждый компьютер связан со следующим. Для обеспечения отказоустойчивости физического кольца в FDDI-сетях применяется топология двойного кольца. При такой топологии каждый компьютер связан с двумя независимыми друг от друга кольцами, в которых трафик движется в противоположных направлениях. Если случается повреждение кабеля в основном кольце, трафик переводится на второе кольцо, и поэтому все компьютеры, входящие в данную сеть, остаются доступными. Такое состояние называется "свернутым кольцом" (wrapped ring). На рис. 2.21 показано двойное кольцо FDDI в обычном и свернутом состоянии.

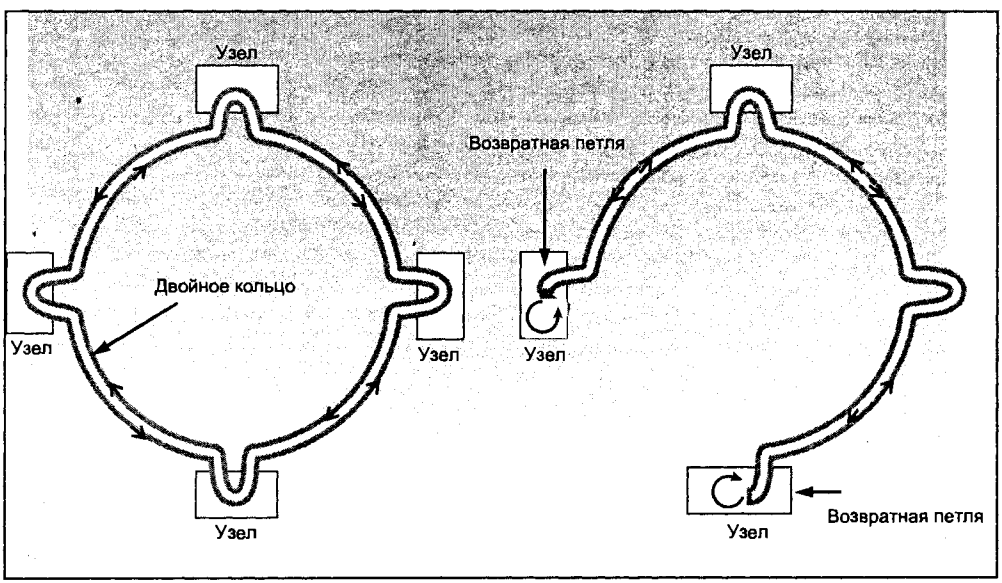


Рис. 2.21. Двойное кольцо FDDI в обычном режиме работы (слева) и в свернутом состоянии (справа)

Компьютеры, которые соединены с обоими кольцами в сети типа FDDI, называются "станциями двойного подключения" (Dual Attachment Stations, DAS). В некоторых компьютерных сетях типа FDDI также используется концентратор, называемый "концентратором двойного подключения" (Dual Attachment Concentrator, DAC). DAC-концентратор соединен с обоими кольцами и, во многом так же, как и MAU-модуль в сетях типа Token Ring, создает внутри себя логическое кольцо. Компьютеры, соединенные с DAC-концентратором, называются "станциями одиночного соединения" (Single Attachment Stations, SAS).

Кадр протокола FDDI

Так же, как и в протоколе типа Token Ring, в протоколе FDDI используется механизм эстафетной передачи маркера. Формат маркерного кадра в протоколе FDDI используется почти тот же самый.

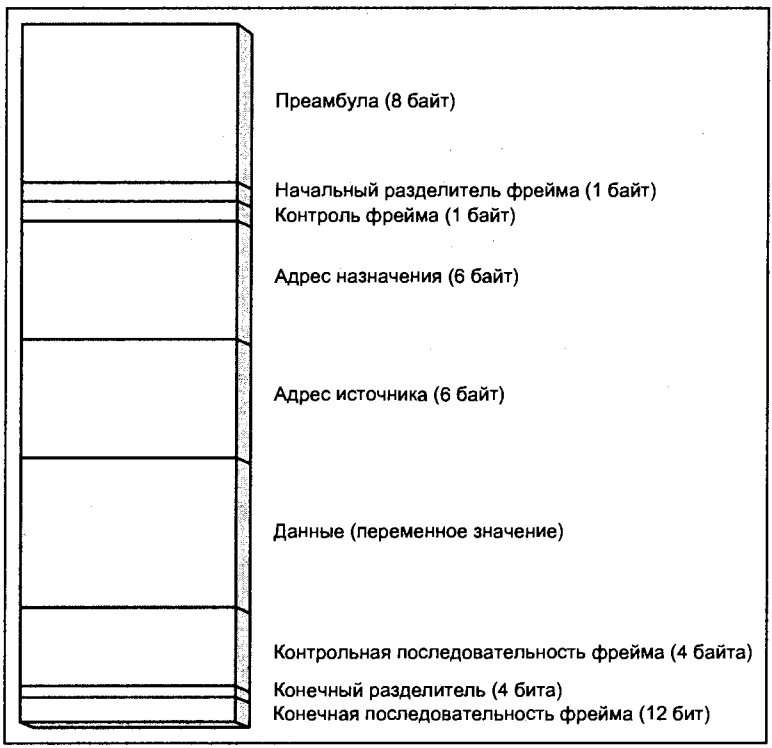


Рис. 2.22. Кадр данных протокола FDDI

Кадр данных в протоколе FDDI также служит для передачи прикладных данных, созданных протоколами верхнего уровня. На рис. 2.22 показана схема кадра данных, используемого в протоколе типа FDDI, а входящие в него поля выполняют следующие функции.

- Преамбула (8 байт). Поле преамбулы (Preamble) содержит последовательность битов, которые служат для синхронизации часов передающей и принимающей системы.
- Начальный ограничитель кадра (1 байт). Поле начального ограничителя (Start Delimiter) содержит значение, которое сигнализирует о начале кадра.
- Управление кадром (1 байт). В поле управления кадром (Frame Control) определяется тип содержащихся в пакете данных. Значение этого поля сообщает о том, что именно содержится в поле данных: данные управления станцией, данные управления доступом к передающей среде или данные управления логической связью.

- Адрес назначения (6 байт). В поле адреса назначения (Destination Address) указывается стандартный адрес компьютера, который должен принять кадр. Этот адрес аппаратно "зашит" в сетевой плате.
- Адрес источника (6 байт). В поле адреса источника (Source Address) сообщается стандартный аппаратный адрес компьютера, отправившего кадр. Этот адрес закодирован в сетевой плате компьютера.
- Данные (переменное значение). В этом поле содержится информация, сгенерированная протоколом сетевого уровня, или данные управления станцией, или данные управления доступом к передающей среде, в зависимости от значения поля управления кадра.
- Контрольная последовательность кадра (4 байт). Поле контрольной последовательности кадра (Frame Check Sequence) содержит значение контрольной суммы, которая служит для выявления ошибок.
- Конечный ограничитель (4 бит). Поле конечного ограничителя (Ending Delimiter) содержит значение, которое служит для обозначения конца кадра.
- Конечная последовательность кадра (12 бит). Данная последовательность битов (End of Frame Sequence) содержит указатели ошибок, подтверждения приема и копирования (Error, Acknowledge, and Copy indicators), которые используются промежуточными системами для определения состояния кадра.

Резюме

В этой главе были даны основные сведения о топологиях компьютерных сетей, кабелях и протоколах канала передачи данных. Описано семь топологий: шинная, звездообразная, шинно-звездообразная, иерархическая звездообразная, кольцеобразная, решетчатая и беспроводная. Описано три вида кабеля: коаксиальный кабель, кабель на основе витой пары и оптоволоконный кабель. Также были описаны три элемента протоколов канального уровня: формат кадров, механизм, регулирующий доступ к сетевой среде, и принципы построения физического уровня компьютерных сетей.

Дополнительные ресурсы

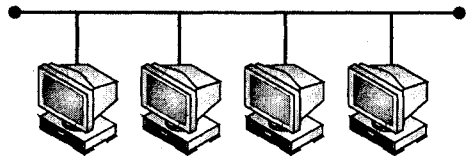
Если у вас есть доступ к сети Интернет, воспользуйтесь следующими адресами, чтобы найти дополнительную информацию по затронутым выше вопросам.

Американский национальный институт стандартизации (American National Standards Institute, ANSI): **http://www.ansi.org/**.

Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers, IEEE): **http://www.ieee.org/portal/index.jsp**.

Ассоциация электронной промышленности (Electronic Industry Association, EIA): **http://www.eia.org/**.

Ассоциация телекоммуникационной промышленности (Telecommunications Industry Association, TIA): **http://www.tiaonline.org/**.



ГЛАВА 3

Сетевые протоколы

Для того чтобы взаимодействовать в вербальной или письменной форме, сторонам, участвующим в этом взаимодействии, необходимо знать и придерживаться некоторого набора правил. Эти правила могут быть простыми, как, например, необходимость ставить вопросительный знак в конце письменного утверждения, которое требует ответа, или они могут быть довольно сложными и обширными, как, например, правила английского или французского языка. Без таких правил обеим сторонам было бы трудно, если вообще возможно, понимать друг друга.

Сказанное верно и для обмена данными — взаимодействующие устройства должны следовать одним и тем же общим правилам. Другими словами, в них должен применяться общий протокол. Этот протокол или набор правил может определять только какие-то основы взаимодействия: например, что считать началом передачи, а что концом, или же он может представлять собой довольно сложный набор правил: например, какой должна быть максимальная продолжительность ожидания перед получением сообщения от какой-либо из взаимодействующих сторон. Знание и понимание правил какого-либо протокола является абсолютно необходимым для того, чтобы уметь выявлять и разрешать проблемы. Без знания правил вы никогда не сможете понять, когда это правило нарушается, а если вы не знаете, когда правило нарушается, вам намного труднее определить, правильно ли работают взаимодействующие устройства и как они должны работать.

В этой главе мы рассмотрим основные сетевые протоколы. Сначала пойдет речь о модели взаимодействия открытых систем (Open Systems Interconnection, OSI) — эталонной модели, которая была разработана для описания того, как происходит обмен данными между компьютерами в сетевой среде. После этого мы рассмотрим некоторые из наиболее распространенных сетевых протоколов, используемых в локальных компьютерных сетях.

Эталонная модель OSI

В 1984 году Международная организация по стандартизации — всемирная федерация, в которую входят государственные организации по стандартизации из около 140 стран — разработала эталонную модель сетевого обмена данными, называемую "Моделью взаимодействия открытых систем" (или OSI-моделью). Эта модель опи-

сывает то, каким образом информация из приложения в одном компьютере перемещается посредством сетевой среды в приложение в другом компьютере. Сегодня эта модель считается главной архитектурной моделью межмашинного взаимодействия и служит в качестве основы для существующих стандартов.

Эталонная модель разрабатывалась для определения архитектурных рамок, ограничивающих задачи логического взаимодействия при обмене информацией между разными компьютерными системами. Основным предназначением OSI-модели является определение и группирование логических функций потока данных между системами, но без детального определения работы каждой функции. Для этой цели была разработана семиуровневая модель, в которой каждому уровню соответствует группа связанных логических функций. Модель определяет общую функцию каждого уровня, а также связь этого уровня с вышестоящими и нижестоящими уровнями, тогда как внутренним содержанием и деталями каждого уровня занимаются уже системные разработчики.

Устанавливая стандартную функцию для каждого уровня, а также определяя взаимосвязи между ними без учета деталей и содержания каждого уровня, OSI-модель позволяет производителям добиться совместимости между своими продуктами без необходимости жертвовать какими-либо элементами в них. Итак, OSI-модель состоит из следующих семи уровней:

- уровень 7 — прикладной;
- уровень 6 — представительский;
- уровень 5 — сеансовый;
- уровень 4 — транспортный;
- уровень 3 — сетевой;
- уровень 2 — канальный;
- уровень 1 — физический.

Каждый уровень объединяет некоторую группу логически связанных между собой задач, которые могут рассматриваться и решаться вполне независимо от задач других уровней. Это позволяет выполнять разработку полнофункциональных решений внутри одного уровня, не касаясь основных функций, описываемых другими уровнями OSI-модели.

Уровни OSI-модели

Уровни OSI-модели можно разделить на две категории: верхние уровни и нижние уровни. Верхние уровни (уровни 5—7) связаны с вопросами, которые относятся к приложениям, и реализуются при помощи программного обеспечения. Нижние уровни (уровни 1—4) связаны с передачей информации посредством компьютерной сети и могут быть реализованы при помощи аппаратного, программного и/или программно-аппаратного обеспечения.

Важно отметить, что модель является только концептуальной формой и не определяет метод взаимодействия. Взаимодействие между компьютерами осуществляется посредством протоколов, которые определяют правила обмена информацией между системами. Протокол реализует функции одного или нескольких уровней модели OSI.

Существует множество разных протоколов, которые предназначены для выполнения совершенно разных задач. Например, протокол маршрутизации действует на 3 уровне сетевой модели и описывает метод, по которому маршрутизаторы определяют

путь движения пакета по компьютерной сети. В отличие от него протокол, действующий на 2 уровне (канальный уровень), в большей степени связан с форматированием и адресацией пакета для его передачи по какому-то конкретному виду передающей среды.

Хотя оба протокола отличаются друг от друга и работают независимо друг от друга, они должны работать согласованно, чтобы передать пакет из одной системы в другую. Поскольку оба этих протокола играют важную роль в передаче пакета по компьютерной сети, необходимо, чтобы, например, канальный уровень не изменял содержание пакета, полученного с сетевого уровня. Наоборот, он должен добавить к пакету ту информацию, которая необходима. На таком порядке зависимости уровней между собой и строится работа OSI-модели, но прежде чем перейти к подробному описанию работы уровней в целом, мы рассмотрим эти уровни и их функции по отдельности.

Уровень 1 (физический)

Уровень 1, или физический уровень, определяет электрические характеристики сети. На этом уровне работают как физическая среда передачи информации на основе коаксиального медного кабеля, средств радиосвязи или оптоволоконного кабеля, так и сетевой адаптер вашего ПК. На этом уровне информация представляет собой последовательность электрических или оптических импульсов, соответствующих нулям и единицам двоичной структуры данных. Не зависимо от информации, ее исходной структуры или содержания, все сводится к этой стандартной общей структуре, которая направляется через сеть.

Следует помнить о том, что если кабель или кабельный сегмент имеет недостаточную длину, то для его удлинения сверх пределов, установленных для данной среды передачи, необходимо использовать *повторитель*, который позволяет регенерировать сигнал. Поэтому физический уровень также включает в себя и повторители.

Уровень 2 (канальный)

Уровень 2, также называемый канальным уровнем, определяет стратегию доступа к разделяемой физической среде. Он подготавливает информацию, или данные, принятые с верхних уровней, для передачи через существующую специфическую среду. На данном уровне устройства имеют дело с двумя областями информации. Первая касается управления доступом к передающей среде (Media Access Control, MAC). Она определяет особые свойства, присущие данной конкретной физической среде, а также способ, позволяющий разделить эту среду между множеством устройств. Вторая касается управления логическим соединением (Logical Link Control, LLC). Она определяет правила использования соединения, синхронизации кадра, контроля за потоком данных и выявления ошибок. Поэтому считается, что канальный уровень состоит из двух подуровней: MAC-подуровня и LLC-подуровня.

LLC определяется в спецификации IEEE 802.2 и поддерживает как службы без установления соединения, так и службы с установлением соединения, используемые протоколами верхних уровней. В соответствии с этой спецификацией в кадрах канального уровня определяется ряд полей, которые позволяют множеству разных протоколов верхнего уровня совместно использовать один и тот же физический канал передачи данных. MAC-подуровень канального уровня управляет доступом к

физической среде. Он содержит описания MAC-адресов, которые позволяют разным устройствам идентифицировать друг друга на канальном уровне.

Функции канального уровня включают следующие элементы.

- *Физическая адресация.* К физическому сегменту шины может быть присоединено множество устройств, как, например, в сети типа Ethernet. Для того чтобы однозначно идентифицировать эти устройства, каждое из них имеет свой уникальный MAC-адрес, который представляет собой число, назначенное производителем устройства. Распределением этих адресов занимается Институт инженеров по электротехнике и электронике (IEEE), одна из организаций по регулированию сетевых стандартов.
- *Топология локального сегмента.* Кроме адресации устройств в локальном сегменте, следует учитывать и другой фактор: логическую топологию сети. Эта топология может представлять собой двухточечное соединение (point-to-point link) между устройствами, или же множество устройств, разделяющих один общий сегмент. В последнем случае устройства могут быть логически организованы в виде кольца, звезды или шины (как в сети типа Ethernet). Кроме того, локальный сегмент, в свою очередь, тоже может быть разделен на сегменты при помощи моста. В этом случае мост ведет регистрацию устройств, находящихся в разных сегментах (рис. 3.1), и направляет пакет данных в тот сегмент, в котором расположено принимающее устройство. Мост перенаправляет пакеты с одного своего порта на другой, только если нужно связать два устройства из разных сегментов. Тем самым достигается сокращение излишнего трафика в сегментах.
- *Обнаружение ошибок.* На этом уровне выявляются ошибки, которые возникают во время передачи сигналов через физическую среду. Механизм обнаружения ошибок защищает верхние уровни от недостатков физической среды передачи. Вычисляемое контрольное значение (например, по методу CRC) помещается в конце кадра перед тем, как отправить его на физический уровень. Принимающий компьютер повторно вычисляет значение CRC и сравнивает его с тем, которое было получено вместе с принятыми данными. Если оба значения совпадают, считается, что данные приняты без ошибок. В противном случае протоколу верхнего уровня, возможно, придется передать этот пакет заново. Хотя канальный уровень предусматривает обнаружение ошибок, он не обязательно включает функцию исправления ошибок. Эта задача перекладывается на верхние уровни — главным образом на транспортный уровень.

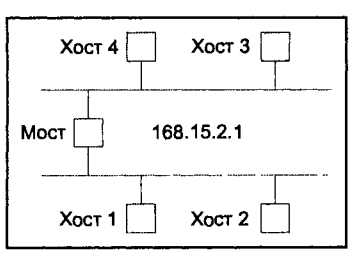


Рис. 3.1. Мост, связывающий два сегмента

Необходимо помнить о следующем принципе: для соединения нескольких передающих сегментов, имеющих один общий сетевой адрес, требуется использовать

мост или *коммутатор 2-го уровня* (layer 2 switch). На рис. 3.2 перечислены основные спецификации локальных и глобальных компьютерных сетей и их связи с физическим и канальным уровнями.

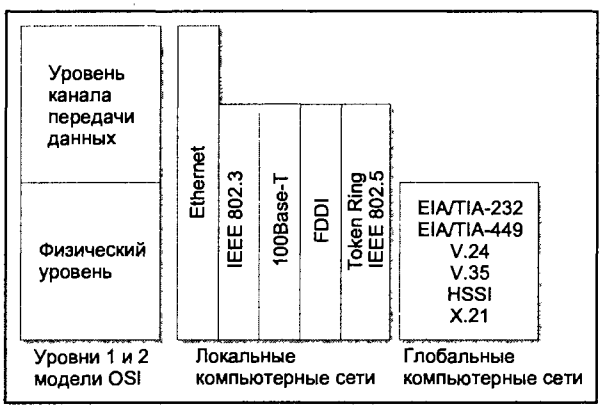


Рис. 3.2. Основные спецификации, используемые на физическом и канальном уровнях в локальных и глобальных компьютерных сетях

Уровень 3 (сетевой)

Сетевой уровень, с точки зрения интернет-протокола, определяет процессы и задачи, обеспечивающие прокладку маршрута передачи пакета. Для этого на 3 уровне определяются логические адреса исходного и конечного устройств, а также всех других устройств (маршрутизаторов), участвующих в передаче пакета через сеть. Здесь же определяется путь передачи пакета.

Если взаимодействующие системы находятся на одном сегменте локальной сети, обмен пакетами между ними может осуществляться непосредственно при помощи канального и физического уровней передающей и принимающей сторон. В этом случае пакет передается с сетевого уровня передающей системы на ее канальный и физический уровни. Уровень канала подготавливает пакет для передачи и перемещает его в физическую среду. Принимающая станция принимает поток битов и восстанавливает изначальную структуру пакета, которая затем передается на сетевой и более высокие уровни принимающего устройства.

Если же передающая и принимающая системы находятся в разных сетях, необходимы маршрутизаторы, которые должны направить пакеты либо по заранее определенному пути, либо по динамически определяемому пути. Маршрутизатор — это устройство, которое действует на первых трех уровнях OSI-модели, как это показано на рис. 3.3. Другими словами, маршрутизатор имеет интерфейс, который непосредственно соединен с физической средой передачи и выполняет функции, определяемые уровнями 2 и 3. Маршрутизаторы способны динамически трассировать компьютерные сети при помощи протокола маршрутизации. Тем не менее путь в сети может быть предопределен, если используются статические маршруты — описания, в которых указан правильный исходящий интерфейс для каждой сети внутри сетевого комплекса.

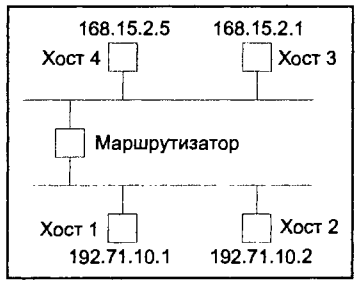


Рис. 3.3. Маршрутизаторы работают на уровнях 1—3

Ниже приводятся некоторые наиболее важные функции сетевого уровня:

- сетевая адресация;
- определение пути между исходным и конечным узлами, расположенными в разных сетях;
- маршрутизация пакетов между сетями.

Необходимо помнить о следующем базовом принципе: для перемещения пакетов между разными сетями требуется *маршрутизатор.*

Уровень 4 (транспортный)

На уровне 4, или транспортном уровне, располагается протокол управления передачей данных. В соответствии со стандартами этот уровень предназначен для того, чтобы освободить сеансовый уровень (уровень 5) от обязанности контролировать целостность и достоверность данных. Если сетевой уровень служит для перемещения пакетов из одной системы в другую, транспортный уровень имеет более широкое назначение. Он должен обеспечивать передачу пакета и исправление всех ошибок, которые были выявлены или о которых поступило предупреждение. Для этих целей на транспортном уровне выполняются следующие задачи:

- управление потоком данных для обеспечения целостности данных;
- мультиплексирование данных, поступающих от приложений верхнего уровня;
- сегментирование дейтаграмм верхнего уровня;
- установление и разрыв соединений между взаимодействующими конечными точками;
- маскирование сложности сети от верхних уровней;
- обеспечение безошибочной передачи данных до места назначения;
- обеспечение надежной доставки сегментов исходных данных, и это не то же самое, что гарантированная доставка;
- общее управление соединениями и передачей данных.

Уровень 5 (сеансовый)

Основное назначение уровня 5, или сеансового уровня, заключается в установлении, управлении и завершении сеансов связи между двумя взаимодействующими точками

представления. *Сеанс* (session) представляет собой ряд взаимосвязанных передач на основе соединения (connection-oriented) между взаимодействующими точками. Организация сеанса может включать в себя идентификацию пользовательской учетной записи и определение типа устанавливаемого взаимодействия.

Здесь нужно учитывать следующее. Если, например, пользователь решает сделать какие-то покупки на Web-сайте и начинает заполнять "корзину покупателя", необходимо, чтобы сеанс сохранился на том же самом Web-сервере, на котором пользователь начал делать свои покупки. Если случайно, в результате действия механизма выравнивания пользовательской нагрузки, клиент окажется перенаправленным на другой сервер из данной группы серверов, начатый процесс покупки (или сеанс) может быть прерван. Поэтому перераспределение пользовательской нагрузки должно происходить в начале сеанса, но не во время нее. По этой причине механизм выравнивания пользовательской нагрузки (который, как правило, работает на транспортном уровне) должен также понимать сеансовый уровень.

Уровень 6 (представительский)

Основной задачей представительского уровня является определение форматов данных, используемых для выполнения различных служб прикладного уровня. В число задач, осуществляемых на этом уровне, входит преобразование протоколов, кодирование/декодирование и распространение графики.

Уровень 7 (прикладной)

Наконец, прикладной уровень — это уровень, который находится ближе всего к конечному пользователю или конечному приложению. На этом уровне выполняются следующие службы:

- ❒ службы работы приложений;
- ❒ службы работы баз данных;
- ❒ службы работы с файлами;
- ❒ службы печати;
- ❒ службы обмена сообщениями.

В табл. 3.1 приводится список всех уровней модели OSI и их краткие описания.

Таблица 3.1. *Уровни модели OSI*

Уровень	Название	Описание
1	Физический	Переносит поток битов внутри компьютерной сети на электрическом и механическом уровне. Обеспечивает аппаратные средства пересылки и получения данных при помощи какого-либо носителя
2	Канальный	Обеспечивает синхронизацию физического уровня, а также управление и слежение за протоколом передачи
3	Сетевой	Обеспечивает маршрутизацию и продвижение данных внутри компьютерной сети

Таблица 3.1 (окончание)

Уровень	Название	Описание
4	Транспортный	Управляет сквозным контролем передачи данных (например, определяет, все ли пакеты достигли места назначения) и контролем ошибок. Этот уровень обеспечивает полноту передачи данных
5	Сеансовый	Устанавливает, координирует и завершает соединения, обмен и диалоги между приложениями на каждой из конечных точек. Координирует сеансы и соединения
6	Представительский	Преобразует входящие и исходящие данные из одного формата представления в другой
7	Прикладной	Осуществляет идентификацию взаимодействующих сторон, идентификацию качества служб, идентификацию пользователей и обеспечение безопасности, а также соблюдение любых ограничений синтаксиса данных. (Этот уровень *не* является самим приложением, хотя некоторые приложения могут выполнять функции прикладного уровня)

Принцип работы уровней и форматы представления информации

Как уже говорилось выше, OSI-модель является архитектурной моделью, описывающей порядок обмена сообщениями или элементами информации между компьютерами. Совокупность уровней этой модели иногда называют *стеком* (stack), и поэтому модель в целом часто называют *OSI-стеком* (OSI stack). Принцип работы модели заключается в следующем: элемент информации, который отправляется с одного компьютера на другой, движется, начиная с прикладного уровня, вниз, проходя через весь стек уровней, до тех пор, пока не достигнет физического уровня. Дойдя до целевой системы, данные должны пройти вверх через весь стек уровней, начиная с физического уровня, до прикладного уровня (рис. 3.4).

Каждый уровень OSI-модели, как правило, взаимодействует с тремя другими уровнями, расположенными сразу над и под ним. (Исключение составляют два уровня: физический и прикладной, которые взаимодействуют только с двумя другими уровнями.) Соответствующий уровень в целевой системе называется *равноправным* (peer layer).

По мере прохождения данных вниз по стеку OSI-уровней в исходной системе с ними происходят два вида преобразования: во-первых, каждый уровень принимает информацию с вышестоящего уровня и разбивает ее на компоненты; во-вторых, к каждому из этих компонентов присоединяется дополнительная управляющая информация. Эта дополнительная информация используется в процессе взаимодействия между исходным уровнем и равноправным уровнем целевой системы.

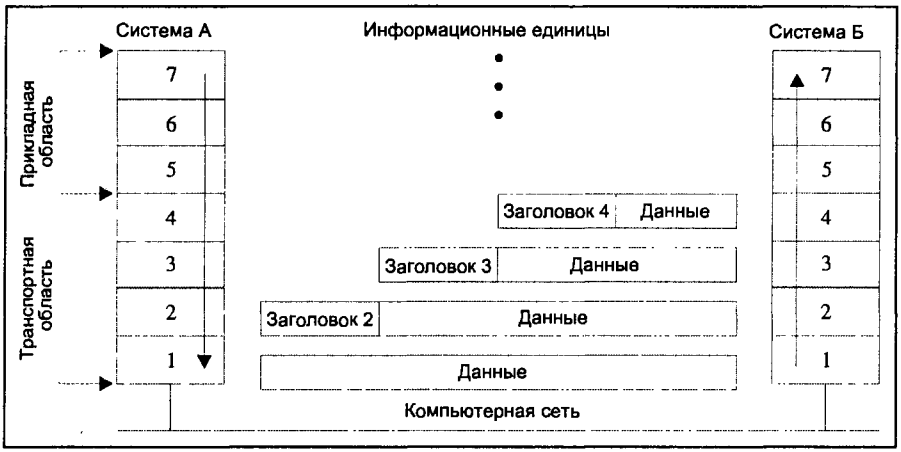


Рис. 3.4. Каждый уровень OSI-модели инкапсулирует или деинкапсулирует поступающую в него информацию

Терминология и форматы

Многие термины применяются для описания данных, пока они перемещаются из одного компьютера в другой. Такие термины, как "сегменты", "сообщения", "пакеты", "дейтаграммы", "кадры", "модули данных" и "ячейки", используются в тот или иной момент времени для описания данных, которые перемещаются от одного компьютера к другому. Во многих случаях они используются как взаимозаменяемые — практика, которая приведет кого-нибудь к вере, что все они имеют одинаковое значение.

В действительности разнообразные термины имеют особый смысл, который напрямую зависит от структуры информации в какой-либо заданный момент ее прохождения из одного компьютера в другой. Термин *"блок данных"* (data unit) является общим обозначением разных видов информационных единиц. Однако все остальные термины имеют конкретные значения. Ниже перечислены наиболее распространенные виды блоков данных.

- Блоки данных служб (Service Data Units, SDUs) — это информационные единицы, поступающие от протоколов верхних уровней, которые определяют запросы служб к протоколу нижнего уровня.
- Блоки данных протокола (Protocol Data Units, PDUs) — используется в OSI-модели для обозначения пакета данных.
- Протокольные блоки данных моста (Bridge Protocol Data Units, BPDUs) — тип блоков данных, которыми обмениваются между собой мосты для того, чтобы избежать циклов.

Кадр — это единица информации, источником и получателем которой являются MAC-адреса, используемые на канальном уровне. Кадр состоит из заголовка и, возможно, завершителя, в которых содержится управляющая информация, характерная для этого уровня. Область кадра, предназначенная для данных, содержит часть исходной информации, поступившей с прикладного уровня, а также другую служеб-

ную информацию, которая была добавлена каждым уровнем по мере прохождения данных через разные уровни стека.

Ячейка также является термином, обозначающим единицу информации, которой обмениваются между собой канальные уровни разных систем. Однако ячейки имеют фиксированный размер и используются в коммутируемых средах (например, в системах с асинхронным режимом передачи данных (Asynchronous Transfer Mode, ATM)). Ячейка состоит из заголовка и области полезной нагрузки (payload). При использовании асинхронного режима передачи данных заголовок ячейки содержит служебную информацию, предназначенную для канального уровня целевого устройства, и ее длина составляет 5 байт. Область полезной нагрузки содержит данные верхнего уровня, которые инкапсулированы в заголовке ячейки; и ее длина составляет 48 байт.

Пакет — это единица информации, которая используется для обмена между сетевыми уровнями разных систем. Структура данных здесь состоит из заголовка и, возможно, завершителя, в котором содержится служебная информация, характерная для сетевого уровня. Область данных состоит из служебной информации, предназначенной для верхних уровней, плюс некоторая часть исходной информации. *Дейтаграмма* также служит для обозначения единиц информации, которыми обмениваются сетевые уровни разных систем. Однако этот термин обычно указывает на сетевые службы *без установления соединения* (connectionless).

Термин *сегмент* служит для обозначения единиц информации, источником и адресатом которых является транспортный уровень. *Сообщение* — это единица информации, которая используется для обмена между любыми уровнями, расположенными выше транспортного (т. е. между уровнями 5—7). На рис. 3.4 показано, как данные перемещаются по стеку OSI-уровней. Каждый последующий уровень, в зависимости от направления потока, либо инкапсулирует, либо деинкапсулирует информацию, поступившую из прилежащих уровней. Поток информации между двумя компьютерами можно описать следующим образом.

1. Пользовательские данные преобразуются в сообщение.
2. Транспортный уровень преобразует сообщение во множество сегментов и передает их на сетевой уровень.
3. Сетевой уровень принимает каждый сегмент и разбивает его на пакеты или дейтаграммы, в зависимости от типа службы (на основе соединения или без соединения). Пакеты и дейтаграммы передаются на уровень канала передачи данных.
4. Уровень канала передачи данных разбивает пакеты или дейтаграммы на кадры или ячейки. Кадры или ячейки направляются в виде потока в физическую среду.

Применение модели OSI в среде Microsoft Windows

Сетевой компонент операционной системы Microsoft Windows реализует различные функции уровней OSI-модели. Протокол не всегда полностью совпадает с соответствующим OSI-уровнем, но даже в этих случаях в протоколе обычно имеются функции, предназначенные для тех же целей, что и в многоуровневой модели OSI. Польза модели OSI заключается уже хотя бы в том, что она дает концептуальный подход к разработке сетевых компонентов, т. е. позволяет организовать разные элементы

системы, начиная от кабелей и заканчивая сетевым окружением (Network Neighborhood), таким образом, чтобы компьютеры могли взаимодействовать через сеть.

Как же модель OSI связана со средствами сетевого взаимодействия, имеющимися в операционной системе Windows NT? Чтобы понять это, мы еще раз пройдем по всем уровням модели OSI, но на этот раз будем их рассматривать вместе с соответствующими протоколами, используемыми в NT-сетях, и обсудим, как эти протоколы связаны с OSI-моделью и как они взаимодействуют между собой, образуя работоспособную NT-сеть.

Физический уровень в среде Windows

Компонентами, которые относятся к физическому уровню, являются сетевые платы, предназначенные для работы в сетях типа Ethernet, Token Ring, беспроводных сетях и других типах компьютерных сетей. Конечно, физическая среда тоже входит в число этих компонентов. Сам физический интерфейс, как правило, соединен с сетевой платой или же работает через отдельное устройство, как это сделано в сетевом адаптере PCMCIA (Personal Computer Memory Card International Association — Международная ассоциация производителей плат памяти для персональных компьютеров) Ethernet. Кроме упомянутых типов карт в системах Windows также предусмотрен соответствующий интерфейс для установления удаленного соединения (dial-up). В операционной системе Windows 2000 сведения обо всех сетевых аппаратных компонентах физического уровня можно получить щелкнув правой кнопкой мыши на пиктограмме **My Computer** (Мой компьютер), расположенной на рабочем столе, затем выбрав в появившемся контекстном меню команду **Properties** (Свойства), далее в открывшемся окне **System properties** (Свойства системы) перейдя на вкладку **Hardware** (Оборудование) и нажав на кнопку **Device Manager** (Диспетчер устройств) (рис. 3.5).

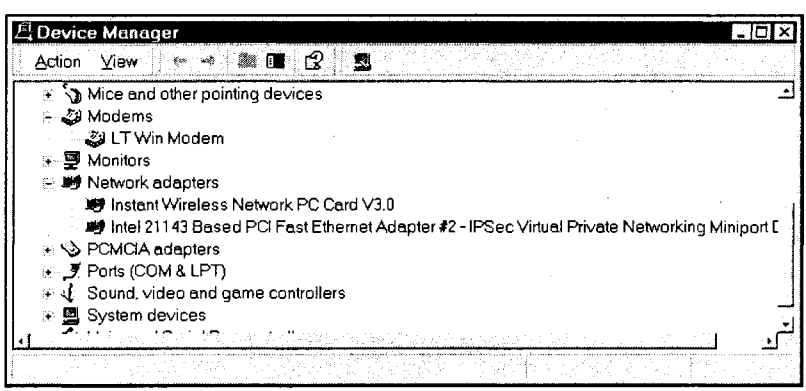


Рис. 3.5. Сведения о компонентах физического уровня в системе Windows можно получить при помощи Device Manager (Диспетчер устройств)

Соединение на физическом уровне внутри среды Windows не ограничивается сетевыми платами. Любой тип интерфейса или кабеля, который служит для взаимодействия между компьютерами, осуществляет функции физического уровня. В число этих компонентов входит последовательный коннектор RS232 (COM1, COM2 и т. д.),

параллельный порт и любые порты типа USB (Universal Serial Bus — универсальная последовательная шина). В последние годы USB-порты стали распространенным средством присоединения широкополосных сетевых устройств к ПК. При организации сетей на основе USB-устройств сетевой адаптер соединяется с компьютером пользователя посредством шины USB.

Канальный уровень в среде Windows

Ethernet является наиболее распространенным протоколом канального уровня в типичном сетевом окружении Windows. Уровень канала передачи данных упаковывает данные в кадры. Затем каждый кадр снабжается исходным адресом и адресом назначения, которые являются физическими аппаратными адресами, закодированными в сетевых картах. По этой причине такие адреса иногда называют "зашитыми" (Burned-In Address, BIA), но правильным названием является "адрес управления доступом к среде" (Media Access Control address) или "MAC-адрес". Эти адреса используются для идентификации той сетевой платы, с которой передается каждый кадр, и той платы, на которую он передается. Важно отметить, что MAC-адрес не обязательно является единственным адресом целевого компьютера, поскольку существуют некоторые конфигурации, в которых ПК может иметь более чем одно соединение с одной и той же, или с несколькими локальными сетями.

Ethernet — лишь один из многих подобных протоколов канального уровня. Другими представителями являются протоколы Token Ring и Arcnet. Если базовое соединение осуществляется не в локальной сети, Windows может использовать другие протоколы канального уровня — например, протокол двухточечного соединения (Point-to-Point Protocol, PPP) или межсетевой протокол для последовательного канала (Serial Line Internet Protocol, SLIP), причем оба применяются для последовательных соединений.

Мы не будем рассматривать протоколы PPP и SLIP подробно, т. к. это выходит за рамки данной главы. Оба протокола используются для установления соединений через Интернет, что позволяет таким программам, как Internet Explorer, Netscape и другим IP-приложениям, например Telnet, работать через модемное соединение. Протокол PPP является в этой паре более новым, он встроен в среду Windows через службу удаленного доступа. Это ориентированный на соединение протокол, который инкапсулирует множество пакетов, поступающих от разных сетевых протоколов, таким образом, что все пакеты могут быть переданы одновременно по одной линии. Протокол PPP содержит три части: одна часть инкапсулирует протокол в общие PPP-пакеты с заголовками, в которых сообщается тип сетевого протокола; вторая часть устанавливает соединение; и третья часть описывает всякие особые условия, свойственные данному протоколу, например разрешение IP-адресов в аппаратные адреса.

В конце этой главы приведены некоторые полезные ссылки, касающиеся протоколов SLIP и PPP.

Сетевой уровень в среде Windows

Одна из основных функций сетевого уровня заключается в том, чтобы назначать и регистрировать логические адреса, которые идентифицируют главные сетевые узлы внутри сети. В среде Windows в качестве протокола сетевого уровня наиболее часто используется IP (Internet Protocol — протокол Интернета) и IPX (Internetwork Pac-

ket Exchange — протокол межсетевого пакетного обмена) *(см. далее в этой главе разд. "IP-протокол" и "Протокол IPX/SPX")*. Как правило, логический сетевой адрес по своему составу соответствует аппаратному адресу. В результате, сетевой адрес (или IP-адрес в случае IP-протокола) может идентифицировать не компьютер, а аппаратный интерфейс. При этом компьютер может иметь несколько сетевых плат для одной или нескольких разных локальных сетей, и каждая из этих карт будет иметь свой сетевой и аппаратный адрес. Вот почему в рамках модели для обозначения сущности, которая описывается сетевым адресом, больше подходит термин "сетевой узел".

В среде Windows 2000 протоколы сетевого уровня можно найти следующим образом: открыть свойства пиктограммы **My Network Places** (Мое сетевое окружение), расположенной на вашем рабочем столе, и затем в открывшемся окне выбрать объект **Local Area Connection** (Подключение по локальной сети) и открыть его свойства (рис. 3.6). Именно здесь происходит назначение сетевых адресов. Более подробно о сетевых адресах мы будем говорить в *разд. "Сетевые протоколы" далее в этой главе.*

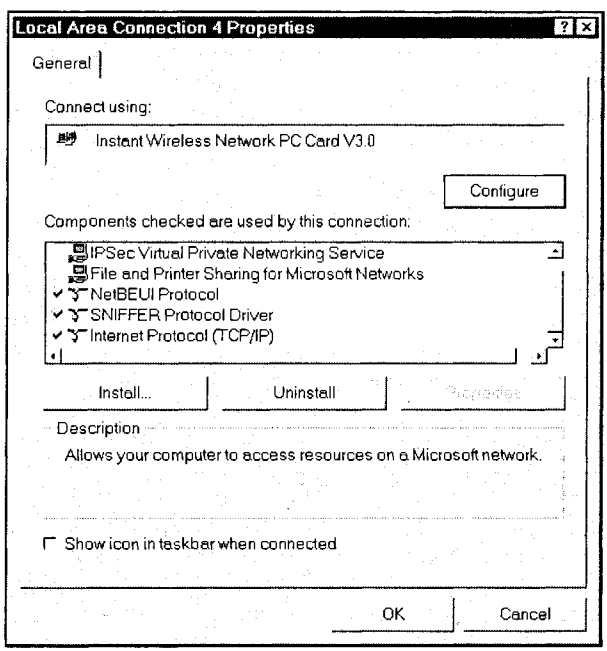


Рис. 3.6. Сетевые протоколы можно увидеть, заглянув в свойства Подключения по локальной сети

Кроме того, существует множество скрытых протоколов, которые своей согласованной работой должны обеспечивать бесперебойное функционирование сети. Одним из таких протоколов является протокол разрешения адресов (Address Resolution Protocol, ARP), который мы подробно изучим далее в этой главе. Этот протокол служит для логического преобразования сетевых адресов в физические аппаратные адреса.

В отличие от аппаратного адреса, который является постоянным адресом сетевой платы, сетевой адрес является изменяемым и в некоторых конфигурациях может изменяться после каждой новой загрузки ПК. Протокол ARP служит для установления динамического соответствия между аппаратным адресом и логическим сетевым адресом.

Для того чтобы увидеть IP-адрес сетевой платы в компьютере с установленной ОС Windows 2000, откройте окно командной строки Windows (выполнив C:\WINNT \System32\cmd.exe) и введите следующую команду:

```
C:\WINNT>ipconfig
```

Вот пример результата:

```
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection 4:
       Connection-specific DNS Suffix  . : carty.testdns.com
       IP Address. . . . . . . . . . . . : 192.168.31.101
       Subnet Mask . . . . . . . . . . . : 255.255.255.0
       Default Gateway . . . . . . . . . : 192.168.31.1
```

Эта команда выдает список всех логических сетевых адресов для всех активных и присоединенных сетевых плат. Также результат этой команды показывает, присоединен или нет физический кабель к сетевой плате.

Транспортный уровень в среде Windows

Протоколы сетевого уровня, например, IP или IPX, прослеживают адреса уровня 3 и в каждый момент времени определяют наиболее эффективный маршрут для передачи данных. Однако в функции этих протоколов не входит обеспечение конечной доставки данных — эта обязанность лежит на протоколах, работающих на транспортном уровне. Обеспечение доставки пакета данных до места назначения является функцией таких протоколов, как TCP (для IP) и SPX (для IPX). Другим транспортным протоколом, используемым совместно с IP, является UDP (User Data Protocol — протокол передачи дейтаграмм пользователя). Сети Windows используют его для межпрограммного взаимодействия, а также для таких приложений, как служба разрешения имен в системе NetBIOS. Оба протокола, TCP и UDP, зависят от IP.

Транспортные протоколы TCP и UDP автоматически становятся доступными всякий раз, когда протокол IP используется в среде Windows. Чтобы отобразить состояние всех соединений с использованием протоколов TCP и UDP, откройте окно командной строки Windows (выполнив C:\WINNT\System32\cmd.exe) и введите следующую команду:

```
C:\WINNT>netstat
```

Вот пример результата:

```
Active Connection
 Proto  Local Address          Foreign Address        State
 TCP    glen_carty-h1:1060     63.249.162.173:http    ESTABLISHED
 TCP    glen_carty-h1:1061     63.249.162.173:http    ESTABLISHED
 TCP    glen_carty-h1:1062     63.249.162.173:http    ESTABLISHED
 TCP    glen_carty-h1:1069     204.71.191.241:http    ESTABLISHED
```

Сеансовый уровень в среде Windows

Система NetBIOS (Network Basic Input Output System — сетевая базовая система ввода/вывода) является стандартным программным интерфейсом приложения (Application Programming Interface, API), используемым такими службами, как служба локализации ресурсов в сетях Windows. Это программа, которая позволяет приложениям разных компьютеров взаимодействовать друг с другом. Однако сама по себе она не поддерживает механизмы маршрутизации и транспортировки данных и поэтому зависит от других транспортных протоколов, таких как TCP или UDP. В качестве альтернативы она может использовать NetBEUI (NetBIOS Extended User Interface — расширенный пользовательский интерфейс на базе NetBIOS), разработанный в качестве ее расширения. Протокол NetBEUI обеспечивает стандартный формат данных для передачи по глобальной сети.

Иногда сбивает с толку то, что в сетях Windows система NetBIOS доступна по умолчанию всегда, когда доступен протокол TCP/IP. Дело в том, что при установке других сетевых протоколов нет возможности подключить NetBIOS поверх TCP/IP (NetBT). Напротив, существование NetBEUI фактически означает подключение NetBIOS через NetBEUI. Чтобы загрузить протокол TCP/IP без поддержки NetBIOS, нужно снять флажок **Enable Internet Connection Sharing for This Connection** (Разрешить совместное использование этого подключения к Интернету), расположенный на вкладке совместного использования окна **Local Area Connection** (Подключение по локальной сети). Совместное использование файлов и принтеров также должно быть отключено.

Представительский и прикладной уровни

Присутствующий в среде Windows *редиректор* (redirector) является функцией прикладного уровня. Он предназначен для обслуживания направляемых к ОС запросов на прикладные данные и позволяет определить, к чему именно относятся эти запросы: к данным, расположенным локально, или же к сетевым ресурсам. Редиректор направляет сетевые запросы на серверы, а локальные команды передает в локальную операционную систему.

Блок серверных сообщений (Server Message Block, SMB) — это протокол представительского уровня, который регулирует совместное использование файлов, принтеров и последовательных портов через локальную сеть. Кроме того, протокол SMB отвечает за обслуживание пользовательских сообщений. SMB-протокол является протоколом типа "клиент-сервер", при котором происходит обмен запросами и ответами между клиентом и сервером. Однако SMB-протокол отвечает только за регулирование совместного доступа, но не за транспортировку данных, поэтому его можно использовать вместе с такими протоколами, как NetBIOS/NetBEUI, NetBIOS/TCP /IP или IPX/SPX.

Сетевые протоколы

В этом разделе мы рассмотрим базовые сетевые протоколы, которые используются в локальных компьютерных сетях предприятий. Для каждого базового сетевого протокола (например, протокол IP или IPX), как правило, есть много дополнительных протоколов, которые охватывают все уровни модели OSI. Обычно они строятся на основе базового сетевого протокола, поскольку именно он отвечает за перемещение

пакетов данных между сетевыми узлами, и именно этот протокол получает наибольшее количество сведений о том, какие хосты в данный момент доступны в локальной сети. Протоколы верхних уровней могут пользоваться службами, предоставляемыми сетевым протоколом, и это избавляет их от необходимости выполнять задачи, отведенные для нижних уровней.

Темой этой главы являются сетевые протоколы, поэтому некоторые из наиболее часто встречающихся протоколов мы рассмотрим подробно. Однако нужно сказать, что сетевые протоколы (как, например, IP-протокол) обычно зависят от протоколов маршрутизации (т. е. протоколов уровня 3), которые позволяют им динамически определять маршрут движения пакета данных по сети. Тем не менее мы не будем вдаваться глубоко в детали протоколов маршрутизации, т. к. *эта тема будет рассмотрена в гл. 14.*

Сетевые протоколы могут работать и без помощи протоколов маршрутизации. Так как сетевые протоколы могут хорошо понимать локальную сеть, они способны эффективно перемещать пакеты данных между хостами. Однако если несколько локальных сетей связаны между собой, то каждой из них нужна помощь, чтобы иметь возможность "видеть" за своими пределами. Маршрутизаторы являются устройствами уровня 3, которые применяются для того, чтобы соединить между собой несколько сетей. Эти устройства помогают передать пакет данных из одной сети в другую. Для этого маршрутизаторы должны иметь сведения о тех локальных сетях, к которым они присоединены, а также о тех сетях, которые находятся за их пределами. Маршрутизаторы могут легко получить сведения о ближайших сетях, к которым они присоединены. Однако если целевой хост находится в сети, расположенной за пределами близлежащих к маршрутизатору сетей, задача усложняется.

В этом случае маршрутизатору необходимо сообщить о тех сетях, к которым он не присоединен непосредственно, но которые могут быть доступны через другой маршрутизатор. Это достигается при помощи статических маршрутов, которые определяют пути к доступным сетям и по которым можно передать предназначенные для них пакеты данных. Вместо этого метода возможен и иной вариант: маршрутизатор может использовать другой протокол, который поможет ему получить необходимую информацию об удаленных компьютерных сетях.

Именно здесь становятся полезными протоколы маршрутизации, которые служат для динамического расчета наилучшего пути передачи пакета данных из одной компьютерной сети в другую. Эти протоколы понимают сеть сетей, межсетевую работу, и отслеживают внутри сетевого комплекса проблемные области. В этой главе мы еще поговорим об этих протоколах и объясним, как они работают в сочетании с базовым сетевым протоколом. Однако прежде всего наше внимание будет сосредоточено на самих базовых сетевых протоколах.

Общие сведения о протоколах

Протокол по сути представляет собой набор заранее согласованных правил. Это верно для всех протоколов, не только сетевых. Нормальная работа сети зависит от того, подчиняется ли этому набору правил каждое из входящих в нее устройств. Для того чтобы заниматься конфигурированием компьютерной сети, а также ее управлением и обслуживанием, менеджер сети должен понимать, как работает каждый протокол и как все они взаимодействуют между собой. Без этого понимания невозмож-

но добиться эффективной работы сети, а тем более устранить в ней какие-либо неполадки.

Стек протоколов Интернета

Протокол TCP/IP на самом деле состоит из двух совершенно разных протоколов, которые работают на уровнях 4 (IP) и 3 (TCP) модели OSI. Название TCP/IP, как правило, используется для обозначения стека протоколов, в котором наиболее распространенными являются протоколы TCP и IP. С этой точки зрения более точным было бы другое обозначение — стек протоколов Интернета.

В этом разделе мы подробно рассмотрим IP-протокол, поскольку он является базовым сетевым протоколом, на котором основаны все остальные протоколы из этого семейства, и, кроме того, этот протокол в наибольшей степени соответствует теме данной главы. Мы также рассмотрим такие вспомогательные протоколы, как протокол разрешения адресов (Address Resolution Protocol, ARP) и протокол динамической конфигурации хоста (Dynamic Host Configuration Protocol, DHCP).

IP-протокол

IP-протокол основан на понятиях хостов и сетей. Хост — это любое устройство, входящее в компьютерную сеть, которое способно передавать и получать IP-пакеты через сеть. Таким образом, в качестве IP-хостов могут выступать маршрутизаторы, рабочие станции, серверы или любые другие устройства, имеющие IP-адрес. Говорят, что совокупность хостов, разделяющая общую адресную структуру, находится в пределах одной и той же IP-сети. Обычно эти хосты также разделяют и один общий кабельный сегмент (например, сегмент Ethernet-кабеля).

Основным правилом построения IP-сетей является следующее: хосты, находящиеся в пределах одной сети, могут взаимодействовать между собой напрямую, но если они находятся в разных сетях, то для взаимодействия им необходим маршрутизатор. Такая логика становится понятной, если рассмотреть ее с точки зрения OSI-модели: маршрутизатор действует на 3 уровне, так же как и IP-протокол. Если два хоста расположены в двух разных сетях Интернет, у них будут два разных сетевых адреса. Другими словами, у них будут два разных адреса уровня 3. Поэтому для различения этих адресов требуется устройство, которое работает на том же уровне. Такое устройство называется маршрутизатором.

Это общее правило помогает легко понять, почему два хоста, которые используют один кабельный сегмент, но имеют разные сетевые адреса, не могут взаимодействовать между собой напрямую. Даже при такой конфигурации для взаимодействия потребуется маршрутизатор, несмотря на то, что оба хоста физически находятся на одном и том же кабеле.

В некоторых конфигурациях разные хосты, входящие в одну сеть, физически могут располагаться на разных кабельных сегментах. В этом случае сегменты должны быть соединены при помощи моста, что является функцией уровня 2. Устанавливая связь между двумя сегментами, мост имитирует для передающего устройства ситуацию, будто целевое устройство физически находится на том же кабельном сегменте. Передающее устройство отправляет кадр на кабель, а мост направляет его на целевой кабельный сегмент. Здесь логично задать вопрос: каким образом передающее уст-

ройство может узнать физический адрес принимающего устройства, если ему известен только его сетевой адрес? На этот вопрос мы ответим далее в разделе, посвященном протоколу разрешения адресов.

Сетевая адресация

Чтобы понять IP-протокол, необходимо разобраться в его схеме адресации. Твердые знания IP-адресации являются первым шагом к постижению задач конфигурирования, обслуживания, управления и поиска неисправностей в IP-сетях. Каждый хост, входящий в сеть, будь то локальная сеть или сеть сетей (как, например, Интернет), должен иметь уникальный адрес.

Сетевые протоколы идентифицируют разные узлы сети тем же образом, каким мы при помощи адресов идентифицируем разные здания. В обычной жизни конкретный адрес служит для обозначения какого-то здания, а почтовый индекс используется для обозначения какой-то большой, но четко определенной области. IP-адрес тоже состоит из двух частей: одна часть служит для обозначения хоста, а другая часть — для обозначения той сети, в которой этот хост расположен.

В некоторых случаях к обычным адресам могут добавляться какие-нибудь названия — например, "Белый дом" или "Эмпайр Стейт Билдинг". Эти названия помогают идентифицировать адрес без необходимости указывать его детали (номер улицы и почтовый индекс). Это же относится и к IP-протоколу — в некоторых случаях хосты могут иметь дополнительные имена. Такие имена удобны тем, что они избавляют от необходимости помнить сложную адресную структуру. Однако, с точки зрения аппаратного и программного обеспечения, такое имя не может использоваться для маршрутизации пакетов данных — вместо него необходим действительный IP-адрес. Поэтому возникает вопрос о том, как эти имена преобразуются в конкретные адреса. Хранящийся на локальном диске *файл хостов* (host file) содержит список имен и соответствующие этим именам IP-адреса. Windows и другие системы используют этот файл для преобразования имен в IP-адреса. Ниже приводится отрывок из такого файла, хранящегося в системной папке Windows. В этом отрывке показано, что имя localhost связано с IP-адресом 127.0.0.1, который является особым адресом, называемым "адресом обратной связи" (loopback address) для данной локальной машины. Строки, начинающиеся с символа #, являются комментарием.

```
#Этот файл является примером файла HOSTS, используемого протоколом
#Microsoft TCP/IP для Chicago.
#Этот файл содержит список IP-адресов и соответствующие им имена хостов.
#Каждая запись должна быть на отдельной строке. Сначала должен идти
#IP-адрес (в первой колонке). За ним должно следовать соответствующее имя
#хоста. IP-адрес должен отделяться от имени хоста по крайней мере одним
#пробелом.
#Кроме того, в этом файле можно помещать комментарии на отдельной строке
#или после машинного имени, которые следует отделять символом #.
#Например:
#102.54.94.97          rhino.acme.com          # исходный сервер
# 38.25.63.10          x.acme.com              # клиентский хост x
127.0.0.1 localhost
```

Этот список может храниться на центральном сервере, называемом службой доменных имен (Domain Name Service, DNS). Для разрешения поступившего имени хоста

IP-протокол в первую очередь попытается использовать список хостов, хранящихся на локальном диске. Если это имя там не обнаружено, IP-протокол отправит запрос по адресу DNS-сервера (если таковой указан) для того, чтобы этот сервер перевел имя хоста в реальный IP-адрес.

Структура и классы IP-адресов

IP-протокол использует схему адресации, состоящую из 32 бит (или 4 байт), которые выражены четырьмя десятичными числами, разделенными точками. Такая схема представления адресов иногда называется "десятичным адресом с разделительными точками" (dotted decimal address). Четыре байта, или четыре десятичных числа, обозначают некоторый конкретный хост и являются его сетевым адресом.

IP-адрес, например, 192.168.14.100 кодирует некоторый хост и сетевой адрес, но по его содержанию трудно понять какая часть обозначает адрес хоста, а какая — сетевой адрес. Если применить самое общее правило адресации, можно определить, что 192.168.14 — это сетевая часть адреса, а 100 — адрес хоста. В чем же заключается это правило?

Оно заключается в том, что существует три основных класса IP-адресов: класс A, класс B и класс C. В адресах класса A больше адресов хостов, чем сетевых адресов. В этих адресах 32 бита логически разбиваются так, что первое десятичное число обозначает сеть, а остальные числа — адреса хостов.

В адресах класса B первые две десятичные позиции используются для обозначения сетевой части адреса, а остальные позиции — для хостов. Таким образом, в адресах класса B встречается почти столько же сетевых адресов, сколько адресов хостов.

В адресах класса C первые три десятичные позиции используются для обозначения сетевой части адреса, а четвертая позиция — для представления адреса хоста. Из этого видно, что вышеприведенный адрес (192.168.14.100) является адресом класса C, т. к. первые три октета в нем являются сетевой частью. Однако это еще не объясняет, почему указанный адрес является адресом класса C. Как можно понять, что именно первые три октета в адресе являются сетевой частью, а не первый из них (в этом случае адрес будет иметь класс A) или первые два из них (в этом случае адрес будет иметь класс B). Ответ можно найти в табл. 3.2, где указаны диапазоны каждого из классов.

Таблица 3.2. *Три основных класса IP-адресов*

Класс	Диапазон сетевых номеров	Число бит	Диапазон номеров хостов	Число бит
A	0.h.h.h–126.h.h.h	7	n.0.0.1–n.255.255.254	24
B	128.0.h.h–191.255.h.h	14	n.n.0.1–n.n.255.254	16
C	192.0.0.h–223.255.255.h	21	n.n.n.1–n.n.n.254	8

Примечание: h = хост (host), n = сеть (network).

Из содержания табл. 3.2 можно с уверенностью заключить, что если первый октет IP-адреса оказывается в диапазоне 192—223, то этот адрес, как в нашем примере, является адресом класса C. Для того чтобы уметь отличать IP-адреса по классу, сле-

дует запомнить эти диапазоны. Однако для тех читателей, которые хотят узнать больше о том, откуда происходят эти диапазоны, мы затронем этот вопрос более подробно.

Основные классы сетевых адресов основаны на первых трех битах 32-битового адреса. Когда маршрутизатор получает пакет данных, он не обращается к таблице для определения класса. Вместо этого он читает первые три бита (высокоуровневые биты, high order bits) адреса. Как показано на рис. 3.7, в адресах класса A все первые биты первого октета равны 0, в адресах класса B первый бит равен 1, а в адресах класса C и первый, и второй биты равны 1, а третий — 0.

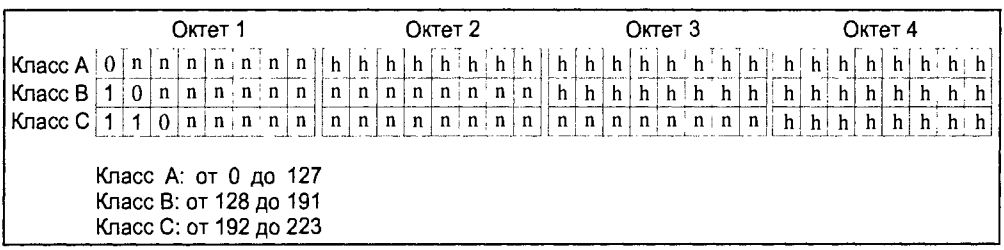


Рис. 3.7. Основные классы IP-адресов

Внимательный читатель мог заметить, что основные классы сетевых адресов в первом октете занимают диапазон только от 0 до 223. Диапазон от 224 до 239 составляет класс D, который зарезервирован для групповых адресов (multicast addresses), использующихся специально для адресации групп хостов. Класс E, который охватывает диапазон от 240 до 247, также зарезервирован. Оставшиеся адреса вплоть до 255 также являются зарезервированными, но, как правило, они не включаются в диапазон класса E.

Развитие концепции IP-адресации

До сих пор мы рассматривали те структуры IP-адресации, которые входят в основные классы IP-адресов. На самом деле использование адресов, входящих в тот или иной класс, — концепция, называемая "классовой адресацией" (classful addressing), — может быть весьма неэффективным. Изначально идея классовой адресации состояла в том, чтобы создать структуру, при которой схема адресации потребовалась бы только для очень больших сетей с тысячами хостов (в то время считалось, что таких сетей будет немного). Для больших компаний (как, например, IBM) назначались сети класса A, т. к. они соответствовали профилю глобальной сети, для которой необходимо адресное пространство, вмещающее огромное число хостов по всему миру. Для компании IBM был назначен адрес 9.0.0.0.

Компании среднего размера должны были получать адреса класса B, а небольшие компании, которые могут иметь всего лишь одну локальную сеть, должны были получать адреса класса C. Такова была логика этой адресной структуры. Однако что произойдет, если небольшая компания вырастет до такой степени, нечто ей потребуется больше чем одна сеть с адресом класса C, как, например, в случае появления двух дополнительных локальных сетей? Или что произойдет, если компания имеет сеть с адресом класса B, но ей необходимо иметь несколько сетевых адресов? В этих случаях классовая адресация оказывается недостаточной.

Для преодоления ограничений классовой адресации используется понятие *подсетей* (subnetting). Организация подсетей — это метод логической сегментации классового адреса на несколько сетевых адресов посредством использования некоторых из хостовых битов для обозначения подсети. Необходимость в организации подсетей становится очевидной, если посмотреть на то, как работает IP-адресация. Сетевой адрес требуется для каждого существующего кабельного сегмента, если эти сегменты не соединены мостом. Адрес класса B мог бы использоваться только на одном сегменте. При введении еще одного сегмента потребовался бы еще один адрес класса B. Однако, в случае применения подсетей, можно использовать один-единственный адрес класса B для обоих сегментов, как это показано на рис. 3.8.

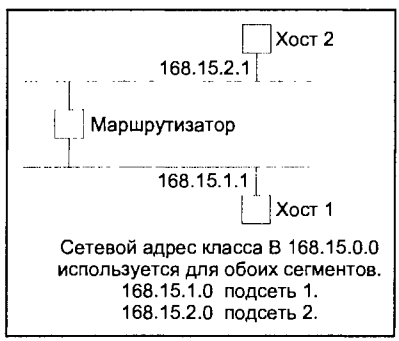


Рис. 3.8. Организация подсетей позволяет создать несколько сетей посредством системы классовой адресации

В основе такой структуры лежит использование *масок подсетей* (subnet masks). Маска — это дополнительная адресная структура, которая служит для указания тех битов в 32-битовом адресе, которые обозначают сетевую часть адреса. В табл. 3.3 указаны маски для рассмотренных трех классов адресов.

Таблица 3.3. *Маски для основных классов IP-адресов*

Класс адреса	Маска
A	11111111.00000000.00000000.00000000
B	11111111. 11111111.00000000.00000000
C	11111111. 11111111. 11111111.00000000

Биты со значением 1 в маске означают, что соответствующие биты IP-адреса являются частью сетевого адреса. Таким образом, в приложении к адресу класса B 168.15.1.100 результат будет следующим (табл. 3.4).

В этом примере маска указывает на то, что адрес 168.15.0.0 является сетевым, а адрес хоста — 1.100. В последней строке таблицы приводится другой способ представления этой информации. Число, которое следует за десятичным адресом с разделительными точками, обозначает число битов, использованных в маске.

Таблица 3.4. Пример 1 маски для IP-адреса 168.15.1.100

Десятичный адрес с разделительными точками	168.15.1.100
Двоичное представление	10101000.00001111.00000001.01100100
Маска	11111111.11111111.00000000.00000000
Маска в десятичном представлении с разделительными точками	168.15.1.100/16

Теперь рассмотрим следующую маску (табл. 3.5).

Таблица 3.5. Пример 2 маски для IP-адреса 168.15.1.100

Десятичный адрес с разделительными точками	168.15.1.100
Двоичное представление	10101000.00001111.00000001.01100100
Маска	11111111. 11111111. 11111111.00000000
Маска в десятичном представлении с разделительными точками	168.15.1.100/24

В этом примере маска указывает на то, что сетевой частью IP-адреса является 168.15.1.0, а хостовой частью — .100. Этот адрес также относится к классу B, но для обозначения подсетей в нем используются некоторые из битов, зарезервированных для хостовых адресов. Число подсетей, определенное маской, равно 254. Такой тип организации подсетей называется "маска подсети с фиксированной длиной" (Fixed-Length Subnet Mask, FLSM).

Маска подсети с переменной длиной (VLSM)

Маска подсети с переменной длиной (Variable-Length Subnet Mask, VLSM) дает больше возможностей, чем маска с фиксированной длиной. В приведенных примерах маска подсети использовалась таким образом, что каждая дополнительная подсеть имеет одно и то же количество хостовых адресов. Например, в уже приведенном нами адресе класса B 168.15.0.0 два последних октета используются для обозначения разных хостовых адресов. Однако при использовании 24-битовой маски третий октет также должен быть использован для обозначения подсетей внутри сети класса B, и в этом случае хостовые адреса будут обозначаться только четвертым октетом. Это означает, что число подсетей может быть равно 254 (определяется третьим октетом), а каждая из них может иметь 254 хоста (определяется четвертым октетом).

Применение метода VLSM позволяет использовать множество масок в одном адресном пространстве для получения разных сетей разных размеров. Этот метод дает возможность установить правильный размер каждой подсети в соответствии с конкретными требованиями адресации. Использование масок с переменной длиной позволяет преодолеть ограниченность IP-адресации, которая существует в классовой адресации (а также в некоторой степени в методе FLSM).

Маска подсети с переменной длиной дает большую свободу, чем маска с фиксированной длиной. Она позволяет распределить ресурсы IP-адресации в соответствии с потребностями подсетей, а не по какому-либо общему правилу. Возьмем, например, сеть Ethernet: чем больше число хостов в сети Ethernet, тем ниже ее производительность. Все хосты должны конкурировать за доступ к физической среде. Здесь нет порядка, регулирующего, в какой именно момент хост может передавать данные, поэтому вероятность возникновения конфликта между обращениями хостов возрастает с увеличением их количества.

Количество хостовых адресов в сети класса С может быть равно 254, но фактически производительность сети Ethernet начинает снижаться намного раньше того, как количество хостов достигает этого числа. Когда их число возрастает до какого-то определенного значения, становится более разумным создать несколько сетей, каждая из которых содержит ограниченное количество хостов. Проблема здесь заключается в том, что для каждой локальной сети потребуется множество адресов класса С, но использоваться будут только некоторые из числа доступных хостовых адресов.

Метод VLSM решает эту проблему посредством назначения разных масок для одного адресного пространства (в данном случае адреса класса С). Например, допустим, что компьютерная сеть под названием NETA начала свое существование как локальная сеть, включающая в себя семь устройств. Для нее назначен адрес класса С, емкость которого составляет 254 хоста. Со временем эта сеть расширилась до 72 хостов, но в то же время ее производительность упала настолько, что это стало серьезной проблемой. Сетевой администратор решает разбить эту сеть на три сети, которые логически объединяют те или иные рабочие функции, и соединить их между собой при помощи маршрутизатора. Разделение сети администратор выполняет по следующей схеме (табл. 3.6).

Таблица 3.6. *Пример трех подсетей*

ЛВС1	Бухгалтерия	14 пользователей
ЛВС2	Отдел программирования	28 пользователей
ЛВС3	Отделы продаж и маркетинга и администрация	30 пользователей

Теперь сетевой администратор должен решить следующее: имеется три сети и один адрес класса С. Необходимо либо использовать два дополнительных адреса, либо более эффективно использовать существующий адрес. Администратор выбирает последнее и применяет метод маски подсети с переменной длиной (VLSM). Он создает три подсети: одну с помощью маски, определяющей 14 хостов, и две других с использованием одной маски, определяющей до 30 хостов в каждой из них, как показано в таблице ниже (табл. 3.7).

Таблица 3.7. *Пример масок переменной длины*

Изначальный десятичный адрес с разделительными точками (класс С)	192.165.11.0	
Двоичное представление	11000000.10100101.00001011.00000000	

Таблица 3.7 (окончание)

Естественная маска (класс С)	11111111.11111111.11111111.00000000	маска 24 бит
Первая маска, определяющая биты 15 хостов	11111111.11111111.11111111.11110000	маска 28 бит
Вторая маска, определяющая биты 31 хоста	11111111.11111111.11111111.11100000	маска 27 бит

При помощи двух разных масок, состоящих из 28 и 27 бит (или 255.255.255.240 и 255.255.255.224), сетевой администратор сможет достичь цели. Теперь у него появилась возможность использовать единственный адрес класса С для создания трех разных подсетей, что более соответствует потребностям компании. При таком подходе появляются дополнительные сетевые адреса и уменьшается число используемых хостов.

Протокол разрешения адресов (ARP)

Мы рассмотрели IP-протокол и используемую в нем схему адресации, в которой каждый хост имеет уникальный адрес, состоящий из хостовой части и сетевой части. IP-пакет содержит IP-адреса источника и назначения. Маршрутизаторы, встречающиеся на пути движения пакета, читают адрес назначения и используют его для определения оптимального пути передачи пакета.

Независимо от того, где именно находится машина, для которой предназначен пакет, этот пакет должен переместиться внутри локальной сети от исходной машины к машине назначения или к маршрутизатору, если пункт назначения находится в другой локальной сети. Канальный уровень следит за перемещением пакета внутри локальной сети, однако на этом уровне различаются только аппаратные адреса. Как только пакет данных переходит с уровня 3 на уровень 2 — с сетевого уровня на канальный — информация об IP-адресе теряет свое значение с точки зрения работы канального уровня. Каким же образом может быть определен соответствующий аппаратный адрес машины назначения на канальном уровне? Для этого IP-адрес пункта назначения должен как-то преобразовываться в физический (аппаратный) адрес.

Проблема преобразования логического адреса в физический известна под названием проблемы "разрешения адресов". Существует два способа решения этой проблемы. Аппаратные адреса могут быть вручную закреплены за соответствующим целевым IP-адресом, либо его можно динамически определять при помощи протокола разрешения адресов (Address Resolution Protocol, ARP).

Для того чтобы вручную закрепить IP-адрес за аппаратным адресом в Windows, в командной строке наберите следующее:

```
arp -s ip-address hardware-address
```

Для того чтобы в Windows отобразить таблицы преобразования IP-адресов в физические адреса, просмотрите результат выполнения следующей команды:

```
arp -a
```

Динамическое определение адреса при помощи ARP-протокола

В большинстве локальных сетей составлять таблицу преобразования адресов вручную неудобно. Необходимо поддерживать такую таблицу на каждом хосте сети. Задача усложняется, если нужно учесть мост или маршрутизатор. При замене сетевых плат, добавлении новых устройств или изменении IP-адресов ситуация еще более усложняется. Намного удобнее находить эти адреса динамически.

Получив IP-адрес приемника, ARP-протокол позволяет определить физический адрес целевого хоста в рамках той же физической сети. Работа протокола основана на передаче всем хостам внутри локальной сети специального пакета с запросом к обладателю того или иного IP-адреса. При получении такого пакета обладатель IP-адреса сообщает свой физический адрес. Остальные хосты игнорируют запрос. При получении ответа хост, сделавший запрос, использует тот физический адрес, который был указан в нем, для передачи данных непосредственно на хост назначения. На рис. 3.9 этот процесс отображен схематически.

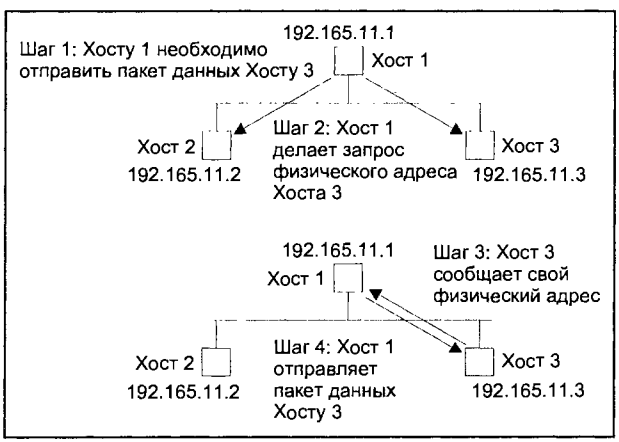


Рис. 3.9. Протокол разрешения адресов динамически определяет аппаратный адрес хоста назначения

Для уменьшения трафика ARP-протокол поддерживает кэш всех недавно определенных хостов. При помощи этого кэша процесс динамического определения адресов происходит только один раз, при первом взаимодействии между хостами. Если физический адрес уже известен, исходный хост отправляет данные, предварительно сверяясь с содержимым кэша. Прежде чем запустить процесс динамического поиска, компьютер всегда проверяет кэш ARP-протокола для связывания IP-адреса с аппаратным адресом.

После внесения какой-либо записи в кэш ARP-протокола, она там сохраняется в течение определенного периода времени. Этот период называется периодом устаревания (age timer), и он каждый раз начинает отсчитываться заново, если при получении ARP-пакета MAC-адрес и IP-адрес совпадают. По истечении заданного времени соответствующая запись стирается из ARP-кэша. В этом случае процесс определения физического адреса при помощи ARP-протокола должен быть повторен заново.

Обратное разрешение адресов

Обратное разрешение адресов (Reverse ARP, RARP) означает именно то, что и подразумевает — функцию, обратную той, которую выполняет протокол разрешения адресов (ARP-протокол). ARP-протокол служит для определения физического адреса, соответствующего известному IP-адресу. Протокол RARP выполняет прямо противоположное действие — он помогает определить IP-адрес по соответствующему аппаратному адресу.

На первый взгляд это может показаться странным. Разве может вообще возникнуть ситуация, когда аппаратный адрес известен, а IP-адрес — нет? RARP, как правило, применяется на рабочих станциях без жестких дисков. IP-адрес нельзя сохранить на машине без жесткого диска. Это создает проблему всякий раз, когда машина перезагружается. Один из способов разрешения этой проблемы состоит в том, чтобы аппаратно "зашить" IP-адрес в машину, но это не удобно, т. к. в случае изменения IP-адреса (например, при перемещении в другую сеть) требуется менять оборудование.

Вместо этого рабочая станция без жестких дисков использует функцию обратного разрешения адресов для получения своего адреса с сервера. Для того чтобы использовать эту функцию, требуется RARP-сервер, служащий для того, чтобы составлять таблицу соответствия IP-адресов и аппаратных адресов. Этот процесс происходит следующим образом.

1. Рабочая станция, не имеющая жестких дисков, делает RARP-запрос ко всем хостам, входящим в сеть.
2. Все хосты принимают посланный запрос, но отвечает только та машина, которая является RARP-сервером. RARP-сервер определяет, какой IP-адрес соответствует данному аппаратному адресу, и сообщает его в своем ответе.
3. Рабочая станция получает ответ и сохраняет IP-адрес в памяти. Протокол RARP не применяется повторно до тех пор, пока не произойдет перезагрузка рабочей станции.

Протокол динамической конфигурации хоста (DHCP)

Протокол динамической конфигурации хоста (Dynamic Host Configuration Protocol, DHCP) используется для динамического присваивания IP-адреса рабочей станции. Он является преемником более старого протокола, называемого *протоколом загрузки* (Bootstrap Protocol, BOOTP), который служил для той же цели. Сегодня протокол DHCP очень часто используется в IP-сетях.

Даже самые простые современные компьютеры оснащены каким-либо устройством хранения. На самом деле, чем больше емкость устройства, тем оно дешевле, поэтому даже типичный домашний ПК имеет запоминающее устройство емкостью в несколько гигабайтов. Однако возникает вопрос: если в большинстве случаев запоминающее устройство все-таки имеется, зачем тогда нужен протокол динамического присваивания IP-адресов? Ответ заключается в его удобстве.

Сегодня IP-протокол широко распространен, а люди стали настолько мобильными, что использовать фиксированные адреса им неудобно. В условиях возрастания количества портативных компьютеров намного удобнее применять схему, при которой происходит динамическое присваивание IP-адресов, чем схему, при которой требуется переконфигурирование каждый раз, когда пользователь соединяется с новой

сетью. Динамическое назначение IP-адресов защищает пользователя от необходимости знать, какая схема адресации используется в той или иной сети. Девиз сегодняшнего дня — Plug-and-Play, и протокол DHCP вполне отвечает ему.

Динамическое присваивание адресов также помогает уменьшить количество IP-адресов. Если адрес жестко закодирован, то он постоянно сохраняется за машиной, даже если она не находится в сети. При динамическом присваивании адресов машины владеют ими временно. После того как происходит отсоединение от сети, адрес освобождается и может быть использован другим пользователем.

Для транспортировки протокола DHCP используется UDP. Это намного эффективнее, чем RARP. В протоколе DHCP одно сообщение может специфицировать множество элементов, например, IP-адрес, адрес шлюза по умолчанию или маску подсети. Фактически одним сообщением можно передать всю необходимую для компьютера конфигурационную информацию.

Протокол DHCP полностью управляет процессом назначения адресов. При этом в зависимости от характеристик клиента или от того, из какой он сети, DHCP-сервер может применять разные методы.

В протоколе DHCP используются три типа назначения адресов.

- *Динамическое конфигурирование.* Распределяет адреса, предназначенные для владения в течение определенного периода времени. Компьютер может использовать такой адрес только до тех пор, пока период аренды адреса не закончится. Как правило, такой период составляет около трех дней, и по прошествии этого времени назначается новый адрес.
- *Ручное конфигурирование.* Позволяет администратору конфигурировать тот или иной адрес для конкретного компьютера.
- *Автоматическое конфигурирование.* Распределяет постоянные адреса при первом соединении компьютера с сетью.

Как работает протокол DHCP

Во время работы протокола DHCP хост проходит через шесть состояний.

1. *Инициализация* (Initialize). При загрузке хост входит в состояние инициализации. Для того чтобы начать использование протокола DHCP, хост должен стать DHCP-клиентом. Для этого он отправляет поисковое сообщение *DHCPDISCOVER*, при помощи которого выполняется поиск всех DHCP-серверов данной сети. После этого хост переходит во второе состояние.
2. *Выбор* (Select). В этом состоянии хост получает сообщения с предложением *DHCPOFFER*, которые отправляют DHCP-серверы, предназначенные для ответа на запросы данного типа клиентов. Если ни один сервер не сконфигурирован таким образом, чтобы он мог ответить на данный запрос, клиент не получает предложения о получении адреса. Если для ответа сконфигурировано несколько серверов, клиент получает несколько предложений. Каждое предложение содержит конфигурационную информацию. Клиент должен выбрать одно из предложений. После того как одно из предложений выбрано (например, первое из полученных предложений), клиент переходит в состояние согласования (negotiation), во время которого клиент и тот сервер, от которого это предложение было принято, согласуют между собой такие вопросы, как, например, продолжительность аренды ад-

реса. Для того чтобы перейти в это состояние, клиент отправляет сообщение *DHCPREQUEST*.

3. *Запрос* (Request). В этом состоянии сервер подтверждает прием запроса и начало передачи адреса в аренду при помощи отправки уведомляющего сообщения *DHCPACK*. После получения подтверждения *DHCPACK* клиент переходит в четвертое состояние.
4. *Связывание* (Bound). В этом состоянии клиент начинает использовать присвоенный ему адрес. Это состояние обычной работы клиента. Клиент может сохранить адрес и запросить его снова при перезапуске. Кроме того, протокол DHCP позволяет клиенту прекратить аренду адреса до того, как закончится установленный период аренды. Для прекращения аренды клиент отправляет на сервер сообщение *DHCPRELEASE*, после чего больше не может использовать данный адрес и должен вернуться в первое состояние. С арендой адреса связаны три таймера: таймер обновления (renewal timer), таймер повторного связывания (rebinding timer) и таймер истечения периода аренды адреса (expiration timer). Для таймера обновления по умолчанию принято значение, равное половине периода аренды адреса. Когда этот таймер останавливается, клиент отправляет сообщение *DHCPREQUEST*, в котором содержится текущий адрес и запрос на продолжение периода его аренды. В течение периода между отправкой запроса на продолжение аренды и получением ответа от сервера клиент переходит в пятое состояние.
5. *Обновление* (Renew). В этом состоянии клиент ждет ответа от сервера на запрос о продолжении аренды адреса. Если сервер соглашается продлить аренду, он отправляет подтверждающее сообщение *DHCPACK*, и клиент возвращается в связанное состояние. В противном случае сервер отправляет сообщение *DHCPNACK*, которое вынуждает клиента вернуться в первоначальное состояние инициализации. Если же клиент не получает ответа в течение периода времени, определенного таймером повторного связывания и составляющего приблизительно 87,5% от периода аренды, клиент переходит в шестое состояние.
6. *Повторное связывание* (Rebind). Клиент переходит в это состояние, если он не получает ответа от DHCP-сервера. В этом состоянии клиент считает, что DHCP-сервер недоступен, и начинает передавать сообщения *DHCPREQUEST* для любого DHCP-сервера. Если какой-либо сервер отвечает клиенту и подтверждает его запрос на продление периода аренды, клиент возвращается в состояние связанности (Bound). Если же запрос не подтверждается, клиент возвращается в состояние инициализации (Initialize).

В случае возникновения ситуации, при которой клиент остается в состоянии повтора (Rebind) из-за того, что ни один из DHCP-серверов не доступен, клиент переходит обратно в состояние инициализации (Initialize) по окончании работы третьего таймера — таймера завершения периода аренды.

Динамическая межсетевая маршрутизация

Теперь мы понимаем, как пакет данных перемещается от одного хоста к другому внутри какой-либо сети. Для этого сначала должен быть определен физический адрес, соответствующий IP-адресу. Затем пакеты перемещаются в виде кадров с канального уровня в физическую среду. Целевой хост получает кадры с сетевого кабеля, отбрасывает информацию об аппаратных адресах и управляющую информацию канального уровня, и отправляет пакеты на сетевой уровень. Сетевой уровень,

в свою очередь, отделяет специфическую информацию этого уровня и передает пакет далее на транспортный уровень. Транспортный уровень сравнивает порядковый номер пакета с тем номером, который ожидает получить. В зависимости от протокола, транспортный уровень может отправлять подтверждения. После этого данные передаются протоколам верхних уровней для выполнения соответствующей обработки.

В нескольких последующих абзацах мы рассмотрим, каким образом пакет данных перемещается между сетями, и какую роль в этом процессе играют протоколы динамической маршрутизации. Как уже говорилось, *подробное обсуждение протоколов маршрутизации выходит за рамки этой главы и будет изложено в гл. 14.* Однако здесь мы вкратце опишем, что они собой представляют и что делают в контексте сетевых протоколов.

Основные функции маршрутизатора

С точки зрения отправителя порядок пересылки пакета на хост, находящийся в другой компьютерной сети, тот же самый, как и при пересылке на хост в пределах сети отправителя. Единственное различие состоит в том, что в этом процессе используется маршрутизатор, который позволяет получить пакет в одном физическом сегменте сети и передать его на другой физический сегмент. Передающий хост также должен определить, находится ли хост назначения в этой же самой сети или в другой, для чего выполняется сравнение сетевого адреса хоста назначения с сетевым адресом хоста отправки. Если эти адреса совпадают, отправитель знает, что целевой хост находится в этой же сети, и передает пакет непосредственно на этот хост. Данный процесс называется прямой доставкой (direct delivery).

Если эти два адреса не совпадают, тогда передающий хост знает, что хост назначения находится в другой физической сети и для передачи пакета требуется маршрутизатор — такая передача называется непрямой (indirect delivery). Это также означает, что передающий хост должен знать адрес маршрутизатора в той локальной сети, в которую будут отправлены пакеты. Маршрутизатор называется шлюзом по умолчанию (default gateway), если на его адрес хост отправляет все пакеты, не имеющие прямых маршрутов. Адрес шлюза по умолчанию может быть сконфигурирован вручную или может определяться при помощи протокола DHCP.

Маршрутизатор по определению выполняет только функции, относящиеся к уровням 1—3, а именно:

1. Получает кадр с физического сегмента сети.
2. Отделяет информацию, связанную с канальным уровнем, и читает сетевой адрес машины назначения.
3. Использует сетевой адрес для определения того выходного интерфейса, который необходим для передачи пакета на машину назначения.
4. Преобразует сетевой адрес следующего транзита (hop, прыжок), т. е. хоста назначения или другого маршрутизатора, в аппаратный адрес при помощи процесса разрешения адресов (ARP) или кэша этого процесса.
5. Подготавливает кадр для передачи по физической среде. Физический адрес назначения — это адрес следующего транзита, который может быть машиной назначения или другим маршрутизатором.
6. Отправляет кадр при помощи соответствующего выходного интерфейса.

Обратите внимание на то, что в предшествующих объяснениях нигде не был упомянут какой-либо конкретный протокол. Основная функция маршрутизатора не зависит от используемого набора протоколов. При рассмотрении других сетевых протоколов мы опять вспомним о маршрутизаторах. И там будет отмечено, что процесс перемещения пакета через сеть, а также основные функции маршрутизатора всегда остаются одинаковыми, независимо от особенностей того протокола, о котором пойдет речь.

За пределами локальной сети

Маршрутизаторы используются для соединения между собой разных сетей. Если хост назначения расположен за пределами локальной сети, необходим маршрутизатор, который позволяет определить путь от одной сети к другой. Для этого маршрутизаторы должны знать, с какими локальными сетями они связаны и какие сети расположены за ними. Сведения об окружающих локальных сетях получить легко, поскольку маршрутизаторы соединены с ними непосредственно. Однако дело усложняется, если хост назначения находится в сети, которая отделена от маршрутизатора несколькими другими сетями.

Маршрутизаторам необходимо сообщить о тех сетях, которые не связаны непосредственно с ним, но доступны через другие маршрутизаторы. Это достигается при помощи создания статических маршрутов или применения протокола динамической маршрутизации. Такие протоколы служат для динамического (т. е. в реальном времени) определения оптимального маршрута для передачи пакета из одной сети в другую. Эти протоколы позволяют описать схему взаимосвязей между сетями и отслеживать области ненадежного сетевого обмена.

Протоколы маршрутизации "видят" объединенную сеть как единую схему и способны определять наиболее подходящий путь на основе этой схемы, а также сведений о текущей обстановке во всем сетевом комплексе. Для определения оптимального пути между двумя хостами протоколы маршрутизации, как правило, используют алгоритмы двух основных категорий: дистанционно-векторный алгоритм (distance vector protocols) и алгоритм состояния связей (link state protocols).

Дистанционно-векторные протоколы (например, RIP) определяют наилучший путь между двумя хостами по расстоянию между ними. Расстояние измеряется в количестве транзитных маршрутизаторов (hops, прыжков) между пунктом отправки и пунктом назначения и не зависит от таких вещей, как, например, длина линии передачи.

Протоколы состояния канала, например, OSPF (Open Shortest Path First — первоочередное открытие кратчайших маршрутов) и IS-IS (Intermediate System to Intermediate System — связь между промежуточными системами) определяют наилучший путь на основе нескольких факторов, в том числе длины и состояния линий передачи между двумя хостами. Из двух путей, один из которых включает в себя три транзита, связанных при помощи DS3-линий (Digital Signal n — обозначение скорости передачи данных по цифровой выделенной линии), а другой — два транзита, связанных при помощи 56-килобитовых линий, протокол состояния канала выберет первый путь (с тремя транзитами), тогда как дистанционно-векторный протокол выберет второй. Другими словами, протоколы состояния канала основаны на предпочтении более скоростных линий передачи.

Независимо от типа протокола маршрутизации, все они способны определять множество разных путей для передачи данных между сетями. Кроме того, некоторые

протоколы маршрутизации (например, OSPF) фиксируют все маршруты, но в таблицу перенаправления (forwarding table) маршрутизатора вносят только самые успешные из них. Таблица перенаправления используется маршрутизатором для определения того, какой интерфейс он должен использовать, чтобы передать пакет данных. Записи для таблицы перенаправления могут быть взяты из таблицы маршрутизации или из назначенных вручную путей при использовании статических маршрутов.

Протокол IPX/SPX

Протокол межсетевого пакетного обмена (IPX) — это протокол уровня 3, который используется в сетях Novell NetWare и служит для обмена данными внутри сети. Он был разработан компанией Novell в начале 1980 годов на основе протокола XNS, разработанного компанией Xerox. В конце 1980 и начале 1990 годов IPX-протокол имел наибольшее распространение в локальных компьютерных сетях.

Протокол последовательного обмена пакетами (SPX) — это протокол с установлением логических соединений (connection-oriented protocol), который работает на транспортном уровне OSI-модели. SPX-протокол обеспечивает надежность доставки пакета данных внутри сети. Так же, как и протокол TCP, он отвечает за повторную передачу потерянных пакетов и использует IPX-протокол для продвижения пакетов.

Так же, как и IP-протокол, протокол IPX работает на уровне 3 модели OSI и требует использования такой схемы адресации, которая позволяет различать между собой узлы разных сетей. Этот протокол также требует того, чтобы каждый узел имел уникальный адрес.

IPX-адрес представляется в шестнадцатеричном формате и состоит из двух частей: сетевого номера и номера узла. Сетевая часть адреса имеет длину в 32 бита, а узловая часть, как и хостовая часть в IP-адресе, — 48 бит. Сетевой администратор определяет сетевой адрес, тогда как узловой адрес представлен MAC-адресом сетевой платы. Приведем пример сетевого и узлового адреса по протоколу IPX:

CA1A20B0.0000.0a5d.ace0

Использование MAC-адреса в качестве узлового адреса избавляет от необходимости того, чтобы протокол разрешения адресов связывал адреса уровня 2 с адресами уровня 3. Кроме того, MAC-адрес позволяет машине-отправителю отсылать пакет на машину назначения непосредственно, используя только узловой адрес, указанный в поле назначения в протоколе MAC.

В протоколе IPX также используется понятие *внутреннего сетевого адреса* (internal network address). Этот термин применяется для описания логической или виртуальной сети внутри каждого сервера (версии 3.x и 4.x). Внутренняя сеть отличается от реальной, которая имеет непосредственное отношение к существующей физической сети или ее кабельной системе. Внутренний сетевой номер используется для объявления (извещения) о службах сервера.

Инкапсуляция в протоколе IPX

Инкапсуляция описывает то, каким образом протоколы верхних уровней пакуются в кадры на канальном уровне для последующей передачи по кабелю. Протокол IPX позволяет определить множество типов инкапсуляции в пределах одной физической

сети. Инкапсуляция — довольно важное понятие для сетей с применением IPX-протокола, т. к. каждый тип инкапсуляции рассматривается как отдельная сеть в пределах одного физического кабельного сегмента.

Именно в этой области происходит множество ошибок. Если используется множество типов инкапсуляции на одном физическом сегменте, тогда каждый тип инкапсуляции должен иметь свой собственный сетевой адрес. Однако проблема состоит в том, что для выполнения маршрутизации между сетями необходим маршрутизатор, поэтому клиент, использующий один тип инкапсуляции, может взаимодействовать с сервером, находящимся на том же сегменте, использующем другой тип инкапсуляции, только одним путем — при помощи маршрутизатора. Для этого в интерфейсе маршрутизатора должны быть определены оба типа инкапсуляции.

Компания Novell использует четыре разных метода инкапсуляции для сетей типа Ethernet.

- Метод, разработанный собственно компанией Novell. Этот метод также называется 802.3 raw (сырой) или Novell Ethernet_802.3. В этом методе IPX-пакеты помещаются непосредственно в кадры без использования 802.2 LLC или SNAP. В маршрутизаторах компании Cisco этот тип инкапсуляции обозначается как NOVELL-ETHER.
- Ethernet version II. Этот метод еще называется Ethernet II и состоит из стандартного заголовка протокола Ethernet версии II (Ethernet version II), за которым следует поле типа. Код типа равен 8137. Структура кадра идентична той, которая используется в собственном методе компании Novell за исключением того, что поле типа используется вместо поля длины. В маршрутизаторах компании Cisco этот тип инкапсуляции обозначается как ARPA.
- 802.3. Этот метод также называется Novell_802.2. Здесь используется формат кадра стандарта IEEE 802.3. Это наиболее распространенный метод в серверах Netware 3.12 и Netware 4.x. В маршрутизаторах компании Cisco этот тип инкапсуляции обозначается как SAP.
- SNAP. Этот метод также называется Ethernet_SNAP. В нем расширяется заголовок 802.2 за счет добавления поля типа. Этот метод редко используется. В маршрутизаторах компании Cisco этот тип инкапсуляции обозначается как SNAP.

Извещение о службах сервера

В сетях IPX серверы извещают о тех службах, которые они предоставляют. Поэтому этот протокол иногда называют "болтливым". Объявление служб выполняется посредством протокола SAP (Service Advertising Protocol — протокол извещения об услугах), при помощи которого сетевые ресурсы, например, файловые серверы и серверы печати могут сообщать свои адреса и извещать о своих службах.

Протокол SAP отправляет извещения о службах каждые 60 сек., а каждая служба обозначается при помощи специального идентификатора — шестнадцатеричного номера, описывающего тип службы. Маршрутизаторы составляют список служб и соответствующие им сетевые адреса, которые являются внутренними или виртуальными сетевыми адресами, обсуждаемыми выше. Эту SAP-таблицу маршрутизаторы рассылают каждые 60 сек. Важно отметить, что IPX-серверы, по существу, выполняют функцию маршрутизации, и поэтому действуют как маршрутизаторы.

Клиенты, которым требуется та или иная служба, делают запрос на нее, а маршрутизаторы отвечают на этот запрос, сообщая сетевой адрес требуемой службы. После этого клиент направляет свой запрос непосредственно по тому адресу, с которого служба объявлялась. В табл. 3.8 приводится список наиболее распространенных идентификаторов служб.

Таблица 3.8. *Примеры идентификаторов, применяемых в протоколе SAP*

Десятичное значение	Шестнадцатеричное значение	Описание
3	0003	Очередь заданий на печать или группа печати
4	0004	Файловый сервер (SLIST-источник)
6	0006	Шлюз
7	0007	Печатный сервер или бесшумный печатный сервер
32	0020	NetBIOS
36	0024	Удаленная служба маршрутизации или мостовая служба
39	0027	Шлюзовой сервер TCP/IP
45	002d	Сервер синхронизации или асинхронный таймер
71	0047	Объявляющий печатный сервер
274	0112	Печатный сервер (HP)
619	026b	Сервер синхронизации (Netware 4.x)
632	0278	Сервер каталогов (Netware 4.x)
807	0327	Диагностика средств Microsoft

Маршрутизация IPX-пакетов

Маршрутизация IPX-пакетов в пределах локальной сети осуществляется довольно просто благодаря тому, что нет необходимости преобразовывать узловой адрес в MAC-адрес — эти адреса совпадают, и поэтому службы канального уровня могут выполнять соответствующую инкапсуляцию, используя узловой адрес в поле адреса назначения MAC-адреса.

Что касается внутренней сети, то здесь для протокола IPX требуется протокол маршрутизации. Так же, как и в IP-протоколе, в IPX для маршрутизации может применяться дистанционно-векторный алгоритм или алгоритм состояния связи. В качестве дистанционно-векторного протокола используется протокол маршрутной информации RIP (Routing Information Protocol), но его логика расчета расстояния отличается от применяемой в протоколе RIP для IP. Прежде всего считаются "тики" (ticks), а затем транзиты (hops). Тик составляет около 1/18 секунды и служит в качестве меры задержки. Последовательная линия равна шести тикам, а Ethernet-линия — одному тику. Выбирается та линия, которая имеет наименьшее количество

тиков. При одинаковом количестве тиков определяется число транзитов. Протокол IPX RIP объявляет всю таблицу маршрутов каждые 60 сек.

Протокол состояния связи, используемый в протоколе IPX, называется протоколом коммуникационных услуг (Novell Link-Services Protocol, NLSP). Он был разработан компанией Novell для того, чтобы преодолеть ограничения протоколов IPX RIP и SAP. Этот протокол основан на протоколе связи между промежуточными системами (протокол OSI Intermediate System-to-Intermediate System, IS-IS) и предназначен для того, чтобы заменить протоколы RIP и SAP, особенно в больших интерсетях, где они особенно неэффективны.

Протокол AppleTalk

AppleTalk — это стек протоколов, который был разработан фирмой Apple в начале 1980-х годов. Существует две версии AppleTalk: AppleTalk Phase I и AppleTalk Phase II. Версия AppleTalk Phase I была разработана для небольших рабочих групп и не имеет возможностей для работы с большой сетью. Количество хостов, которые может поддерживать сеть AppleTalk Phase I, ограничивается 135. В версии AppleTalk Phase II это число расширяется до 253 на одном сегменте, что позволяет поддерживать сеть больших размеров.

Как и стек протоколов Интернет, стек протоколов AppleTalk охватывает большую часть семиуровневой OSI-модели, что показано на рис. 3.10. Зная функции каждого уровня OSI-модели, вы можете оценить, какие типы функций выполняются каждым из протоколов AppleTalk.

Сокеты, зоны, узлы и сети

В сети AppleTalk используется иерархическая структура, состоящая из сокетов, узлов, сетей и зон.

Сокеты AppleTalk

Сокет, в сущности, имеет ту же функцию, что и порт в TCP. Это точка логического соединения между протоколом AppleTalk третьего уровня и верхнеуровневыми функциями AppleTalk. Функции верхних уровней называются сокет-клиентами. Сокет-клиент может иметь один или несколько сокетов, которые используются для передачи дейтаграмм. В основном, сокеты назначаются динамически посредством протокола передачи дейтаграмм (Datagram Delivery Process, DDP). Протокол DDP относится к третьему уровню и работает во многом так же, как протоколы маршрутизации RIP или OSPE. Сокет имеет 8-битовый номер.

Зоны AppleTalk

Зоны AppleTalk — это логические объединения узлов и сетей. Сетевой администратор конфигурирует зоны внутри сети AppleTalk. Как видно на рис. 3.11, для того чтобы принадлежать к одной зоне, сети и узлы не обязательно должны быть смежными.

Узлы AppleTalk

Узел AppleTalk — это устройство, которое присоединяется к сети AppleTalk. Внутри узлов существуют сокеты, которые идентифицируют разные программные процессы.

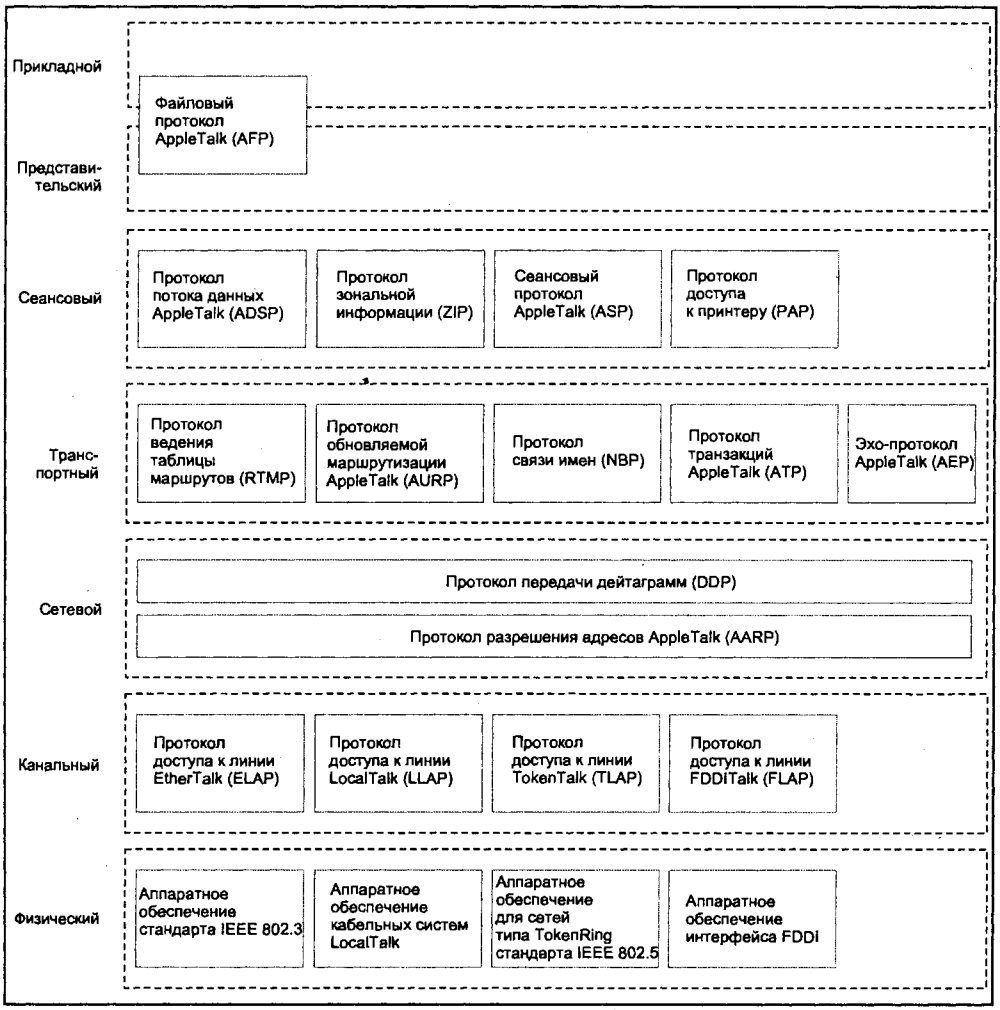


Рис. 3.10. Стек протоколов AppleTalk и OSI-модель

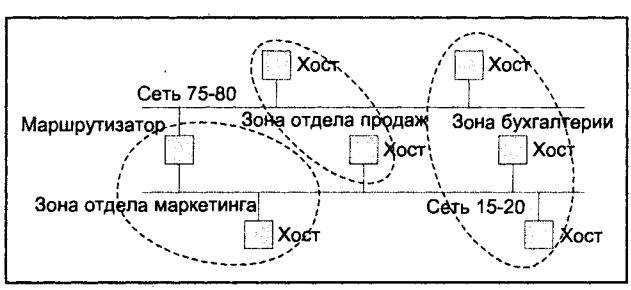


Рис. 3.11. Сеть AppleTalk с зонами, узлами и кабельными диапазонами

Как и в сетях IP и IPX, узел принадлежит к одной сети и одной зоне. Адрес узла определяется 8-разрядным номером.

Сети AppleTalk

Сеть AppleTalk — это локальный сетевой сегмент, который управляется протоколом AppleTalk. Длина адреса сети AppleTalk составляет 16 бит. В отличие от сетей IP, в сети AppleTalk используется понятие расширенной (extended) и нерасширенной (nonextended) сети.

Нерасширенная сеть — это физический сетевой сегмент, которому назначен один сетевой номер в диапазоне между 1 и 1024. Узлы внутри нерасширенной сети должны иметь уникальные адреса. Кроме того, внутри нерасширенной сети не может быть больше одной зоны.

Расширенная сеть — это такая сеть, в которой физический сетевой сегмент может иметь множество последовательных сетевых номеров. Такой подход подобен тому, который применяется в IPX-сетях, где один сегмент может иметь несколько разных типов инкапсуляции, каждый из которых имеет свой собственный сетевой номер. В сетях AppleTalk физический сегмент, который имеет более одного сетевого номера, определяется как кабельный диапазон. Узлы в расширенной сети также должны иметь свои уникальные адреса. Сочетание узлового адреса с сетевым адресом дает уникальное обозначение, идентифицирующее конкретный узел в конкретной сети.

В расширенной сети можно сконфигурировать множество зон, и узел в любой из сетей на данном сегменте может принадлежать какой-либо одной зоне. Рис. 3.11 иллюстрирует понятия кабельных диапазонов, зон и узловых адресов.

Назначение адресов

В большинстве сетей AppleTalk адреса назначаются динамически при первом присоединении к сети. Адрес AppleTalk состоит из 16-разрядного сетевого адреса, 8-битового узлового адреса и 8-разрядного сокетного номера.

При первом запуске узла AppleTalk ему назначается временный сетевой адрес из зарезервированного диапазона между 65 280 и 65 534. Узловой адрес выбирается случайно. Затем узел устанавливает связь с маршрутизатором сети и запрашивает у него доступный кабельный диапазон на том сегменте, к которому этот узел присоединен. Маршрутизатор сообщает, какой диапазон доступен, и узел выбирает из этого диапазона какой-нибудь номер. После этого узел передает в сеть специальное сообщение, чтобы проверить, не занят ли выбранный узловой адрес. Если в ответ не поступает никакого сообщения, значит этот адрес может использоваться. Если поступает ответ о том, что этот адрес занят, процесс повторяется сначала, до тех пор, пока узел не находит свободный номер.

Функционирование узла начинается после назначения сетевого и узлового адреса. Как и протокол IP, протокол AppleTalk использует отдельный протокол для определения связей между физическим аппаратным адресом и сетевым, узловым или сокетным адресом. Он называется протоколом разрешения адресов AppleTalk (AppleTalk Address Resolution Protocol, AARP). После того как адрес назначен, он сохраняется в таблице отображения адресов (Address Mapping Table, AMT), которая выполняет ту же функцию, что и кэш в протоколе ARP в стеке протоколов IP. Каждая запись в таблице отображения адресов снабжается таймером, который обновля-

ется, если новый пакет поступает вместе с соответствующим связыванием. По завершении срока таймера запись удаляется из таблицы.

Дополнительные ресурсы

Поиск неисправностей TCP/IP-соединения в Windows 2000 или Windows NT:
http://support.microsoft.com/default.aspx?scid=kb;EN-US;q102908.

Поиск неисправностей в сетях Novell IPX:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1908.htm.

Руководство пользователя по TCP Windows:
http://www.ncsa.uiuc.edu/People/vwelch/net_perf/tcp_windows.html.

FAQ по интерсетям Campus IPX: **http:// www.net.berkley.edu/dcns/faq/ipxfaq.html**.

Технические советы по локальным компьютерным сетям (Cisco):
http://www.cisco.com/warp/public/473.

Протокол TCP/IP (Cisco): **http:// www.cisco.com/warp/public/535/4.html**.

Сравнение сетевых протоколов Windows NT:
http://support.microsoft.com/default.aspx?scid=kb;EN-US;q128233.

Общие сведения о протоколе DHCP:
http://hotwired.lycos.com/webmonkey/00/39/index3a.html?tw=backend.

Введение в Интернет: **http://www.historyoftheinternet.com/chap4.html**.

Введение в протоколы Интернета:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm.

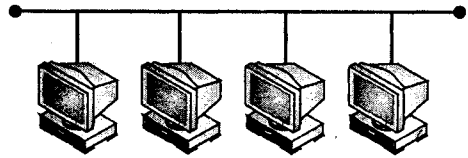
Сетевые калькуляторы: **http://www.telusplanet.net/public/sparkman/netcalc.htm**.

Сетевые ресурсы на сайте **http://www.subnetonline.com/**.

Учебник по маршрутизации в протоколах TCP/IP и IPX:
http://www.sangoma.com/fguide.htm.

Драйверы для сетевого обмена через USB-интерфейс:
http://www.mcci.com/mcci-v3/14_usb_networking_dirvers.html.

Применение сетевых технологий PPP, SLIP и Dial-Up:
http://world.std.com/about/ppp-setup.shtml.



ГЛАВА 4

Сетевые операционные системы

Как было сказано в *гл. 1*, в компьютерных сетях персональные компьютеры могут взаимодействовать с другими сетевыми устройствами посредством кабельной системы и устройств связи. Однако одного аппаратного обеспечения недостаточно для работы сети. Для организации безопасного совместного использования файлов и оборудования серверам и рабочим станциям нужна операционная система (ОС), а для обмена информацией внутри сети требуется протокол (или язык), принятый в качестве стандарта. В этой главе мы объясним роль сетевой ОС и изучим основные свойства наиболее распространенных систем этого типа.

Сетевые операционные системы

Компьютерные сети — это нечто более сложное, чем группа ПК, соединенных кабелями и устройствами связи. Основная задача компьютерных сетей состоит в том, чтобы обеспечивать совместное использование ресурсов (приложений, файлов, сообщений, принтеров, сканеров и т. д.) между этими ПК. Такое совместное использование требует операционной системы (программного обеспечения), способной управлять множеством файлов и устройств, существующих в рамках этой компьютерной сети, и в то же время обеспечивать защиту этих ресурсов от несанкционированного использования. В этом заключается роль *сетевой операционной системы (СОС)*. В этой части главы мы дадим общие понятия о СОС и опишем некоторые их свойства, которые отличают их от автономных операционных систем.

Средства поддержки сетевого режима

Прежде всего нужно понять способ, каким СОС обеспечивают поддержку сетей. Некоторые версии СОС просто добавляют сетевые компоненты поверх той операционной системы, которая уже установлена в персональном компьютере, тогда как другие версии полностью интегрируют сетевую поддержку в операционную систему компьютера, поэтому наличие автономной операционной системы в этом случае не требуется. Наверное, операционные системы NetWare 4.x и 5.x фирмы Novell являются самыми известными и распространенными примерами СОС, в которых средства поддержки сетевого режима в клиентском компьютере добавляются поверх уже установленной ОС. Это означает, что настольному компьютеру необходимы *обе* опе-

рационные системы, для того чтобы он мог выполнять как внутренние, так и сетевые функции. Однако большинство операционных систем все же изначально содержат в себе средства сетевой поддержки, например: Windows 2000 Server, Windows 2000 Professional, Windows NT Server, Windows NT Workstation, Windows 98, Windows 95 и MacOS. Хотя эти интегрированные операционные системы имеют свои преимущества, они не исключают использование других версий СОС. Следует иметь в виду, что оба подхода имеют свои уникальные преимущества и недостатки, о чем будет идти речь далее в этой главе.

Средства поддержки многозадачного режима

Компьютерная сеть — довольно оживленное место, поэтому пользователям часто приходится ожидать получения доступа (хотя такое ожидание может длиться в течение всего лишь нескольких миллисекунд), пока сервер обрабатывает одну задачу за раз. Если бы сервер мог выполнять одновременно несколько задач, производительность компьютерной сети значительно повысилась. *Многозадачная* ОС позволяет серверу обрабатывать более чем одну задачу за один раз, и в принципе многозадачная операционная система должна выполнять столько задач, сколько есть процессоров. Например, если сервер имеет четыре процессора, то многозадачная ОС должна обрабатывать четыре задачи одновременно. Однако, как правило, число задач превышает число процессоров, и поэтому компьютер должен распределять мощности процессоров между задачами, поочередно выполняя каждую из них в течение какого-то времени до их полного выполнения. При таком подходе все выглядит так, как будто компьютер выполняет несколько задач одновременно. Существует две основные формы многозадачности.

- *Многозадачный режим с приоритетами* (preemptive multitasking). В этом режиме операционная система может получить контроль над процессором без всякого взаимодействия с задачами. Такой подход часто оказывается более гибким для сетей, т. к. система с приоритетом, при необходимости, может в любой момент переключить активность процессора с локальной задачи на сетевую.
- *Бесприоритетный многозадачный режим* (nonpreemptive multitasking). В этом режиме задача сама определяет, когда процессор может прекратить ее обслуживание. Программы, написанные для систем с бесприоритетным многозадачным режимом, должны предусматривать механизмы взаимодействия с процессором. Никакая другая программа не может выполняться до тех пор, пока текущая программа не освободит процессор. Этот режим еще называется *кооперативной (совместной) многозадачностью* (cooperative multitasking).

Примечание

Многозадачный режим с приоритетами используется чаще всего и является наиболее широко используемой формой многозадачности благодаря своей гибкости.

Основные сведения о сетевой межоперабельности

Другой важной характеристикой СОС является *межоперабельность* (interoperability, способность к взаимодействию) — способность компьютерных операционных систем функционировать и обращаться к ресурсам в разных сетевых средах. Это особенно важно для неоднородных сетевых сред, содержащих системы разных произво-

дителей. Например, сервер NetWare может взаимодействовать с серверами Windows NT, а пользователи компьютеров Apple могут взаимодействовать как с серверами NetWare, так и с серверами Windows NT. В каждой СОС способность к взаимодействию достигается разными путями, поэтому прежде чем оценивать какую-то операционную систему, следует сначала определить, каким требованиям межоперабельности должна отвечать ваша сеть. Одноранговые сети имеют относительно низкую безопасность (т. к. в таких сетях управление безопасностью производится на каждом ПК) и невысокий уровень межоперабельности из-за ограничений, присущих этой архитектуре. Серверные сети, напротив, обладают более высокой степенью безопасности и межоперабельности.

Сторона сервера или сторона клиента

Также вам следует определить, как будет обеспечиваться межоперабельность на каждом сетевом компьютере: как служба сервера или как клиентское приложение. С сервера ей управлять легче, поскольку в таком случае служба становится централизованной (как и другие службы). Если же межоперабельность обеспечивается со стороны клиента, то требуется установить и настроить соответствующее ПО на каждом ПК, что, естественно, может значительно усложнить управление. На практике часто можно встретить тот случай, когда оба метода одновременно используются в одной сети в виде сетевой службы на сервере и сетевого клиентского приложения на каждом компьютере. Например, в Microsoft Windows межоперабельность достигается за счет установки сетевого клиентского приложения на каждом ПК.

Примечание

Редко бывает, чтобы обеспечение межоперабельности выполнялось только с одной из сторон: клиентской или серверной. В большинстве случаев эти средства применяются одновременно с *обеих* сторон (клиентской и серверной).

Программное обеспечение клиента и сервера

Обычно ОС компьютера организует и контролирует взаимодействие между его аппаратным обеспечением и тем программным обеспечением, которое на нем работает (т. е. приложениями). Операционная система управляет оперативной памятью (распределение и использование), процессором, доступом к запоминающим устройствам (чтение и запись) и периферийными устройствами (видеокарта, клавиатура, мышь, порты ввода/вывода и т. д.). В сетях с клиент-серверной архитектурой процесс управления и организации усложняется, и можно видеть, что ОС клиента и сервера несколько отличаются друг от друга. Сетевое ПО сервера предназначено для того, чтобы предоставлять ресурсы сетевым клиентам, а сетевое ПО клиента — для того, чтобы делать эти ресурсы доступными для клиентского компьютера. Работа серверной и клиентской операционных систем координируется таким образом, чтобы все части компьютерной сети нормально функционировали. Кроме того, клиент-серверное ПО обеспечивает безопасность, управляя доступом к данным и периферийным устройствам.

Клиентское программное обеспечение

На автономно работающем ПК пользователь набирает команду, которая приказывает компьютеру выполнить какую-то задачу. Процессор обрабатывает этот приказ.

Например, если вы хотите увидеть перечень файлов каталога, расположенного на одном из локальных жестких дисков, процессор интерпретирует и выполняет соответствующую команду и затем отображает на экране результаты в виде перечня файлов каталога. Несколько по-иному это происходит в сети, когда пользователь запрашивает какой-либо ресурс, находящийся на сервере в другой части сети. Запрос должен быть направлен (или перенаправлен) от клиента в сеть, а оттуда на сервер с затребованными ресурсами. Это выполняется при помощи *редиректора* (redirector). Редиректор иногда называют оболочкой (shell) или запросчиком (requester), в зависимости от используемого сетевого программного обеспечения. Редиректор — это небольшой сектор кода внутри СОС, который перехватывает запросы в компьютере и определяет, как следует с ними поступить: выполнить на локальной машине или перенаправить через сеть на другой компьютер или сервер.

Когда пользователь делает запрос на какой-либо сетевой ресурс или службу, в клиентском компьютере стартует переадресация этого запроса. Компьютер пользователя называется *клиентом* потому, что он делает запрос к серверу. Этот запрос перехватывается редиректором и направляется в сеть. Сервер обрабатывает запрос, направленный редиректором клиента, и предоставляет ему доступ к запрошенным ресурсам. Таким образом, сервер выполняет запрос клиента. Благодаря редиректору клиент может не беспокоиться о том, где находятся те данные или устройства, которые он запрашивает, или о том, как установить с ними связь. Чтобы получить доступ к данным, находящимся в каком-либо из сетевых компьютеров, пользователю нужно только набрать обозначение диска, на котором ресурс находится, а редиректор сам определит фактический маршрут.

Такой метод дает немало серьезных преимуществ. Предположим, что вы хотите запросить содержимое разделяемого каталога, на использование которого у вас есть разрешение. При работе в Windows NT вы можете воспользоваться Windows Explorer (Проводник) и, щелкнув на пиктограмме **Network Neighborhood** (Мое сетевое окружение), подключиться к сетевому диску. Вы можете также установить соответствие для дисковода (*drive mapping* — назначение буквы алфавита или имени дисководу с тем, чтобы операционная система или сетевой сервер знали о его местонахождении). Для этого щелкните правой кнопкой мыши на пиктограмме каталога в **Network Neighborhood** и выберите команду **Подключить сетевой диск...** Появится диалоговое окно, при помощи которого вы сможете назначить диску одну из доступных букв алфавита в качестве его обозначения (например, G:). После этого вы сможете обращаться к разделяемому каталогу с удаленного ПК как к диску G:, а редиректор будет знать о его местонахождении. Редиректор следит за тем, какие обозначения имеют те или иные сетевые ресурсы.

Редиректоры могут посылать запросы как к периферийным устройствам, так и к совместно используемым каталогам. С компьютера-инициатора запрос направляется через сеть к цели. Например, в качестве цели может выступать сервер печати, управляющий работой принтера. Через редиректор порты LPT1 и COM1 могут обращаться не к локальным, а к сетевым принтерам. Редиректор перехватит любое задание на печать, поступившее на порт LPT1, и направит его из клиентской машины на сетевой принтер.

Серверное программное обеспечение

Благодаря серверному сетевому ПО с клиентских компьютеров можно совместно использовать данные и устройства сервера (в том числе принтеры, плоттеры, катало-

ги и т. д.). Предположим, пользователь запрашивает список файлов каталога, расположенного на совместно используемом удаленном жестком диске. Запрос направляется редиректором в сеть, а затем передается на сервер управления файлами и печатью, который содержит разделяемый каталог. Запрос удовлетворяется, и на клиентский компьютер отправляется перечень файлов каталога.

Простыми словами, серверное сетевое программное обеспечение позволяет совместно и безопасно использовать ресурсы. *Совместное использование* (sharing) — это термин, обозначающий ресурсы, доступные для пользователей компьютерной сети. Большинство СОС не только обеспечивают совместное использование, но и определяют степень доступности ресурсов. Серверное ПО позволяет устанавливать различные уровни доступа для разных ресурсов (т. е. пользователи с большим доступом могут получить больше ресурсов). Кроме того, программы сервера координируют доступ таким образом, что два клиента не могут пользоваться одним и тем же ресурсом одновременно. Например, представим себе, что офис-менеджер хочет ознакомить каждого клиента сети с некоторым документом. Документ нужно поместить на сервер для совместного использования, а доступ к нему отрегулировать так, чтобы все пользователи могли его читать, и лишь те из них, кто имеет достаточный уровень доступа, смогли его редактировать.

Сетевые операционные системы также обеспечивают систему безопасности, предоставляя сетевому администратору возможность определять, какие пользователи (или их группы) могут получить доступ к сетевым ресурсам. При помощи серверного ПО администратор может создавать пользовательские права доступа (privileges, полномочия), определяющие, кто становится обладателем сетевых ресурсов. Администратор предоставляет указанные полномочия в виде разрешений или запретов, а также исключает пользователей из списка авторизованных пользователей. Сетевой администратор может организовывать пользователей в группы и назначать полномочия для этих групп, а не для отдельных пользователей. В таком случае все участники группы будут иметь одинаковые полномочия в доступе к сетевым ресурсам. При появлении новых пользователей администратор может просто присоединить их к какой-либо из существующих групп и, таким образом, предоставить им соответствующие привилегии (rights, разрешения на выполнение определенных действий в сети) и полномочия.

И наконец, некоторые виды продвинутого сетевого ПО для серверов содержат в себе специальные инструменты управления (management tools), при помощи которых сетевые администраторы могут следить за ситуацией в сети. При возникновении какой-либо проблемы эти средства позволяют выявить ее и получить соответствующие данные в виде графиков или в другой подходящей форме. При помощи этих инструментов администраторы могут предпринять корректирующие действия до того момента, как проблема обрушит сеть.

Вопросы межоперабельности СОС

Компьютерные сети редко бывают цельными системами. Обычно они представляют собой разнообразие аппаратных платформ, объединение физических топологий и целую коллекцию серверного и клиентского ПО. В большинстве случаев за несколько лет аппаратное и программное обеспечение сетей меняется из-за модернизации, добавления заплат, обновлений и т. д. Для нормального функционирования сети

необходим некий общий язык, при помощи которого все компьютеры могли бы взаимодействовать. ОС сервера, ОС клиента и редиректор должны быть совместимы между собой. Следовательно, технический специалист должен понимать основы взаимодействия между платформами. Например, вопрос межоперабельности становится главным в ситуации, когда сервер на основе Windows NT должен взаимодействовать с клиентом на основе Windows 95, UNIX или AppleTalk. Различия в аппаратном, программном обеспечении и протоколах являются потенциальными источниками проблем в компьютерных сетях.

Клиент-серверная межоперабельность

Существует два подхода к обеспечению межоперабельности: серверный (server-side или back-end) и клиентский (client-side или front-end). Выбор того или иного подхода зависит от того, какими сетевыми продуктами вы пользуетесь.

- *Клиентский подход.* В сетях с несколькими операционными системами ключом к межоперабельности является редиректор. Ваш компьютер может иметь несколько редиректоров, предназначенных для взаимодействия с разными сетевыми службами, точно так же, как вы можете пользоваться услугами нескольких провайдеров для получения доступа в Интернет. Каждый редиректор обрабатывает *только* те пакеты, которые отправляются на понятном ему протоколе или языке. Если вам известен пункт назначения (и к какому ресурсу вы хотите обратиться), вы можете вызвать соответствующий редиректор, который направит ваш запрос на этот пункт назначения. Например, допустим, что клиент на основе Windows NT хочет получить доступ к серверу на основе Novell. Для этого сетевой администратор устанавливает на клиенте редиректор Microsoft (предназначенный для обеспечения доступа к Novell-серверам) поверх Windows NT.
- *Серверный подход.* Другой метод взаимодействия между клиентом и сервером состоит в том, что службы взаимодействия устанавливают на сервере. Этот подход обычно применяется для того, чтобы состыковать Apple Macintosh со средой Windows NT. Например, компания Microsoft поставляет специальное программное обеспечение Services for Macintosh, которое позволяет взаимодействовать серверу на основе Windows NT Server с клиентом на основе Apple. Если на Windows NT Server установлен компонент Services for Macintosh, пользователи компьютеров Apple могут получить доступ к ресурсам на этом сервере. Служба Services for Macintosh также конвертирует файлы между компьютерами Apple и Windows NT, поэтому пользователи этих компьютеров могут использовать свои собственные интерфейсы для того, чтобы иметь совместный доступ к одним и тем же файлам. При таком типе межоперабельности пользователи Apple могут применять стандартные процедуры Apple и видеть пиктограммы Macintosh (например, **Choose** и **Finder**) даже во время обращения к ресурсам сервера Windows NT.

Межоперабельность продуктов Microsoft

Редиректор Microsoft распознает компьютерные сети Microsoft под управлением Windows 2000/NT/95/98. Редиректоры автоматически компонуются во время установки операционной системы. Установочная утилита загружает необходимые драйверы и затем редактирует запускающие файлы таким образом, чтобы редиректор запускался при загрузке компьютера. Редиректор Microsoft позволяет клиентам не

только получать доступ к ресурсам, но также и предоставлять свои ресурсы для совместного использования.

Продукты Microsoft и Novell способны взаимодействовать, поэтому для подключения клиента Windows NT Workstation к сети Novell NetWare 3.x или 4.x следует использовать либо службы NWLink и Client Service for NetWare (CSNW), либо службу NetWare Client for Windows NT фирмы Novell. Для того чтобы присоединить систему Windows NT Server к сети NetWare, необходимо использовать службы NWLink и Gateway Service for NetWare (GSNW). Для подключения клиента Windows 95/98 к сети NetWare следует использовать сети IPX/SPX и Microsoft CSNW. Служба Microsoft для службы каталогов NetWare (NetWare Directory Services, NDS) представляет собой клиентское ПО для сетей NetWare, которое поддерживает службы каталогов Directory Services для Novell Network 4.x и 5.x. Microsoft NDS обеспечивает пользователям вход и возможность просмотра файлов для служб NetWare 3.x и 4.x.

Межоперабельность продуктов Novell

Текстовые клиенты NetWare, работающие под управлением MS-DOS, могут соединяться с серверами Novell NetWare и компьютерами Windows NT Server. Клиенты Windows NT, на которых установлен запросчик Novell NetWare и редиректор Windows NT, могут соединяться с серверами Novell NetWare и компьютерами Windows NT Workstation или Server. Фирма Novell поставляет запросчики (иначе называемые редиректорами Novell) для клиентских операционных систем, включая DOS, OS/2 и NetWare Client for Windows NT.

Межоперабельность продуктов Apple

Редиректор для клиентского ПО AppleShare поставляется вместе с ОС AppleTalk и обеспечивает функции совместного использования файлов. Клиентское ПО включается в каждую копию ОС Apple. Кроме того, существует сервер печати AppleShare (который является серверным спулером печати). Сетевое программное обеспечение AppleShare позволяет клиентам, работающим под управлением DOS, иметь доступ к обоим серверам AppleShare. Если на ПК установлено ПО LocalTalk и карта LocalTalk, пользователь может получить доступ к томам файлового сервера и принтерам в сетях AppleTalk. Платы LocalTalk содержат прошивку для управления соединением между сетью AppleTalk и компьютером. Драйверы карты LocalTalk способны работать со многими из протоколов AppleTalk и управляют процессом отправки и получения пакетов данных.

При помощи службы Services for Macintosh клиенты Apple могут получить доступ к серверу Windows NT. Эта служба позволяет клиентам DOS и Apple совместно использовать файлы и принтеры. Компонент Services for Macintosh включает в себя протоколы AppleTalk Protocol версии 2.0 и 2.1, LocalTalk, EtherTalk, TokenTalk и FDDITalk. Кроме того, эта служба поддерживает принтеры LaserWriter версии 5.2 и выше.

Windows XP

Традиционно компания Microsoft выпускает разные семейства программных продуктов для бизнеса и для домашних пользователей. Ярким примером этого был выпуск ОС Windows ME для домашнего применения и Windows 2000 для использования

в компьютерных сетях и на предприятиях. Однако в последние годы компания Microsoft старается объединить свои операционные системы для личного и коммерческого применения в одном семействе. Выпущенная в конце 2001 года, ОС Windows XP является следующей версией Microsoft Windows, которая объединяет в себе Windows 2000 и Windows Millennium. ОС Windows 2000 привнесла в нее основанную на стандартах сетевую безопасность, управляемость и надежность, а Windows 98/ME обеспечила легкий в использовании интерфейс, превосходную аппаратную совместимость и новейшие службы поддержки. Операционная система Windows XP доступна в двух основных версиях: XP Home Edition (версия для домашних пользователей) и XP Professional (для корпоративных пользователей). В этом разделе мы расскажем о возможностях, развиваемых в обеих версиях ОС.

Пользовательский интерфейс

Большинство пользователей Windows умеют проходить через множество диалоговых окон в Windows 2000 и Windows 98/ME. Для Windows XP пользовательский интерфейс был переработан (рис. 4.1).

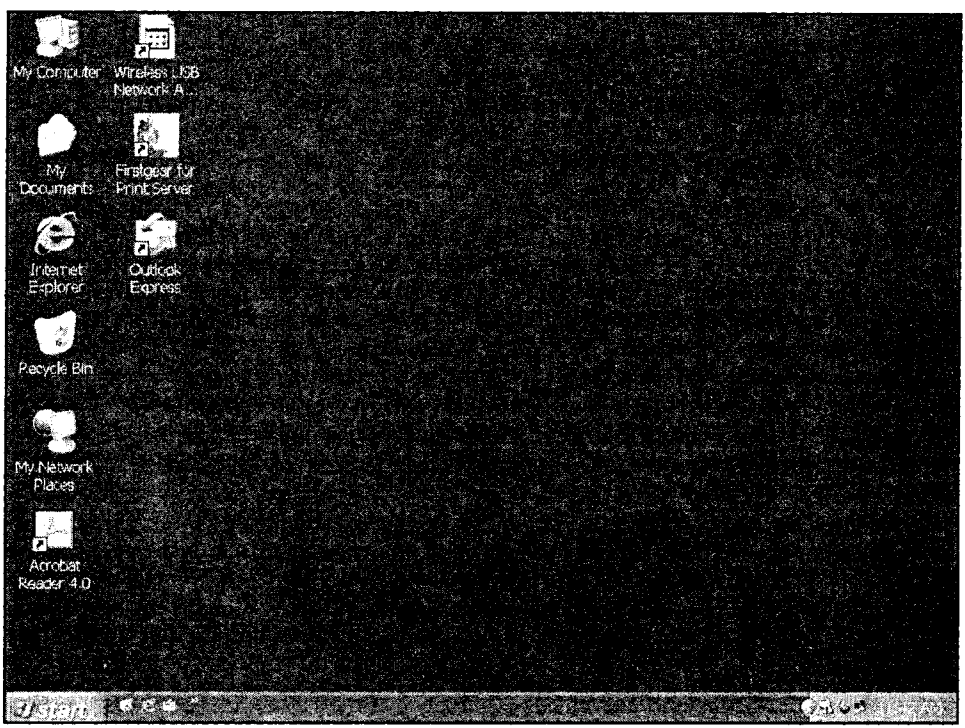


Рис. 4.1. Рабочий стол в Windows XP Professional

Стандартные задачи были сгруппированы и упрощены. Новые визуальные подсказки помогают пользователю перемещаться по интерфейсу. В Windows XP появились новые визуальные стили и темы, в которых используются 24-разрядные цветные

пиктограммы и свои особые цвета, по которым задачи можно легко отличить друг от друга. Например, зеленый цвет обозначает те задачи, при помощи которых вы можете сделать что-либо или перейти куда-либо (как в **Главном меню**).

Переключение пользователей

В текущих версиях Windows пользователь должен сохранить свою работу и выйти из системы, прежде чем другой сможет в нее войти. В Windows XP применяется механизм *быстрого переключения пользователей* (fast user switching), основанный на терминальных службах, допускающий совместные пользовательские сессии. Пользователям не нужно каждый раз выходить из системы и входить в нее заново, при этом данные каждого из них полностью отделены друг от друга. Например, один человек входит в систему, чтобы внести изменения в бухгалтерскую книгу. Если он отойдет от компьютера, в это время другой пользователь сможет войти в систему и запустить какую-нибудь игру. При этом сеанс работы, начатый первым пользователем, перейдет в фоновый режим. Для надежной работы механизма многопользовательского доступа на домашнем ПК требуется не менее 128 Мбайт оперативной памяти. Указанный механизм доступен и в Windows XP Professional, если ПК работает автономно или подключен к рабочей группе. Если вы подключите компьютер с Windows XP Professional к сетевому домену, механизм быстрого переключения пользователей станет недоступным.

Управление файлами

В Windows XP для управления файлами используется технология Web-просмотра. Например, выбирая файл или каталог, вы видите список действий, позволяющих переименовать, переместить, скопировать, отправить по электронной почте, удалить или опубликовать этот файл в сети Интернет. То же самое происходит и в Windows 2000, если вы щелкните правой кнопкой мыши по файлу или каталогу, но в Windows XP эти пункты меню отображаются автоматически, прямо на рабочем столе. В Windows XP также имеется более удобная панель задач, в которой однотипные программы могут объединяться в одну группу. Например, девять файлов Microsoft Word могут быть расположены на панели задач не горизонтально, а в виде группы, объединенной под одной кнопкой. Таким образом, вы видите только одну кнопку, на которой показано количество файлов, открытых в этом приложении. При нажатии на эту кнопку отображается вертикальный список всех файлов.

Мультимедийные средства

В связи с взрывным ростом цифровых средств аудиовизуальной информации, как в домашней сфере, так и в бизнесе, в операционную систему Windows XP были включены улучшенные версии программ Windows Media Player и Windows Movie Maker, а также улучшенная поддержка работы с фотографиями.

Программа Media Player 8

Программа Windows Media Player предназначена для выполнения обычных мультимедийных задач, в том числе: воспроизведение CD- и DVD-дисков, управление многодисковыми системами, создание записей CD-аудио, воспроизведение интернет-радио, перенос мультимедиафайлов на портативные устройства (например, MP3-плееры). Формат Windows Media Audio 8 позволяет сохранять почти в три раза

больший объем музыкальных файлов, чем формат MP3, а также с большей скоростью выполнять запись компакт-дисков и осуществлять более удобное управление мультимедийными ресурсами. Специальный каталог My Music, предназначенный для звуковых файлов, облегчает выполнение связанных с ними задач. Кроме того, в программе Windows Media Player 8 имеются следующие возможности:

- отключение функций программы Windows Media Player в управляемой сети;
- поддержка цифровой ретрансляции;
- ускоренное отображение видеоданных;
- отображение смешанного видео;
- расширенная поддержка большинства звуковых плат с учетом их характеристик.

Программа Movie Maker

Программа Windows Movie Maker 1.1 обладает основными возможностями по захвату аудиовизуальной информации и созданию файлов, выполнению простого редактирования видео- и аудиоданных, а также их сохранению и опубликованию в Интернете. Вы можете записывать, редактировать, организовывать и совместно использовать домашнюю видеотеку на своем персональном компьютере. Кроме того, вы можете обмениваться своими домашними видеозаписями со своей семьей и друзьями посредством электронной почты или Интернета. Если вы хотите создать слайд-шоу, то можете соединить друг с другом статичные изображения и опубликовать их в формате Windows Media Format (WMF). Хотя эта программа может экспортировать файлы только в формате WMF, она способна импортировать все форматы и типы компрессий, поддерживаемые архитектурой DirectShow. Даже если ваш компьютер не оснащен оборудованием для захвата видео, все другие возможности остаются доступными и позволяют импортировать и редактировать мультимедиафайлы, уже находящиеся на ПК.

Цифровые фотографии

В ОС Windows XP расширена поддержка цифровых устройств и предоставлено множество функций для манипулирования изображениями, например, опубликования в Интернете, пересылки по электронной почте (в том числе с возможностью предварительного сжатия), демонстрации изображений в виде автоматического слайд-шоу, увеличения изображения и др.

Аппаратная совместимость

В операционной системе Windows XP была улучшена поддержка устройств и аппаратных средств. Так же, как и Windows 2000, Windows XP упрощает процесс установки, конфигурирования и управления оборудованием ПК. В Windows XP предусмотрена поддержка Plug-and-Play (PnP) для сотен устройств, ранее не поддерживаемых в Windows 2000. Кроме того, в ней имеется расширенная поддержка интерфейсов USB, IEEE 1394, PCI и других шинных архитектур. Предусмотрена также поддержка мониторов с разрешением 200 dpi и новых 64-разрядных процессоров Intel Itanium.

Поддержка DVD и CD

Достижения в технологиях создания накопителей информации сделали работу с CD- и DVD-дисками более легкой и доступной (по цене). В Windows XP встроена

поддержка операций чтения и записи приводов DVD-RAM, а также ОС позволяет читать формат UDF 2.01 (Universal Disk Format), общепринятый стандарт DVD-сред, включая диски DVD-ROM и DVD-видео. В отличие от Windows XP, Windows 2000 может читать только диски, совместимые с форматом UDF 1.02 и 1.5.

Windows XP также позволяет создавать компакт-диски в форматах CD-R и CD-RW при помощи простой операции drag-and-drop и мастера записи. Перед сохранением или копированием файла на компакт-диск ОС создает его образ на жестком диске и только затем переносит данные на устройство записи CD. Премастеринг эффективно минимизирует опустошение буфера, которое может генерировать ошибки в процессе записи и заполнять диск бесполезными данными (что часто случается во время записи "на лету").

Программная совместимость и службы

Операционная система Windows XP совместима почти со всеми из 1000 наиболее распространенных приложений, работающих под Windows 9x, и почти с каждым приложением, работающим под Windows 2000. Единственным исключением являются антивирусные программы, системные утилиты и приложения для создания резервных копий. Однако к тому времени, когда пользователи начинают устанавливать у себя новую систему, большинство производителей уже выпускают обновления своих программ, совместимые с ОС. Функции улучшения работы приложений в Windows XP помогают разрешить проблемы совместимости (например, неправильное определение версии ОС или обращение к освобожденной памяти). Эти функции улучшения работы приложений включаются автоматически самой операционной системой без вмешательства пользователя. При помощи функции автоматического обновления (аналогичной той, которая используется в Windows ME) с сайта Windows Update можно скачивать обновления и исправления, необходимые для работы новых приложений. Кроме того, в Windows XP имеется множество служб для печати и работы с файлами.

Технология WebDAV

Технология WebDAV (Web Digital Authoring & Versioning — цифровая система авторской разработки и управления версиями через Web), которая применена в Windows XP, позволяет публиковать документы на интернет-серверах и потом обновлять их. WebDAV — это стандартный интернет-протокол доступа к файлам, который переносится посредством протокола HTTP через существующую инфраструктуру Интернета (брандмауэры, маршрутизаторы и т. д.). Windows XP содержит в себе редиректор WebDAV, поэтому пользователь может получить доступ к интернет-серверам тем же образом, что и при совместном использовании файлов и серверов дома или в офисе. Если традиционные протоколы обмена файлами не дают доступа к данным из любого места, то технология WebDAV позволяет использовать интернет-протоколы, которые дают доступ к хранилищам данных в любой точке Интернета. Технология WebDAV дает возможность доступа к данным из любой точки при помощи стандартного программного обеспечения (аналогично технологии iFolder, разработанной фирмой Novell для NetWare 6). Другими словами, вы можете использовать редиректор WebDAV для того, чтобы публиковать свои Web-данные или использовать интернет-хранилища для хранения своих данных и обмена информацией.

Шифрование на клиентской стороне

Операционная система Windows XP позволяет шифровать базу данных автономно просматриваемых (оффлайновых) файлов (известную как клиентский кэш, Client-Side Cache, CSC). Шифрование базы защищает ее от несанкционированного доступа и увеличивает степень защиты хранимых в кэше данных. Это новая возможность по сравнению с ОС Windows 2000. Ее можно использовать, например, для хранения в защищенном виде важных данных, а сетевые администраторы могут использовать эту функцию для защиты всех локальных файлов. Эта функция также весьма полезна на случай кражи вашего ноутбука, если содержащиеся в нем конфиденциальные данные сохранены в автономном кэше. Для управления функцией шифрования автономных файлов требуются полномочия администратора.

FAT32 для DVD-RAM

Вы можете воспользоваться диском DVD-RAM в формате FAT32, и Windows XP сумеет опознать, смонтировать и отформатировать ваш том FAT32 на диске DVD-RAM в superfloppy-формат (т. е. диск без таблицы разделов). Для применения подобного DVD-RAM нужен обычный съемный мультимедиапривод (например, магнитооптический или Jaz).

NetCrawler

NetCrawler ("сетевой червяк") способен искать, автоматически инсталлировать и подключаться ко всем принтерам совместного использования, которые он находит в домашней или офисной сети. Этот компонент позволяет неопытным пользователям получить легкий и автоматически конфигурируемый доступ к компьютерам и устройствам, находящимся в рабочей группе. Он выполняет свою работу путем перебора всех сетевых каталогов и поддержки соединений со всеми сетевыми ресурсами. Например, если вы настраиваете новый компьютер и хотите распечатать какие-нибудь документы, NetCrawler находит свободные принтеры и сообщает вам о них. Если NetCrawler не может найти какие-нибудь устройства совместного доступа в течение 48 часов, ярлыки к этим ресурсам будут удалены из каталога My Network Places. NetCrawler включается по умолчанию при установке Windows XP Home, а также при установке Windows XP Professional, если компьютер функционирует в режиме рабочей группы (не соединен с доменом). Кроме того, этот компонент проверяет наличие новых ресурсов при каждом входе в сеть и при открытии или обновлении папок Printers (Принтеры) и My Network Places (Сетевое окружение).

Совместное использование факсов

Совместное использование факсовых устройств позволяет вам отправлять и принимать факсимильные сообщения при помощи соответствующего оборудования (например, факс-модема или факс-платы) или через сеть, предоставляющую необходимый сервис. Вы можете отправлять факсовые сообщения при помощи программы Microsoft Outlook или клиента групповой работы (или любого другого приложения, которое поддерживает функцию печати). Функция совместного использования факса в Windows XP обеспечивает интеграцию со списком контактов программы Outlook, возможность предварительного просмотра сообщения перед его отправкой и опцию получения электронного письма, подтверждающего прием сообщения. Администраторы могут управлять функциями использования факса при помощи Microsoft Management Console (MMC, консоль управления) и компонентов TAPI

(Telephony Application Programming Interface — интерфейс прикладного программирования для работы по телефонным линиям). Эта функция Windows XP также полностью совместима с факс-службами пакетов Back Office Server (BOS)/Small Business Server (SBS) 2000.

Работа в сети и связь

Windows XP упрощает установку и администрирование сетей и расширяет возможности типичных сетевых архитектур.

Технология Plug-and-Play

Обычные возможности Plug-and-Play позволяют администраторам устанавливать, конфигурировать и добавлять периферийные устройства к ПК. Технология Universal Plug-and-Play распространяет простоту этих операций на всю сеть — она позволяет находить и контролировать различные устройства (в том числе сетевые устройства и службы), например: сетевые принтеры, интернет-шлюзы, потребительские электронные устройства. Universal Plug-and-Play поддерживает механизм нулевого конфигурирования (zero-configuration), невидимую работу в сети (invisible networking) и автоматическое обнаружение различных категорий устройств разных производителей. При помощи Universal Plug-and-Play устройство может динамически присоединиться к сети, получить IP-адрес, сообщить о своих характеристиках и получить сведения о присутствии и характеристиках других устройств, — и все это автоматически. В технологии Universal Plug-and-Play используются стандартные TCP/IP и интернет-протоколы.

Сетевые соединения

Впервые появившийся в Windows 98 механизм совместного использования интернет-соединений (Internet Connection Sharing, ICS) обеспечивает удобное и экономичное подключение нескольких компьютеров домашней сети к одному коммутируемому соединению, служащему в качестве шлюза (для доступа как к Интернету, так и к корпоративной сети). В этом случае каждое из устройств, находящихся за шлюзом, может иметь не уникальный IP-адрес, а частный адрес (private address).

В дополнение к этому существует Home Networking Wizard (Мастер домашней сети в составе Мастера новых подключений), который автоматически конфигурирует сеть и службу ICS. В нем применяются мосты для того, чтобы можно было создать локальную сеть без знаний о сетевых протоколах и требованиях к физической организации сети. Раньше при построении типичной многосегментной IP-сети требовалось присваивать номер подсети каждому сегменту, конфигурировать хосты в каждой подсети, настраивать процесс продвижения пакетов данных между подсетями. В Windows XP входит мостовой компонент доступа к среде (MAC bridge component), который прозрачно соединяет между собой сетевые сегменты при помощи "алгоритма связующего дерева" (Spanning Tree Algorithm, STA). Включенный в Windows XP MAC-мост позволяет всей домашней сети работать как единая IP-подсеть. *Мост* — это сетевое устройство, которое служит для соединения между собой двух или более физических сетей. Мост создает список устройств, имеющихся в сети, и при каждой передаче данных проверяет, существует ли указанный адрес получателя в данной сети.

Удаленный рабочий стол

При помощи Удаленного рабочего стола (Remote Desktop) вы можете запускать приложения на удаленном ПК, работающем под управлением Windows XP Professional, с любого другого клиента, работающего под управлением ОС Microsoft Windows. Приложения запускаются на ПК с Windows XP Professional, с клиентского компьютера передаются только данные от клавиатуры, мыши и возвращаются данные на дисплей. Удаленный рабочий стол позволяет вам получить доступ к вашему ПК с Windows XP откуда угодно, через любое соединение, используя любой клиент на основе Windows. Этот механизм предоставляет вам безопасный доступ ко всем вашим приложениям, файлам и сетевым ресурсам, как если бы вы находились прямо перед своей рабочей станцией. Любые приложения, которые вы оставляете запущенными в своем офисе, продолжают работать в тот момент, когда вы устанавливаете соединение. Если вы являетесь сетевым администратором, то Удаленный рабочий стол может послужить в качестве средства быстрого ответа. Он позволяет получить удаленный доступ к серверу, работающему под управлением Windows 2000 Server или Whistler Server (2003), и увидеть поступающие сообщения, администрировать компьютер удаленно или применить автоматическое управление сервером.

Надежность системы

Надежность ПК и его ресурсов критически важна для любой компьютерной сети. Операционная система Windows XP включает ряд улучшений, предназначенных для повышения ее надежности.

Откат драйвера

Функция отката к предыдущему драйверу (Driver Rollback) помогает обеспечить надежность системы, как и функция возврата к последней работоспособной конфигурации (Last Known Good Configuration), которая впервые появилась в Windows 2000 в безопасном режиме (Safe Mode), или как функция восстановления системы (System Restore). При обновлении драйвера копия предыдущего драйвера автоматически сохраняется в специальном подкаталоге системных файлов. Если новый драйвер работает некорректно, вы можете восстановить предыдущий драйвер. Функция Driver Rollback допускает только один уровень отката (только одна версия предыдущего драйвера может быть сохранена) и работает для всех классов устройств, кроме принтеров.

Восстановление системы

Восстановление системы (System Restore) позволяет вернуть компьютер в предыдущее состояние при возникновении какой-либо проблемы, не связанной с потерей персональных данных — документов, рисунков или электронной почты. Механизм System Restore активно следит за изменениями в системе и в некоторых файлах приложений и автоматически создает легко определяемые точки восстановления. По умолчанию Windows XP создает точки восстановления каждый день, а также при таких значительных событиях, как, например, установка приложения или драйвера. Пользователь может в любое время создать свою собственную точку восстановления и обозначить ее каким-либо именем. Механизм System Restore не отслеживает изменения в пользовательских файлах и не восстанавливает их.

Аварийное восстановление системы

Утилита автоматического Аварийного восстановления системы (Automated System Recovery, ASR) позволяет сохранять и восстанавливать приложения. Кроме того, она поддерживает механизм Plug-and-Play, необходимый для создания резервных копий системного реестра и их использования в целях восстановления. Эта утилита может быть полезна для восстановления системы после серьезных сбоев. Например, при отказе жесткого диска и потере всех конфигурационных параметров и информации утилита ASR может быть применена для восстановления данных сервера.

Динамическое обновление

Надежность системы усилена механизмом динамических обновлений (Dynamic Update), который позволяет получить обновления, улучшающие совместимость приложений и устройств, обновления драйверов и срочные исправления, решающие проблемы установки и безопасности. Для получения пакета обновлений используется Web-служба Windows Update. Если вы выбрали режим динамического обновления во время установки системы, обновления для устройств и приложений загружаются прямо с сервера Microsoft (вместо компакт-диска с исходными файлами). Механизм полезен и для организаций, поскольку сетевые администраторы могут скачать полный пакет обновлений, возможно содержащий необходимые пользователям исправления. Используя этот пакет, администраторы могут быть уверенными, что все пользователи, устанавливающие данную систему, получили обновленные файлы.

Автоматическое обновление

Этот режим (AutoUpdate) обновления системы не требует прерывать вашу работу во Всемирной паутине. Нет необходимости заходить на специальные Web-страницы, прерывать навигацию в Интернете или помнить о том, что нужно периодически обновлять систему. Процесс фонового автоматического обновления настроен так, чтобы минимизировать влияние на скорость реакции сети, и автоматически возобновляется в случае разрыва связи, до полной загрузки обновления. После того как обновление будет полностью загружено, пользователь сможет разрешить его установку.

Служба Windows Update

Служба Windows Update может использоваться для получения драйверов устройств и выступает в роли дополнения к той обширной библиотеке драйверов, которая содержится на установочном компакт-диске. Windows Update — это онлайновое расширение Windows XP, обеспечивающее централизованное размещение усовершенствованных продуктов в виде сервисных пакетов, драйверов устройств и обновлений системной безопасности. Например, если вы устанавливаете новое устройство, механизм Plug-and-Play будет выполнять поиск нужного драйвера как на локальном диске, так и в службе Windows Update. Если ваш компьютер *не* соединен с Интернетом и на нем не обнаружен подходящий драйвер, вам будет предложено установить связь с Интернетом для продолжения поиска. Если обновленная версия драйвера найдена в службе Windows Update, будет загружен cab-файл с этим драйвером, и элемент управления ActiveX службы Windows Update выберет для установки соответствующий inf-файл.

Интернет-безопасность

Для любой сети очень важна система безопасности, обеспечивающая защиту ценных файлов, сетевых ресурсов и доступ к сети. Windows XP поддерживает набор улучшенных средств безопасности, которые позволяют защитить сеть от неавторизованного доступа.

Интернет-брандмауэр

Windows XP обеспечивает интернет-безопасность с помощью встроенного средства, называемого Internet Connection Firewall (ICF, брандмауэр интернет-подключений), которое подходит как для домашних пользователей, так и для небольших организаций. ICF защищает компьютеры, непосредственно связанные с Интернетом или подключенные к нему через службу Internet Connection Sharing, действующую на хост-компьютере вместе с ICF. Это средство пресекает попытки сканирования портов и ресурсов (файлов и принтеров коллективного пользования), совершаемые извне. Брандмауэр блокирует все незатребованные подключения, исходящие из Интернета, используя логику преобразования сетевых адресов (Network Address Translator, NAT) с целью подтверждения правильности входящих запросов на доступ к сети или локальному хосту. Если попытка установления связи была произведена не из защищаемой сети или если не было создано отображение портов, поступающие данные блокируются. Компонент Internet Connection Firewall может использоваться для локальных компьютерных сетей, виртуальных частных сетей (Virtual Private Network, VPN), при двухточечном соединении в Ethernet-сети (PPoE) или при коммутируемом соединении.

Политики ограничения

Политики ограниченного использования программ (software restriction policy) в Windows XP обеспечивают прозрачный способ изолирования и применения небезопасного, потенциально вредного кода таким образом, чтобы защитить вас от различных вирусов, троянов и червей, распространяемых через электронную почту и Интернет. Эти политики позволяют определять порядок использования ПО в системе. Запуская потенциально опасный код и сценарии в ограниченной среде (известной как "песочница"), вы получаете выигрыш оттого, что доказываете их безопасность или предотвращаете разрушительные действия зараженного кода. Например, потенциально опасный код не сможет отправить электронное письмо, или получить доступ к какому-либо файлу, или выполнить какую-либо другую обычную задачу, пока не будет признан безопасным. Политики ограниченного использования программ защищают от зараженных вложений электронной почты, в том числе вложенных файлов, которые сохраняются во временном каталоге, встроенных объектов и сценариев.

Безопасность беспроводных соединений

Средство Secure Wireless/Ethernet LAN позволяет создавать безопасные беспроводные и проводные локальные сети. При работе этого компонента компьютер обычно не может получить доступ к сети, пока пользователь не введет свою регистрационную информацию. Однако если устройство использует "машинную аутентификацию" (machine authentication), компьютер может получить доступ к локальной сети после прохождения аутентификации и авторизации на сервере IAS/RADIUS. Компонент Secure Wireless/Ethernet LAN в ОС Windows XP осуществляет защиту как

проводных, так и беспроводных локальных сетей, основанных на спецификации IEEE 802.11. Он работает в сочетании с открытыми сертификатами (public certificates), используемыми в картах авторегистрации или смарт-картах. Они управляют доступом к проводным интернет-сетям и беспроводным сетям спецификации IEEE 802.11, установленным в таких общественных местах, как большие магазины или аэропорты.

Управление мандатами

Служба управления мандатами (Credential Management) обеспечивает безопасное хранение мандатов пользователя, включая пароли и сертификаты безопасности X.509 RSA. Это упрощает процедуру получения доступа, в том числе и для мобильных пользователей. Если вы обращаетесь к приложению внутри компьютерной сети компании, то при первом обращении вам придется пройти аутентификацию и предоставить свой мандат. После предоставления мандата он будет ассоциирован с запрошенным приложением. При последующих обращениях будет использоваться сохраненный мандат, который не придется вводить заново. Служба Credential Management состоит из трех компонентов: менеджер мандатов (Credential Manager), пользовательский интерфейс списка мандатов (Credential Collection User Interface) и управление ключами (Keyring).

Windows 2000

Построенная на основе технологии Windows NT, полностью интегрированная СОС Windows 2000 предлагает встроенные службы для работы с Web и приложениями, стандартные для Интернета средства безопасности и хорошую производительность. Эта ОС была выпущена в 2000 году и быстро стала популярной среди тех, кто занимается бизнесом в Интернете (рис. 4.2).

Windows 2000 легко масштабируется от одного или двух серверов с дюжиной клиентов до сотен серверов и тысяч клиентов. Эта ОС считается надежной и отказоустойчивой. Последний выпуск Windows 2000 (а также недавно выпущенная Windows XP Professional) лучше всех поддерживает новое оборудование для ПК (от небольших мобильных устройств до самых крупных и мощных серверов, используемых в электронной коммерции). Windows 2000 существует в нескольких основных вариантах, подходящих для разных сетевых конфигураций.

- Windows 2000 Professional. Поддерживает до двух процессоров и 4 Гбайт оперативной памяти. Эта ОС хорошо подходит для коммерческих настольных компьютеров и ноутбуков и предназначена для перемещающихся пользователей и пользователей Интернета. Windows 2000 Professional не поддерживает кластеризацию.
- Windows 2000 Server. Это серверная ОС начального уровня, рассчитанная на серверы файлов, печати, интранета и сетевой инфраструктуры. Версия поддерживает до четырех процессоров и 4 Гбайт оперативной памяти и не поддерживает кластеризацию.
- Windows 2000 Advanced Server. Обладает повышенной надежностью, доступностью и масштабируемостью, что позволяет использовать ее для работы с приложениями электронной коммерции и бизнеса. Windows 2000 Advanced Server поддерживает до восьми процессоров и 8 Гбайт оперативной памяти. Кроме то-

го, имеется поддержка кластеризации на уровне двухузлового отказоустойчивого файлового сервера (failover, файловер) и служба 32-узловой балансировки сетевой нагрузки.

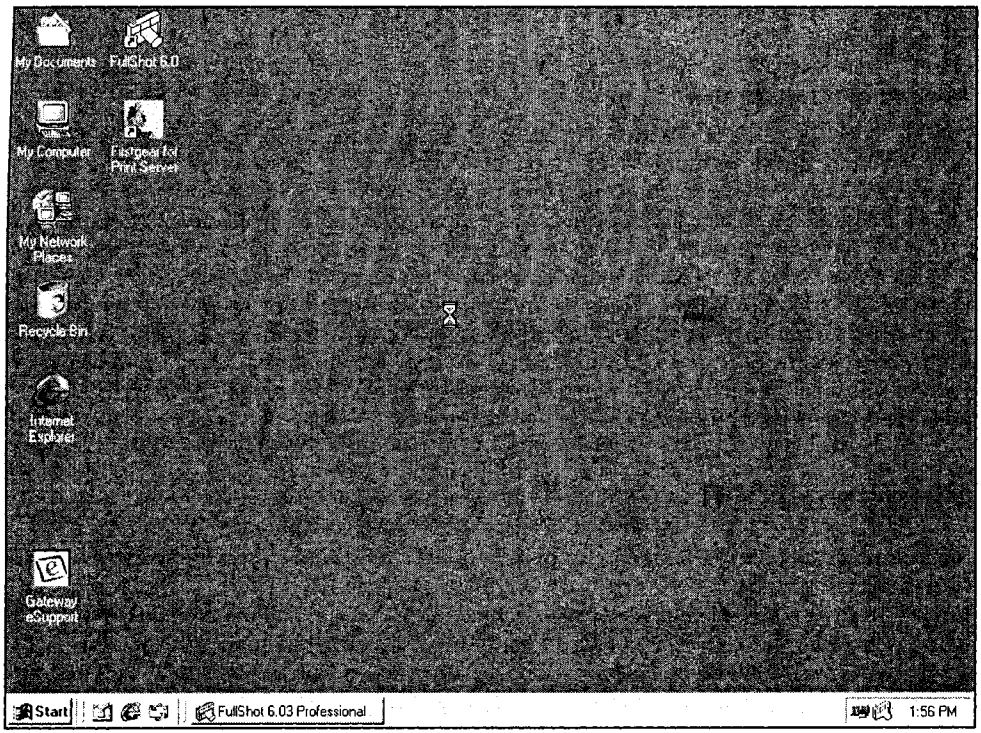


Рис. 4.2. Рабочий стол в Windows 2000 Server

- Windows 2000 Datacenter Server. Это самая мощная серверная ОС, предлагаемая компанией Microsoft. Она предназначена для предприятий, которым требуется наивысший уровень доступности и масштабируемости. С ней вы можете использовать до 32 процессоров и 64 Гбайт оперативной памяти. Кроме того, она поддерживает файловер, который может переключаться между четырьмя узлами кластера, и службу 32-узловой балансировки сетевой нагрузки.

Примечание

Более подробно об ОС Windows 2000 и ее поддержке можно узнать на сайте компании Microsoft по адресу: **www.microsoft.com/windows/default.asp**.

Особенности Windows 2000

Windows 2000 Professional проще в установке, управлении и сопровождении, чем другие версии этой ОС. Централизованные утилиты управления, средства поиска и устранения неполадок, поддержка "самовосстанавливающихся" приложений — все

это упрощает администраторам и пользователям установку и управление настольными и портативными компьютерами. В свою очередь, эти удобства помогают сократить расходы. Данная версия ОС объединяет мощь и безопасность Windows NT Workstation с традиционной простотой использования Windows 98. В ней поддерживается большее количество различных мастеров (wizards), централизованная область часто используемых задач и меню, адаптируемое к стилю вашей работы. Если использовать Windows 2000 Professional в сочетании с Windows 2000 Server, то можно получить выигрыш от применения технологий IntelliMirror. При этом важная информация и настройки пользователя сохраняются на центральном компьютере. IntelliMirror позволяет вам работать на любом компьютере, присоединенном к сети, как на своем собственном.

В Windows 2000 Professional внесены коренные усовершенствования для повышения ее надежности (например, модификации в ядре операционной системы для защиты от сбоев и обеспечения самовосстановления), которые делают эту ОС самой надежной настольной системой, когда-либо выпущенной компанией Microsoft. Кроме того, Windows 2000 включает в себя комплекс средств безопасности для защиты ценной информации как локально, на отдельной рабочей станции, так и во время ее передачи по локальной сети, телефонным линиям или через Интернет. Благодаря поддержке компонентов безопасности интернет-стандарта (например, IP Security, Layer 2 Tunneling Protocol, Virtual Private Networking) ОС Windows 2000 считается настолько безопасной, что ее используют даже в банках.

Windows 2000 Professional включает в себя все компоненты Windows NT Workstation, а также множество дополнений и усовершенствований к ним. Новые компоненты разработаны таким образом, чтобы ОС сочетала в себе простоту использования, характерную для Windows 98, и стабильность, высокую производительность и безопасность Windows NT. Многие из этих улучшений приведены в списке.

- 64-разрядная готовность. Компания Microsoft разработала базовый код ОС Windows 2000 в виде, готовом к переходу на 64-разрядную архитектуру. В будущем компания Microsoft планирует создать полноценную 64-разрядную операционную систему, которая будет полностью совместима с 32-разрядными приложениями. Эта система предназначена специально для 64-разрядного процессора Itanium фирмы Intel.
- Active Directory. Это встроенная в Windows 2000 служба каталогов. Она повышает управляемость, безопасность и улучшает совместимость Windows 2000 с другими ОС.
- Group Policy (Групповая политика). Позволяет администратору разграничивать и управлять состоянием компьютеров и/или пользователей в организации. Действие групповой политики регулируется путем изменения их принадлежности к той или иной группе безопасности.
- Hardware Wizard (Мастер оборудования). Предоставляет единый и простой интерфейс для решения множества вопросов, связанных с оборудованием ПК. Он дает возможность добавлять, конфигурировать, удалять, модернизировать и устранять неполадки в используемых периферийных устройствах.
- Index Server. Эта утилита работает в фоновом режиме и создает упорядоченный список (индекс) содержания локального диска или файлов в сети (если компьютер соединен с ней). Она позволяет индексировать выбранные каталоги и свой-

ства файлов. Index Server может работать как локально, так и с сетевыми ресурсами и улучшает скорость и точность поиска информации и сортировку результатов.

- Intellimirror Desktop Management. Этот компонент позволяет пользователям работать на любой станции, присоединенной к компьютерной сети, применяя личные настройки рабочего стола и приложений и используя свои документы. Intellimirror дает возможность администраторам автоматически распространять программное обеспечение (в том числе проводить удаленную установку ОС). Кроме того, администраторы могут удаленно управлять конфигурацией рабочего стола и поддерживать его функционирование.
- Internet Explorer 5.x. Последняя (на момент выхода ОС) версия браузера Internet Explorer полностью интегрирована в Windows 2000 Professional.
- Network Connections Wizard (Мастер сетевых подключений). В системном каталоге Control Panel (Панель управления) содержится подкаталог Network and Dial-up Connections (Сеть и удаленный доступ к сети), который заменил компонент Network Settings Панели управления NT 4.0. При щелчке мышью на пиктограмме **Make New Connection** (Создание нового подключения) открывается мастер Network Connections Wizard, который содержит меньше шагов, чем это было в ОС NT 4.0. В сочетании с компонентом Active Directory, существующим в Windows 2000 Server, в ОС добавляется ряд новых функций, позволяющих упростить управление компьютерной сетью.
- Диалоговые окна **Open/Save/Save As**. В Windows 2000 в левой части диалоговых окон, предназначенных для открытия и сохранения файлов, отображается дерево каталогов (как в программе Outlook), при помощи которого можно быстро и легко переходить в другие каталоги жесткого диска.
- Персонализированное меню **Start** (Пуск). В Windows 2000 производится регистрация тех программ и файлов, которые были запущены из меню **Start** (Пуск), **Programs** (Программы). После первых шести сессий система изменяет содержание меню **Programs** (Программы), оставляя в нем только те программы, которые были запущены недавно. Остальные элементы скрываются и их можно отобразить, щелкнув мышью по двойным стрелкам. В Windows 2000 выполняется слежение за открываемыми файлами и в соответствии с этим изменяет содержание стартового меню.
- Plug-and-Play. ОС Windows 2000 совместима с существующим стандартом Plug-and-Play, включая поддержку самых современных шин (USB, IEEE 1394, или FireWire, и AGP) и других устройств, например: DVD-проигрывателей, сканеров и цифровых камер.
- Поддержка SMP (Symmetrical Multiprocessing). Симметричная многопроцессорная обработка позволяет использовать несколько процессоров, работающих под управлением разных версий ОС Windows 2000. Windows 2000 Professional и Windows 2000 Server поддерживают до двух процессоров одновременно, тогда как Windows 2000 Advanced Server поддерживают до восьми процессоров.
- Windows 2000 Explorer. Программа Explorer (Проводник) в Windows 2000 содержит все настраиваемые элементы, которые имеются в Windows 98 Explorer. Также имеются следующие новые опции: отображение в виде пиктограмм всех файлов, а не только отдельных папок, настраиваемые панели инструментов, модернизи-

рованное диалоговое окно **Folder Options** (Свойства папки) на панели управления.

- Windows Installer. Утилита Windows Installer упрощает процесс установки программ и уменьшает проблемы, связанные с заменой совместно используемых DLL-файлов другими версиями во время процесса установки. Windows Installer позволяет приложениям проверять существующие DLL-файлы, для того чтобы сохранить уже установленные совместно используемые файлы. Кроме того, утилита позволяет добавлять новые программные компоненты спустя какое-то время после выполнения установки программы и может использоваться для восстановления поврежденных приложений. Windows Installer требует совместимости с устанавливаемыми приложениями, поэтому разработчики ПО должны писать программы с MSI-сценариями, позволяющими работать с этой утилитой.

Межоперабельность Windows 2000

ОС Windows 2000 обеспечивает или поддерживает большой набор протоколов. Клиент практически любой другой платформы может взаимодействовать с серверами, работающими под управлением Windows 2000 Server, а клиенты, использующие Windows 2000 Professional, могут взаимодействовать с серверными платформами таких фирм, как Novell, IBM и др. Для обеспечения межоперабельности в Windows 2000 предусмотрена поддержка ряда распространенных средств коммуникации и протоколов безопасности, включая TCP/IP, LDAP, DHCP, DNS и протокол аутентификации Kerberos версии 5.0. На основе этой поддержки Windows 2000 может взаимодействовать с другими ОС, например: Novell NetWare, Macintosh, HP/UX, Solaris, IBM AIX и Linux; со службами каталогов, например: Novell NDS, Lotus Notes, Exchange и каталогами на основе LDAP; и с базами данных, разработанными фирмами IBM, Informix и Oracle.

"Services for UNIX" (Службы для UNIX) версии 2.0 содержит компоненты, которые могут быть использованы для интеграции Windows 2000 с существующими средами UNIX. Это дополнительное ПО содержит средство для синхронизации паролей, службу Network Information Service (NIS), мастер для перехода с NIS на Active Directory (NIS-to-Active Directory Migration Wizard), службу разрешения пользовательских имен и серверное клиентское и шлюзовое программное обеспечение для сетевой файловой системы (Network File System). Microsoft Interix 2.2 обеспечивает среду для выполнения UNIX-приложений и сценариев на ОС Windows NT и Windows 2000. Для поддержки систем фирмы IBM может использоваться Host Integration Server (преемник SNA Server), который позволяет объединять ОС Windows с другими типами корпоративных ОС, работающих на мэйнфреймах фирмы IBM, например, AS/400 и UNIX.

Services for Macintosh (Службы для Macintosh) представляет собой встроенный компонент Windows 2000 Server, который включает File Server for Macintosh (Файловый сервер для Macintosh), Print Server for Macintosh (Сервер печати для Macintosh), службы поддержки протокола AppleTalk и AppleTalk Control Protocol (ATCP). Службы для Macintosh позволяют компьютерам, работающим под ОС Windows и Macintosh, совместно использовать файлы и принтеры. Компьютер, работающий под управлением Windows 2000 Server, при использовании Services for Macintosh может работать как файловый сервер, сервер удаленного доступа и сервер печати для

клиентских компьютеров Macintosh. Кроме того, Windows 2000 Server может выполнять функцию маршрутизатора AppleTalk.

Как отдельный продукт существует программное обеспечение Services for NetWare (Службы для NetWare). Ее версия 5.0 позволяет клиентам с Windows 2000 Professional (и серверам Windows 2000 Server) взаимодействовать с серверами NetWare. Программное обеспечение Services for NetWare включает в себя файловую службу и службу печати для ОС NetWare версий 4.0 и 5.0, Directory Service Manager for NetWare (Менеджер службы каталогов для NetWare), Microsoft Directory Synchronization Services (MSDSS, службы синхронизации каталогов Microsoft) и File Migration Utility (Утилита миграции файлов). Кроме того, Windows 2000 содержит несколько встроенных технологий, которые поддерживают NetWare. Например, Client Services for NetWare (Клиентские службы для NetWare) позволяет клиентам с Windows 2000 Professional получать доступ к ресурсам на серверах NetWare. Gateway Service for NetWare (Шлюзовая служба для NetWare) позволяет серверам Windows 2000 взаимодействовать с серверами NetWare.

Windows NT

В отличие от операционной системы NetWare, Windows NT представляет собой интегрированную платформу, которая соединяет в себе как компьютерную операционную систему, так и сетевую. Windows NT Server наделяет компьютер серверными функциями и позволяет ему предоставлять сетевые ресурсы. Windows NT Workstation превращает компьютер в клиента компьютерной сети.

Примечание

Более подробно об ОС Windows NT и ее поддержке можно узнать на сайте компании Microsoft по адресу: **www.microsoft.com/windows/default.asp**.

Особенности и версии ОС Windows NT

Работа Windows NT основана на доменной модели. *Домен* (domain) — это группа компьютеров, которые совместно используют общую базу данных и политики безопасности. Каждый домен имеет уникальное имя (идея доменов очень важна с точки зрения создания учетных записей и групп в сетях Windows). Внутри каждого домена один сервер должен быть назначен как основной контроллер домена (Primary Domain Controller, PDC). PDC-сервер обеспечивает работу служб каталогов и осуществляет аутентификацию пользователей. Службы каталогов в Windows NT могут быть организованы различными способами при помощи базы данных безопасности (security database) и базы данных учетных записей (account database). Существует несколько разных доменных моделей. *Однодоменная сеть* (single-domain) ведет базу данных учетных записей и базу данных безопасности. *Сеть с одним главным доменом* (single-master network) может иметь несколько доменов, но один из них работает в качестве основного и хранит пользовательские учетные записи. *Сеть с несколькими главными доменами* (multiple-master network) включает в себя группу доменов, некоторые из которых ведут базу данных учетных записей. Такой подход используется для очень больших организаций. *Сеть с полностью доверительными отношениями* (complete-trust network) состоит из нескольких доменов, ни один из которых не является основным — все домены работают согласованно.

Службы Windows NT

Сочетание Windows NT Server и Windows NT Workstation обеспечивает мощный набор служб, среди которых присутствуют файловые, защитные, печатные и сетевые службы.

Файловые службы

В сети Windows NT применяется два подхода к совместному использованию файлов. Первый является простым совместным использованием файлов, как это происходит в одноранговых сетях. Любая рабочая станция или сервер может предоставить каталог для совместного доступа в сети и устанавливать свойства хранящихся в нем данных (например, запрет доступа, доступ только для чтения, доступ для изменения или полный доступ). Единственное отличие Windows NT от других ОС (например, Windows 95/98) заключается в том, что для предоставления совместного доступа необходимо иметь администраторские права. Другой метод позволяет получить все преимущества системы безопасности в Windows NT. Вы можете устанавливать разрешения доступа на уровне каталога или файла и таким образом ограничивать доступ для тех или иных пользователей или групп. Для этого необходимо использовать файловую систему NTFS. Во время установки Windows NT вы можете выбрать одну из файловых систем: NTFS или FAT16 (DOS). Вы можете установить обе файловые системы на разные жесткие диски (или на разные тома одного диска), но при работе в режиме DOS каталоги NTFS будут недоступны. Любой клиент, не использующий файловую систему NTFS, может предоставлять свои ресурсы для совместного использования, но ограничен публичным доступом и лишен преимуществ безопасности файловой системы NTFS.

Примечание

В Windows 98 используется файловая система FAT32 Windows NT не совместима с FAT32, поэтому она не может быть установлена на диск с этой файловой системой и не может распознавать файлы на томе с FAT32.

Службы безопасности

Windows NT обеспечивает безопасность всех ресурсов сети. Сетевой доменный сервер Windows NT ведет все учетные записи, управляет разрешениями и хранит сведения о пользовательских правах. Для того чтобы получить доступ к какому-либо сетевому ресурсу, необходимо обладать правами на выполнение нужного действия и иметь разрешение на пользование этим ресурсом.

Службы печати

В сети Windows NT любой клиент или сервер может функционировать как сервер печати. Разделяемый принтер доступен для каждого, кто находится в сети (в соответствии с принятыми условиями совместного использования ресурсов). При установке принтера обозначьте его как локальный принтер (My Computer) или как сетевой принтер. Если вы выберете сетевой принтер, то возникнет диалоговое окно, в котором будут перечислены все доступные сетевые принтеры — вам остается только выбрать один из них. Помните, что в сети может быть установлено более одного принтера. Если вы устанавливаете локальный принтер, то вам будет задан вопрос

о том, хотите ли вы предоставлять этот принтер для совместного сетевого использования.

Сетевые службы

Windows NT содержит несколько служб, предназначенных для обеспечения надежной работы компьютерной сети. Служба сообщений (Messenger service) отправляет и получает сообщения внутри сети. Служба предупреждений (Alert service) отправляет извещения, которые принимаются службой сообщений. Служба обозревателя (Browser service) предоставляет список доступных серверов в доменах и рабочих группах. Служба рабочей станции (Workstation) работает на рабочей станции и обеспечивает соединения с серверами (другое название этого службы — редиректор). Служба сервера (Server) обеспечивает совместный доступ к ресурсам на компьютере.

Межоперабельность Windows NT

Сетевой протокол NWLink обеспечивает совместимость Windows NT с ОС NetWare. В первую очередь для этого предназначен компонент Gateway Services for NetWare (GSNW, шлюзовые службы для NetWare). Для соединения с сервером NetWare все клиенты Windows NT, входящие в состав домена, должны использовать единый источник — компонент GSNW, который служит в качестве шлюза между доменом Windows NT и сервером NetWare. Этот шлюз подходит для медленно работающих сетей, но по мере увеличения числа запросов он может снизить производительность сети. Компонент Client Services for NetWare (CSNW, клиентские службы для NetWare) позволяет рабочей станции Windows NT получать доступ к службам печати и файловым службам на сервере NetWare и входит в состав компонента GSNW. Компонент File and Print Service for NetWare (FPNW, файловая служба и служба печати для NetWare) позволяет клиентам NetWare получать доступ к файловым службам и службам печати Windows NT (однако этот компонент не входит в пакет Windows NT и должен приобретаться отдельно). Дополнительная утилита Directory Service Manager for NetWare (DSMN, менеджер службы каталогов для NetWare) интегрирует информацию о пользовательских и групповых учетных записях NetWare и Windows NT. И наконец, Migration Tool for NetWare (Инструмент миграции для NetWare) используется администраторами для пересылки информации об учетных записях из NetWare на контроллер домена Windows NT.

Примечание

Компьютеры, работающие под управлением ОС Windows 95 или 98/SE, также хорошо работают в качестве клиентов в локальных сетях Windows NT и NetWare. Для этого требуется установить соответствующее клиентское программное обеспечение. Однако пользователи Windows 95/98 не могут в полной мере воспользоваться механизмами безопасности Windows NT, поскольку эти механизмы работают с файловым форматом NTFS, который несовместим с Windows 95/98.

Novell NetWare

Благодаря превосходной межоперабельности NetWare, разработанная фирмой Novell, является одной из наиболее популярных ОС. NetWare может выступать как в роли серверной, так и клиентской системы. В клиентской конфигурации эта ОС

может работать поверх разнообразных клиентских операционных систем. Серверная конфигурация NetWare может работать с клиентскими компьютерами, работающими под управлением DOS, Windows (3.x, 95, 98/SE, NT и Windows 2000), OS/2, AppleTalk или UNIX. Именно поэтому NetWare часто применяется в больших сетях, в которых используется несколько разных операционных систем. Однако в небольших сетях NetWare может быть неудобной и создавать трудности для недостаточно опытных специалистов.

Примечание

Более подробно об ОС NetWare и ее поддержке можно узнать на сайте компании Novell по адресу: **www.novell.com**.

Особенности и версии NetWare

NetWare версии 3.2 представляет собой 32-разрядную сетевую операционную систему, которая поддерживает Windows 3.x/95/98/NT, а также UNIX, MacOS и DOS. В ОС NetWare 4.11, которая также называется IntranetWare, впервые появился компонент Novell Directory Services (NDS, служба каталогов Novell). ОС NetWare 5.x позволяет интегрировать локальные сети, глобальные компьютерные сети, сетевые приложения, интранет-сети и Интернет в одну глобальную сеть. ОС NetWare 6 (**http://nw6launch.novell.com/nw6launch/index.jsp**) объединяет дополнительную сеть и Web-ориентированные службы и способна поддерживать до 32 серверов в кластере и до 32 процессоров.

Компонент Novell Directory Services (NDS, служба каталогов Novell) содержит в себе службы разрешения имен, а также службы безопасности, маршрутизации, обмена сообщениями, управления, Web-публикации, печати и управления файлами. На основе архитектуры каталогов X.500 этот компонент организует все сетевые ресурсы (в том числе пользователей, группы, принтеры, серверы и тома). Кроме того, компонент NDS предоставляет пользователю единый доступ ко всем серверам сети и позволяет ему использовать свои обычные права и полномочия.

Службы NetWare

NetWare Client (Клиент NetWare) позволяет клиентской рабочей станции, на которой этот компонент установлен, использовать все службы, предоставляемые NetWare Server, в том числе файловые службы, а также службы безопасности, печати и обмена сообщениями.

Файловые службы

Файловые службы NetWare являются частью базы данных NDS. Компонент NDS обеспечивает единый доступ к серверам сети и позволяет как пользователям, так и администраторам не только просматривать сетевые ресурсы одинаковым образом, но и просматривать всю сеть в том формате, который поддерживается операционной системой рабочей станции. Например, клиент Windows NT может отобразить в виде логического диска любой том или каталог файлового сервера NetWare, и ресурсы NetWare будут показаны как логические диски на его компьютере. Такие логические диски функционируют как любой другой диск на рабочей станции.

Сегодня Интернет связывает почти каждую компьютерную сеть с каждой другой компьютерной сетью. Тем не менее получить доступ к файлам, находящимся в одной компьютерной сети, из другой сети довольно не просто, а иногда и невозможно. Вместе с NetWare 6 фирма Novell стала поставлять компонент iFolder, который уменьшает ограничения, традиционно привязывавшие пользователей к их конкретному оборудованию. Кроме того, компонент iFolder устраняет проблему местоположения как наиболее важный аспект доступа к файлам и предоставляет инструменты для синхронизации, резервирования и использования файлов или приложений в любом месте и в любое время.

Службы безопасности

NetWare обеспечивает широкий диапазон безопасности. Система безопасности при регистрации обеспечивает аутентификацию пользователя по имени и паролю, а также ограничения на доступ по времени и по бюджету учетной записи. Опекунские права (trustee rights) определяют, к каким каталогам и файлам пользователь может иметь доступ и какие действия он может совершать с ними. Свойства каталогов и файлов определяют, какие действия могут совершаться с ними (т. е. только чтение, запись, копирование, совместное использование или удаление).

NetWare 6 позволяет проводить аутентификацию каждого пользователя не только при доступе к каталогам. Простая регистрация дает доступ ко всем серверам сети независимо от типа или операционной системы (что достигается при помощи компонента Novell Account Management — Управление учетными записями Novell). Политики (policies), регулирующие работу групп пользователей или использование сетевых ресурсов, уменьшают время на администрирование сети и обеспечивают для пользователей и партнеров большую гибкость работы с сетью. Novell BorderManager Enterprise Edition — это мощный набор компонентов для управления безопасностью работы в Интернете, включающий в себя средства межсетевой защиты и аутентификации, инструменты для работы в виртуальных частных сетях и службы кэширования для компьютерных сетей любых размеров. BorderManager тесно интегрирован с eDirectory и обеспечивает первый уровень управления безопасностью, который устанавливает единый порядок регистрации и получения доступа к информации через любую внутреннюю или внешнюю сеть. Наиболее важные коммуникации внутри корпоративной сети или между компанией и ее партнерами могут быть обеспечены при помощи Novell Certificate Server (который входит в NetWare 6). Novell Certificate Server 2.0 представляет собой расширяемый продукт, предназначенный для выполнения криптографических задач на основе открытых ключей, и позволяет создавать, выпускать сертификаты и управлять ими. Сертификаты — это цифровые приложения, которые служат для идентификации отправителя сообщения. Кроме того, сертификаты предоставляют получателям простой способ зашифровать свой ответ.

Службы печати

Службы печати полностью прозрачны для пользователя клиентского компьютера. Любой запрос на печать, поступивший от клиента, перенаправляется на файловый сервер, откуда он передается на сервер печати, а затем пересылается на принтер (нужно отметить, что в качестве сервера файлов и печатного может выступать один и тот же компьютер). Для совместного использования могут быть предоставлены принтеры, которые подключены к серверу, к рабочей станции или непосредственно

к компьютерной сети через собственную сетевую плату. Службы печати NetWare поддерживают до 256 принтеров одновременно.

Управление сетевыми принтерами в NetWare осуществляется при помощи eDirectory, куда принтеры, очереди заданий на печать и печатные серверы помещаются в качестве объектов. Компонент eDirectory в NetWare 4.x сделал процесс печати более быстрым и надежным благодаря использованию тех же инструментов управления, которые используются для всех других сетевых ресурсов. Пользователям стало проще находить и использовать принтеры, чем раньше. Компонент Novell Distributed Print Services (NDPS, распределенные службы печати Novell) увеличил возможности управления печатью и поддержки пользователя. В NetWare 6 возможности печати еще более широкие благодаря опции "наилучшая сетевая печать" ("best network print" option), на основе которой построен компонент Novell Internet Printing. Этот компонент построен с использованием Internet Printing Protocol (RFC-2910-1), одобренного проблемной группой проектирования Интернета (Internet Engineering Task Force, IETF), и предназначен для управления печатью посредством Web-браузеров и технологии Web-серверов.

Службы обмена сообщениями

NetWare позволяет пользователям обмениваться короткими сообщениями. Сообщения можно отправлять как отдельным пользователям, так и группам. Если все адресаты сообщения находятся в одной группе, то вы можете просто отправить это сообщение всей группе, а не каждому пользователю по отдельности. Пользователи могут включать и отключать получение сообщений на их рабочую станцию. Если пользователь отключает получение сообщений, никакие из отправленных сообщений не будут получены рабочей станцией. Кроме того, сообщения могут обрабатываться посредством службы обработки сообщений (Message-Handling Service, MHS). Эту службу можно установить на любой сервер и настроить для работы в качестве полноценной системы сообщений, выполняющей распределение электронных сообщений. Служба MHS поддерживает большинство популярных программ электронной почты.

Межоперабельность NetWare

В других операционных системах предусматривается клиентское программное обеспечение, предназначенное для взаимодействия с серверами NetWare. Например, в ОС Windows NT для этого служит Gateway Service for NetWare (GSNW). Эта служба позволяет использовать сервер сети Windows NT в качестве шлюза в сеть NetWare. Через сервер Windows NT любая рабочая станция сети Windows NT может запрашивать ресурсы и службы, имеющиеся в сети NetWare. После этого запроса сервер Windows NT будет выступать в роли клиента для сети NetWare и выполнять обмен запросами между этими двумя сетями. При помощи этой же службы GSNW сервер Windows NT может получать доступ к файловым службам и службам печати в сети NetWare.

Частные (фирменные) протоколы (например, IPX или DECnet) привели к появлению таких стандартных протоколов, как TCP/IP. Тем не менее еще существует множество других протоколов, и ОС NetWare 6 поддерживает различные протоколы, каждый из которых является стандартом на своих рынках. Файловые протоколы

позволяют разным клиентским машинам взаимодействовать с файловой системой NetWare. При помощи NetWare 6 вы можете подключить компьютер iMac к своей сети и сразу же получить доступ к файлам на сервере NetWare 6 без необходимости устанавливать какое-либо дополнительное клиентское ПО. Это же верно и для клиента Windows, рабочей станции UNIX, клиента FTP или Web-браузера. Цель в том, чтобы использовать уже существующую инфраструктуру, опираясь на преимущества каждой платформы и клиента, а не заменять эту инфраструктуру.

Linux

В конце 1998 года большое внимание стала привлекать упрощенная версия операционной системы UNIX, которая называется Linux. Со времени своего появления в 1991 году (и открытия исходного кода в 1993 году) ОС Linux разрабатывалась при участии сотен программистов по всему миру. Развитие этой операционной системы было ускорено благодаря тому, что ее исходный код распространяется бесплатно, и люди могут изменять его любым образом с одним условием: любые дополнения и улучшения должны быть общедоступными. Создатель этой операционной системы Линус Торвальдс (Linus Torvalds) сам определяет, какие изменения должны войти в нее, и нужно сказать, что не все предлагаемые изменения включаются в "официальную" версию.

По мере того как Linux становится все более популярной операционной системой среди разработчиков, производителей оборудования и программного обеспечения, компания Microsoft все больше беспокоится о том, что эта ОС представляет угрозу для Windows. И для этого есть основания, поскольку эту систему создает группа преданных своему делу разработчиков. Кроме того, Linux работает на компьютерах x86, Digital Alpha и станциях Sun SPARC, а значит, она более гибка, чем Windows NT, которая работает только с машинами x86 и Digital Alpha. Также Linux относительно менее требовательна к аппаратным ресурсам. Например, Linux позволяет превратить в Web-сервер даже компьютер на основе процессора 486, тогда как системные требования Windows 2000 *во много раз* выше.

На сегодняшний день Linux является самой быстро развивающейся серверной ОС, и ее все чаще устанавливают на обычные машины. В отличие от фирменных операционных систем, Linux можно установить и модернизировать бесплатно, что делает ее чрезвычайно привлекательной для тех компаний, которые не имеют большого бюджета, но хотят, чтобы у них была превосходная операционная система. Однако цена — это не главный фактор ее популярности. Многие компании — как большие, так и маленькие — предпочитают Linux просто потому, что она надежна в работе. Сообщают о случаях, когда эта операционная система бесперебойно работала месяцы и даже годы без перезагрузки. Поскольку исходный код открыт, ошибки в нем можно легко и быстро исправить, не ожидая, пока будут выпущены "официальные" заплаты. Кроме того, компании ценят открытость кода потому, что это дает возможность нескольким компаниям объединяться для того, чтобы вместе решать проблемы в программном обеспечении, не беспокоясь об антимонопольном законодательстве. Linux можно установить практически на любую машину (включая устаревшие модели), и она обеспечивает высокую степень гибкости, которая недостижима с другими операционными системами.

Ограничения Linux

Тем не менее Linux вряд ли сможет в ближайшее время покорить рынок персональных компьютеров. Пользователи могут скачать эту операционную систему с FTP-сайта компании Red Hat (**www.redhat.com**), заказать ее на компакт-диске или даже купить в компьютерном магазине. Хотя все больше компаний используют эту операционную систему для своих серверов, ее ограничения, связанные с оборудованием и совместимостью с приложениями, продолжают сдерживать ее распространение среди пользователей, которые отдают предпочтение Windows NT или 2000.

Важным моментом, ограничивающим использование Linux в качестве ОС, является способ разделения времени обработки данных. Если в Windows NT и других основных коммерческих ОС разделение процессорного времени происходит *по потокам* для операций ядра, то в Linux это происходит по процессам, что делает разделение ресурсов процессора намного менее четким. Потоки, запущенные пользователем (при работе приложений), также распределяются таким образом, что приложения в Linux работают медленнее, чем приложения, разработанные для Windows NT или 2000. На практике, Linux действует как Windows 3.x, используя кооперативную многозадачность для того, чтобы приложения освобождали процессор по завершению своей работы. В современных 32-разрядных версиях Windows используется вытесняющая многозадачность, которая требует от приложений освобождать процессор через регулярные промежутки времени. Наконец, код Linux разработан таким образом, что эта ОС может работать только на одном процессоре, поэтому она не может работать с многопроцессорным оборудованием. Следовательно, с ней несовместимы некоторые приложения для серверов предприятий.

Будущее Linux

Несмотря на свои ограничения, Linux можно получить от множества поставщиков программного обеспечения. Разработчики этой ОС постоянно улучшают ее для того, чтобы расширить ее функциональность, увеличить гибкость и повысить ее производительность на большем количестве платформ. Версии Linux (например, Red Hat 7.2) используются многими крупными корпорациями и отдельными пользователями для серверов и персональных компьютеров. Linux сегодня является одной из наиболее мощных и надежных систем, и благодаря своему открытому коду может быть изменена в соответствии с потребностями пользователей.

Другие операционные системы

Хотя Windows NT/2000 и NetWare, безусловно, сегодня наиболее популярные сетевые операционные системы, они вряд ли являются единственными. В числе прочих распространенных продуктов можно также встретить UNIX, AppleTalk и Banyan VINES. Кроме того, Windows 95/98/SE могут служить в роли клиентов в других операционных системах. В этой части главы мы дадим краткое описание этих операционных систем.

UNIX

ОС UNIX продолжает оставаться гибкой, универсальной, многозадачной и многопользовательской операционной системой. Она существует в двух основных версиях:

Linux и Solaris (фирмы Sun Microsystems). Хотя ОС UNIX изначально была разработана специально для больших компьютерных сетей, она может применяться и для персональных компьютеров (Linux становится все более популярной в качестве настольной операционной системы). Вообще говоря, операционная система UNIX состоит из одного центрального компьютера и множества терминалов для индивидуальных пользователей. UNIX хорошо работает как на независимых компьютерах, так и в сетевой среде.

ОС UNIX обладает очень гибкими возможностями для адаптации в сетевой среде типа "клиент-сервер". Она может использоваться в качестве операционной системы для файлового сервера, и в этой роли она может обрабатывать запросы рабочих станций. Программное обеспечение для файлового сервера в этой операционной системе становится простым приложением, которое работает в многозадачном компьютере. Сервер UNIX может поддерживать клиентов, работающих под DOS, OS/2, Windows или MacOS 7/8 (посредством файлового редиректора рабочая станция сможет сохранять и запрашивать UNIX-файлы, как если бы они были в исходном формате клиента).

AppleTalk

Поддержка компьютерных сетей Apple полностью интегрирована в операционную систему каждого компьютера, работающего под управлением MacOS. Первая версия (под названием LocalTalk) была довольно медленной в работе, но предоставляла пользователям необходимые сетевые возможности. LocalTalk продолжает входить в состав ОС Apple. Службы каталогов AppleTalk основаны на *зонах* (zones), т. е. логических группах, объединяющих компьютерные сети и сетевые ресурсы. Эти зоны позволяют группировать сетевые ресурсы в функциональные единицы. Например, сеть AppleTalk phase 1 состоит из не менее чем одной зоны, тогда как сеть AppleTalk phase 2 может включать в себя до 255 зон. Однако эти две модификации несовместимы друг с другом и с трудом поддерживают одинаковые сетевые кабельные системы.

Текущая версия AppleTalk предоставляет высокоскоростные одноранговые сетевые возможности для объединения компьютеров Apple. Кроме того, она обеспечивает способность к взаимодействию с другими компьютерами и сетевыми операционными системами. Однако эта межоперабельность не является частью ОС Apple. Пользователям других компьютеров (не Apple) проще всего получить доступ к ресурсам в сети Apple посредством протокола Apple IP (вариант протокола TCP/IP для Apple). Протокол Apple IP позволяет получать доступ к Apple-ресурсам (например, файлам баз данных) с не-Apple компьютеров. Компьютеры, которые работают под управлением сетевой операционной системы Apple, могут соединяться с другими компьютерными сетями посредством служб, поставляемых производителями этих других сетевых операционных систем, установленных на их сетевых серверах. Например, в операционных системах Windows NT Server, Novell NetWare и Linux есть службы, предназначенные для взаимодействия с Apple. Это позволяет пользователям Apple обращаться к ресурсам в этих сетях.

Banyan VINES

Banyan VINES (сокр. от Virtual Networking System — виртуальная сетевая операционная система) — это еще одна сетевая операционная система типа "клиент-сервер".

Она основана на протоколах Xerox Network Systems. Текущая версия ОС Banyan VINES содержит в себе программное обеспечение для обмена сообщениями Intelligent Messaging и BeyondMail. Сетевые службы создаются и управляются посредством последней версии интерфейса StreetTalk Explorer. Этот интерфейс работает с пользовательскими профилями Windows, что позволяет каждому пользователю применять свои настройки при перемещениях по сети. Кроме того, ОС VINES поддерживает основанное на TCP/IP программное обеспечение межсерверного обмена, управляет работой до четырех процессоров и включает в себя клиентскую поддержку рабочих станций Windows NT, Windows 95/98. Программное обеспечение Banyan Intranet Connect обеспечивает удаленный клиентский доступ посредством стандартного Web-браузера.

Популярные клиентские операционные системы

Как следует из сказанного в этой главе, для того чтобы получить доступ к компьютерной сети или ее ресурсам, клиентская машина не обязательно должна управляться сетевой операционной системой. Кроме распространенных клиентских СОС, таких как Windows 2000 Professional или Windows NT Workstation, существуют и другие ОС, которые могут взаимодействовать со многими современными версиями СОС, хотя только в роли клиента (рабочей станции). Двумя распространенными "клиентскими" операционными системами являются Windows ME и Windows 98/SE.

Windows ME

Для того чтобы усилить свои позиции на рынке домашних пользователей ПК, компания Microsoft выпустила в сентябре 2000 года ОС Windows Millennium Edition (ME). Хотя тестирования не выявили существенного повышения ее производительности в сравнении с Windows 98/SE, ОС Windows ME содержит большое количество улучшений, прежде всего связанных с развлечениями, мультимедиа и домашними компьютерными сетями.

Основными улучшениями в Windows ME (в сравнении с Windows 98/SE) являются мультимедийные средства, например: автоматический видеоредактор с мощными возможностями сжатия данных и импорта из видеокамер, мастер работы с автоматическим захватом изображений со сканера и фотокамер и инструмент для работы с многодисковыми устройствами чтения и записи медиаданных. Новые возможности защиты системы дает мастер, который позволяет вернуть неустойчиво работающую систему в предыдущее состояние, а новые средства установки упрощают доступ к домашним и широкополосным компьютерным сетям. Кроме того, поддержка спецификации Universal Plug-and-Play позволяет этой операционной системе взаимодействовать с такими устройствами, как холодильник или переносной компьютер (хотя эти возможности не всегда необходимы).

Есть еще два важных изменения — во-первых, это удаление стандартной для Windows 9x опции перезагрузки или загрузки в MS-DOS (хотя сохранилась возможность запускать DOS-приложения в специальном окне DOS) и, во-вторых, это капитально переделанные службы работы с Интернетом, которые повысили производительность ОС. В Windows ME используется тот же интерфейс рабочего стола, что и в Windows 2000 Professional, а также новый стек TCP/IP, который соединяется с Интернетом, но несовместим с некоторыми широко используемыми программами

работы с Интернетом. Существенно была улучшена система помощи: в ней были изменены средства устранения неполадок и появились дополнительные сообщения об ошибках. В целом система стала более удобной как для эксперта, так и для начинающего пользователя.

Утилита System Restore (Восстановление системы) создает резервные копии важных системных файлов в то время, как компьютер простаивает — таким образом, после каждых десяти часов работы на компьютере создается "мгновенный снимок" состояния системы. Кроме того, в любой момент времени можно принудительно создать дополнительный "снимок" при помощи мастера системного восстановления (System Restore Wizard). Если система перестает работать, но остается возможность перезагрузки (хотя бы в безопасном режиме, Safe Mode), вы можете запустить этот мастер, чтобы выбрать любое из сохраненных состояний для восстановления системы. Этот механизм не сохраняет текущее состояние документов и электронной почты, но позволяет восстановить поврежденные системные файлы. Компонент System Restore включается в тот момент, когда вы удаляете какие-либо важные файлы в каталоге Windows или Program Files. Например, если вы удалите данные из каталога Program Files, Windows в фоновом режиме восстановит их.

Механизм System File Protection (основанный на аналогичной утилите Windows File Protection в Windows 2000) запрещает приложениям заменять важные DLL-файлы на старые или нестандартные версии и предназначен для того, чтобы значительно уменьшить риск нарушения работы других программ из-за установки какого-либо нового приложения. Кроме того, имеется опция автообновления системы (AutoUpdate), которая в фоновом режиме скачивает новые версии системных файлов и затем предлагает их к установке.

Мультимедиа

Программа Windows Movie Maker записывает видеоизображение с присоединенной видеокамеры или импортирует существующие файлы и затем разбивает его на клипы для редактирования при помощи технологии, которая была заимствована из профессионального программного обеспечения для редактирования видео. Существующие видеофайлы можно импортировать из стандартных форматов (кроме RealMedia), но экспорт данных возможен только в формате Windows Media Format — форматы AVI и MPEG недоступны.

Функция Windows Image Acquisition (WIA) включает в себя мастер для предварительного просмотра, создания и управления изображениями, получаемыми при помощи сканеров и цифровых фотокамер. Основные функции могут быть использованы с любым сканером, поддерживающим Plug-and-Play, но с камерами, совместимыми с WIA, вы можете просматривать и управлять изображениями без необходимости их скачивания. На рынке сегодня существует более 60 моделей цифровых фотокамер (включая самые выпускаемые в последние месяцы), поддерживающих функцию WIA. Этот мастер работает автоматически при подключении к компьютеру подобной фотокамеры (через порт USB) или сканера.

Проигрыватель Windows Media Player 7 работает с большинством стандартных аудио- и видеоформатов за исключением RealMedia и снабжен тюнером для прослушивания радио через Интернет, средством для работы с многодисковыми устройствами и утилитой для переноса файлов, которая может копировать и сжимать существующие файлы или потоковые данные на переносные MP3-плееры и устройства Windows

CE. Проигрыватель Windows Media Player 7 имеет более простой интерфейс, чем в большинстве других медиапроигрывателей, но занимает довольно много экранной памяти для того, чтобы иметь более привлекательный внешний вид. Кроме того, эта программа более подвержена сбоям, чем все другие программы в Windows ME.

Сетевые возможности

Мастер создания домашних сетей позволяют установить и настроить функции совместного использования файлов, принтеров и Интернета при работе на машине с установленной операционной системой Windows ME и соединенной с любой одноранговой сетью. Кроме того, мастер позволяет создать диск для установки сетевого ПО из состава Windows ME на другие компьютеры, которые вы хотите включить в данную сеть, даже если они работают под управлением Windows 95/98. В Панели управления появился новый элемент (Folder Options), при помощи которого можно устанавливать файловые ассоциации и другие настройки. Здесь же можно установить флажок, позволяющий скрыть в окне Проводника важные системные файлы, защитив их от неправильного использования.

Если вы когда-нибудь устанавливали домашнюю сеть, или виртуальную частную сеть, или программное обеспечение для широкополосных сетей под управлением Windows 95 или 98, вы, вероятно, сталкивались с сообщением об ошибке, в котором говорилось, что вы можете использовать только шесть экземпляров соединения TCP/IP. Это означало, что Windows 9x могла установить соединение с Интернетом не более чем для шести сетевых компонентов и что для нового подключения не было доступных интернет-соединений. Новое программное обеспечение для работы через TCP/IP, которое появилось в Windows ME, позволяет устранить это ограничение и устанавливать любое количество сетевых подключений.

В состав Windows ME входит Internet Explorer 5.5 и Outlook Express 5.5, однако единственным заметным улучшением в сравнении с предыдущими версиями является функция предварительного просмотра при печати в программе Internet Explorer. В состав Windows ME также входит программа NetMeeting 3.1, но ее компоненты, предназначенные для использования в домашней сети, можно получить только в версиях, доступных через Интернет.

Рекомендации по модернизации

Итак, следует ли рекомендовать своим клиентам переходить на Windows ME? Хотя в Windows ME содержится множество инструментов для домашних пользователей, стабильность этой операционной системы вызывает некоторые вопросы. Тесты показывают, что Windows ME работает несколько *медленнее*, чем Windows 98/SE. Поэтому, как правило, следует немного подождать, пока разработчики не выполнят доводку этой операционной системы (и пока не появится один или два сервисных пакета для нее), прежде чем переходить с Windows 98/SE на Windows ME.

Windows 98

По мере того как для персональных компьютеров появлялось множество новых аппаратных стандартов и устройств, операционная система Windows 95 все меньше могла использовать эти новые системные ресурсы. Windows 98 была разработана на основе Windows 95 посредством внесения в нее большого набора исправлений и улучшений для получения полноценной 32-разрядной операционной системы. По-

явились новые мастера (wizards), утилиты и ресурсы, которые заметно повышают устойчивость работы системы. Повысилась производительность выполнения многих основных задач, в том числе запуска приложений, системной загрузки и закрытия. Полная интеграция с Интернетом обеспечивает работу в оперативном режиме и расширяет функциональность системы. Выпуск Windows 98 много раз откладывался и наконец состоялся в июне 1998 года. В сентябре 1999 года была выпущена ее улучшенная версия под названием Windows 98 Second Edition (вторая редакция, или Windows 98 SE), которая появилась после приблизительно года работы, посвященной ее изучению и улучшению (рис. 4.3). После этого компания Microsoft выпустила Windows ME (Millennium Edition), которая была предназначена для широкого спектра домашних пользователей, однако Windows 98/SE продолжает оставаться гибкой операционной системой, распространенной как среди домашних пользователей, так и в малых предприятиях. Приведем наиболее значимые особенности и функции Windows 98/SE.

- Утилита резервирования. Новая программа поддерживает накопители на магнитной ленте через интерфейс SCSI и позволяет упростить процесс резервирования информации и сделать его более комплексным.

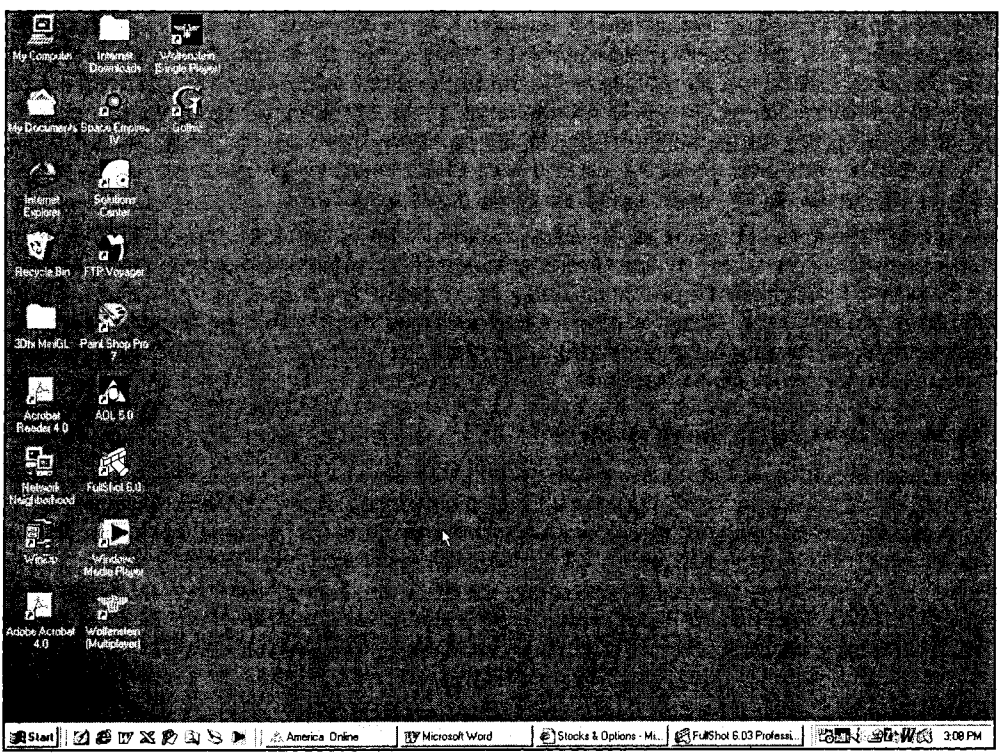


Рис. 4.3. Рабочий стол в Windows 98/SE

- Архитектура поддержки широковещательных сетей. При установке ТВ-тюнера Windows 98 позволяет принимать и отображать телевизионный сигнал и другие

данные, распространяемые через широковещательные сети, включая специальные телевизионные программы, в которых передача стандартного ТВ-сигнала сочетается с информацией в формате HTML.

- Улучшенная работа через коммутируемое соединение (dial-up). Функция сетевого соединения посредством телефонных линий была модернизирована в Windows 98. Была обеспечена поддержка сценариев, а также поддержка агрегирования многозвенных соединений (multilink channel aggregation), которое позволяет сочетать возможности всех доступных телефонных линий для повышения скорости передачи информации.
- Мастер дефрагментации жесткого диска. Этот новый мастер использует процесс дефрагментации жесткого диска для повышения скорости работы наиболее часто используемых приложений.
- Улучшение в конфигурации работы дисплея. Улучшенные настройки дисплея позволяют динамически изменять параметры разрешения и глубины цвета. Также появилась возможность изменять частоту обновления видеосигнала при использовании большинства новых графических адаптеров.
- DCOM (сокр. от Distributed Component Object Model — распределенная модель компонентных объектов). Windows 98 обеспечивает инфраструктуру, которая позволяет DCOM-приложениям (эта технология также известна под названием Network OLE) взаимодействовать между собой посредством компьютерных сетей без необходимости модернизировать эти приложения.
- Dr. Watson. Windows 98 содержит улучшенную версию утилиты Dr. Watson. При возникновении сбоя в работе программного обеспечения (например, ошибка в работе приложения или системный сбой) эта утилита анализирует ситуацию и сообщает о том, в каком программном обеспечении возникла ошибка (и почему). Dr. Watson также собирает подробную информацию о состоянии системы в момент сбоя. При этом создается регистрационный файл, который может помочь техническому специалисту разрешить проблему. Утилита Dr. Watson по умолчанию не запускается. Ее следует запускать вручную или через ярлык в стартовом меню.
- Более быстрый процесс закрытия системы. Время закрытия системы значительно сократилось в Windows 98.
- FAT32. FAT32 является улучшенной версией файловой системы FAT и позволяет форматировать диски емкостью более 2 Гбайт. Кроме того, в FAT32 используются кластеры меньшего размера, чем в FAT, что позволяет более эффективно использовать пространство больших дисков.
- Поддержка стандарта IrDA 3.0. Windows 98 поддерживает стандарт Ассоциации передачи данных в инфракрасном диапазоне (Infrared Data Association, IrDA) для установления беспроводных соединений с периферийными устройствами или другими компьютерами. Взаимодействуя с другими устройствами через инфракрасный порт, портативные или настольные компьютеры могут устанавливать сетевые соединения, передавать файлы или выводить данные на печать без помощи кабелей.
- Поддержка процессоров Intel MMX. Windows 98 обеспечивает поддержку программного обеспечения, предназначенного для работы с мультимедийными расширениями процессора Pentium (MMX и SSE). Это позволяет ускорить обработ-

ку аудио- и видеоданных при использовании новых поколений процессора Pentium.

- Совместное использование интернет-соединения (для Windows 98/SE). Эта функция позволяет конфигурировать домашнюю сеть для совместного использования одного соединения с сетью Интернет.
- Поддержка нескольких дисплеев. Эта функция позволяет использовать одновременно несколько мониторов и/или несколько графических адаптеров на одном компьютере.
- Поддержка NetWare Directory Services (NDS). Windows 98 включает в себя компонент Client Services for NetWare, предназначенный для поддержки Novell NDS. Этот компонент позволяет получать доступ к серверам Novell NetWare 4.x, в которых используется NDS, для получения доступа к файлам и службам печати.
- Поддержка нового оборудования. Windows 98 обеспечивает поддержку множества новаций, которые появились в области компьютерного оборудования за последние несколько лет, в том числе поддерживаются такие стандарты, как USB, IEEE 1394, AGP, ACPI и DVD.
- Модернизация поддержки спецификации PCMCIA. Для поддержки спецификации PCMCIA в Windows 98 было внесено несколько улучшений, в том числе поддержка PC Card32 (CardBus) для работы с приложениями, требующими большой пропускной способности — например, видеозахват или 100-мегабитовые компьютерные сети. Кроме того, была предусмотрена поддержка плат, работающих под напряжением 3,3 V, а также многофункциональных интегрированных плат (например, сетевых и модемных карт или SCSI и звуковых карт).
- Поддержка сетевой технологии PPTP. Протокол PPTP (Point-to-Point Tunneling Protocol — двухточечный туннельный протокол) позволяет использовать открытые сети (например, Интернет) для создания виртуальных частных компьютерных сетей, соединяющих клиентские ПК с серверами. Протокол PPTP обеспечивает такую инкапсуляцию данных, при которой возможна поддержка множества протоколов через соединение TCP/IP, а также шифрование данных, что повышает надежность передачи информации через незащищенные компьютерные сети.
- Улучшение управления режимом энергопотребления. В Windows 98 входит поддержка ACPI (Advanced System Configuration and Power Interface — усовершенствованный интерфейс конфигурирования системы и управления энергопитанием), а также APM 1.2 (Advanced Power Management — усовершенствованные средства управления энергопотреблением), в том числе функции выключения жесткого диска и модема PCMCIA, а также включения системы при поступлении телефонного звонка.
- Сервер удаленного доступа. Windows 98 включает в себя все необходимые компоненты для использования настольного компьютера в качестве сервера удаленного доступа (dial-up server). Это позволяет удаленным клиентам устанавливать соединение с данным сервером посредством телефонной линии для получения доступа к локальным ресурсам.
- Утилита настройки системной конфигурации (System Configuration utility). Эта утилита служит для настройки процедур запуска и закрытия системы. При помощи этой утилиты можно включать и отключать элементы в настроечных файлах AUTOEXEC.BAT, CONFIG.SYS, SYSTEM.INI, WIN.INI, что позволяет уст-

ранять конфликты и проблемы в конфигурации системы. Эта утилита заменяет собой Windows 95 Sysedit и значительно превосходит ее по функциональности.

- Программа проверки системных файлов (System File Checker). Данная утилита позволяет следить за изменениями или порчей системных файлов Windows 98 (*.dll, *.com, *.vxd, *.drv, *.ocx, *.inf, *.hlp и т. д.). Эта утилита также является удобным механизмом для восстановления измененных начальных версий системных файлов.
- Системная информация (System Information tool). Данная утилита позволяет получить полную информацию о системном оборудовании и программном обеспечении. В ней имеется меню **Tools** (Инструменты), в котором можно выбрать многие из новых утилит, предназначенных для устранения неполадок, ремонта и получения отчетов.
- Инструмент по устранению системных неисправностей (System Troubleshooter). Эта утилита автоматизирует процесс поиска и устранения неполадок в настройках системы. В ней предусмотрено определение конкретных областей и устройств. Список инструментов для устранения неполадок приводится в утилите Help.
- Инструмент ведения отчетов (Windows 98 Report tool). Эта программа запускается из меню **Tools** в утилите System Information и позволяет отправить отчет о проблеме в компанию Microsoft, при этом вся необходимая информация о системе включается в отчет автоматически.
- Проигрыватель Windows Media Player. Windows 98 поддерживает новую архитектуру передачи потоковых медиаданных ActiveMovie, которая обеспечивает высокое качество воспроизведения распространенных типов медиаданных, в том числе MPEG audio, WAV audio, MPEG video, AVI video и Apple QuickTiME video. Проигрыватель Windows Media Player поддерживает многие распространенные форматы аудио- и видеофайлов. С Web-сайта можно скачать обновления для этой программы и ее новые версии.
- Системное обновление (Windows System Update). Эта утилита позволяет получать самые новые драйверы и системные файлы. Данная Web-служба сканирует систему и определяет, какое аппаратное и программное обеспечение на ней установлено. Полученная информация сравнивается с базой данных на сервере Microsoft, чтобы определить, какие новые драйверы или системные файлы необходимо установить. Если новые версии имеются, служба системного обновления может установить их автоматически.

Дополнительные ресурсы

AppleShare: **www.apple.com/applesharеip/**.

Linux: **www.redhat.com**.

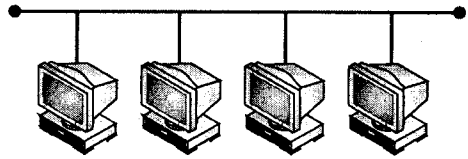
Novell NetWare: **www.novell.com**.

UNIX: **www.unix.com**.

Windows 2000: **www.microsoft.com/windows2000**.

Windows NT: **www.microsoft.com/windows/default.asp**.

Windows XP: **www.microsoft.com/windowsxp**.



ГЛАВА 5

Службы каталогов, присваивания имен и Интернета

В современных компьютерных сетях действует масса разнообразных служб. Некоторые из них применяются для идентификации компьютеров и других устройств, иные помогают обнаруживать местонахождение объектов в рамках сети, а есть службы, которые делают Интернет более удобным местом для работы и посещений. В этой главе речь пойдет обо всех этих службах — о том, как они работают, а также о наиболее вероятных источниках неприятностей.

Сначала мы рассмотрим службы каталогов. Так называются средства, помогающие обнаружить в компьютерной сети любой объект — будь то принтер, документ, пользователь или группа пользователей. Мы поговорим о стандартных блоках, на основе которых строятся службы каталогов, а затем обсудим конкретные службы, предлагаемые компаниями Microsoft и Novell.

Далее разговор пойдет о службах присваивания имен. Они являются средством преобразования таинственных адресов IP-протокола в нечто более удобное для восприятия человеком. Для выполнения разных задач предназначены различные службы присваивания имен, будь то доменная система имен (Domain Name System, DNS) или служба имен Интернета для Windows (Windows Internet Naming Service, WINS). Кроме того, мы рассмотрим протокол динамической конфигурации хоста (Dynamic Host Configuration Protocol, DHCP), упрощающий процесс назначения IP-адресов.

Наконец, "интернет-службы" — это общий термин, обозначающий различные компоненты сети Интернет. Какой бы протокол ни применялся для загрузки Web-страниц, передачи файлов или отправки электронной почты, он подкрепляется незаметной работой множества других протоколов.

Службы каталогов

Если вам понадобится кого-то найти, вы, вероятно, возьмете телефонный каталог, чтобы выяснить номер телефона, а может быть — даже адрес этого человека. Кроме того, чтобы разыскать номер телефона, добавочный номер или адрес электронной почты искомого лица, вам могли бы пригодиться церковная книга или реестр служащих компании. При поиске объекта в компьютерной сети применяется служба каталогов, причем механизм ее использования не слишком сильно отличается от вышеприведенного. Впрочем, в данном случае каталог хранится на сетевом сервере,

а в его записях содержится информация, связанная с группами пользователей, принтерами, папками и файлами. К тому же службы каталогов применяются при выполнении таких задач, как обслуживание электронной почты, аутентификация пользователя и обеспечение безопасности в сетях. Более того, такой каталог недоступен для пользователей. Обращаться к этим службам могут приложения, которым необходима помощь в выполнении их задач.

Использование служб каталогов позволяет автоматически отправлять приложения и обновления продуктов на компьютеры всех пользователей. Службы каталогов применяются для обеспечения таких функций безопасности, как однократное предъявление пароля, позволяющее пользователю, однажды зарегистрировавшись, в дальнейшем получить доступ к множеству защищенных областей и приложений, и при этом не подтверждать свои полномочия заново. В результате проще становится не только пользователю. Администратор сберегает время и силы, поскольку идентификация пользователя выполняется только один раз и может централизованно управляться с помощью службы каталогов. К примеру, в среде Windows служба Active Directory предусматривает управление полномочиями пользователя в рамках всей сети из единого центра. Более того, интеграция Active Directory с Microsoft Exchange обеспечивает комфортные условия труда как для пользователей, так и для администраторов.

Хотя службы каталогов привлекательны для сетевых администраторов, это не единственные люди, кто обретает выгоду. Пользователи получают преимущества в виде расширенной функциональности. К примеру, регистрация в сети с любого компьютера дает привычную среду окружения, включая опции рабочего стола, приложения и доступ к данным; при этом не имеет значения, находится ли пользователь за своим рабочим столом, в дороге или в помещении филиала компании.

Стандарт X.500

X.500 — это стандарт служб каталогов, предложенный Международным союзом по телекоммуникациям (International Telecommunications Union, ITU). Первоначально он был разработан в 1988 году, но пять лет спустя была выпущена новая версия X.500. Несмотря на то, что вариант 1993 года современнее, большинство реализаций X.500 еще следуют стандарту 1988 года.

В X.500 используется распределенный подход к службам каталогов, чтобы максимизировать его эффективность и работоспособность. В соответствии с ним, организация поддерживает свою информацию средствами одного или нескольких агентов системы каталогов (Directory System Agent, DSA). DSA представляет собой базу данных с двумя характерными чертами:

- информация хранится в структуре, организованной согласно спецификации X.500;
- существует возможность взаимного обмена информацией с другими DSA стандарта X.500.

Агенты службы каталогов в X.500 взаимосвязаны на основе древовидной модели, с которой мы более подробно ознакомимся далее в этой главе. Каждый DSA содержит часть *глобального каталога*, который является своеобразной дорожной картой системы в целом.

Все данные, хранящиеся в рамках служб каталогов X.500, фиксируются в записях. Каждая запись принадлежит по крайней мере к одному классу объектов. К примеру, если в пределах вашей организации вы захотите найти человека по имени Лари Хатчинсон, элемент `LarryHutchinson`, вероятно, будет являться членом объекта `Production`. Информация в рамках каждой записи определяется атрибутами. Например, атрибутами записи `LarryHutchinson` могут быть `JobTitle`, `PhoneNumber`, `EMailAddress`, и т. д.

Протокол LDAP

Стандарт X.500 не был идеальным решением для службы каталогов. Поскольку для большинства реализаций каталогов он был слишком сложным, в Университете штата Мичиган был разработан более простой протокол доступа к каталогам на основе TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/протокол Интернета), известный под названием "Упрощенный протокол доступа к службе каталогов" (Lightweight Directory Access Protocol, LDAP), для применения в сети Интернет.

В большинстве вычислительных сред сотрудники испытывают потребность в доступе к различным службам и приложениям наподобие принтеров и системы электронной почты, а также к совместно используемым файлам и папкам. По существу, им нужно обращаться к ресурсам, расположенным на разным платформам (Windows, NetWare, и т. д.). Для того чтобы эти ресурсы можно было систематизировать, необходима единая служба каталогов, которая смогла бы обеспечить подтвержденный доступ по всем направлениям. Эта служба каталогов должна не только поддерживать имена пользователей и пароли, но и хранить разные типы данных, как-то: данные о способах связи с клиентами, информацию о конфигурации приложений, и личные документы, в одном месте. Более того, сотрудники должны иметь возможность доступа к этой базе данных с любой рабочей станции сети, а при необходимости — и из удаленного местонахождения.

Деревья каталогов

Дерево каталогов — это иерархическая группировка доменов, совместно использующих одно и то же пространство имен. В отличие от настоящих деревьев, вершина этого дерева называется *корневым* доменом. Иногда как синоним употребляется термин "родительский домен". По мере того как мы опускаемся вниз по дереву, из него разрастаются субдомены (их также называют дочерними доменами).

В большинстве случаев структура любого дерева службы каталогов отражает корпоративную структуру соответствующей организации. В качестве примера рассмотрим рис. 5.1. В данном случае организация в целом обозначена сверху, подразделение располагается ниже организации, и т. д.

Естественно, что детали структуры от компании к компании варьируют, но стандартная компоновка остается неизменной. Независимо от того, какой службой каталогов вы пользуетесь (Active Directory или, скажем, NDS eDirectory), деревья способны обеспечить ту степень гибкости, которая необходима для формирования иерархической структуры любой организации.

Связь служб каталогов с древесной терминологией этим не ограничивается. Совокупность деревьев называется *лесом*. Несмотря на то, что у каждого дерева есть свое,

уникальное пространство имен, они объединяются в лес через доверительные отношения. Таким образом, если администратор одного из деревьев решает, что организация в достаточной степени связана с другим деревом, они входят в доверительные отношения, вследствие чего получают совместный доступ к ресурсам друг друга.

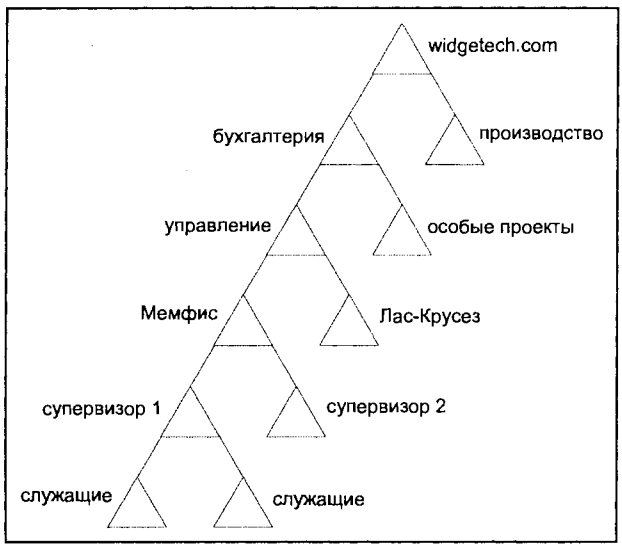


Рис. 5.1. Деревья каталогов воспроизводят организационную структуру компании

Резервирование

Нетрудно догадаться, что службы каталогов играют важную роль в организации. Если необходимая служба каталогов ухудшит свою работу или выйдет из строя, то для организации это обернется серьезными последствиями. Обычно, чтобы избежать проблем, базы данных служб каталогов размещаются и обслуживаются на нескольких серверах. Размещение баз данных более чем на одном сервере известно как *резервирование*. Это крайне важный принцип, т. к. если что-то случится с одним сервером (или его придется отключить от сети для проведения регламентных работ), перенять его обязанности в организации может другой сервер.

Резервирование чрезвычайно полезно, особенно в больших организациях, но множество серверов обеспечивают также функцию *выравнивания (балансировки) нагрузки*. Для примера представим себе организацию, которая располагает тысячей клиентских ПК. При условии поддержания трех серверов со службами каталогов ни один из них не будет нести нагрузку самостоятельно. Напротив, эти серверы можно настроить таким образом, чтобы клиентская нагрузка равномерно разделялась ими через сеть.

Синхронизация и репликация

Резервирование порождает необходимость в синхронизации и репликации. Именно благодаря синхронизации и репликации все серверы организации содержат одина-

ковую информацию в службах каталогов. Это крайне важно: не будь в базах данных службы каталогов на всех серверах организации самой свежей информации, результаты будут противоречивыми. Например, один пользователь может попытаться найти определенный ресурс в одной части организации (и найдет его), в то время как другой, обращающийся к другому серверу службы каталогов с устаревшей информацией, не сможет обнаружить тот же самый ресурс. Хуже того: если ресурс удален или перемещен, то в отсутствие новейших данных о его местоположении пользователи будут направляться туда, где его уже нет.

К примеру, в среде Windows NT среди серверов задействуется иерархическая модель. Согласно этой модели, существуют основные контроллеры домена (Primary Domain Controller, PDC) и резервные контроллеры домена (Backup Domain Controller, BDC). Это замечательный способ взять под контроль особенности конкретной сети, т. к. в случае отказа PDC один из BDC возьмет на себя его обязанности. Иллюстрация этой модели приводится на рис. 5.2.

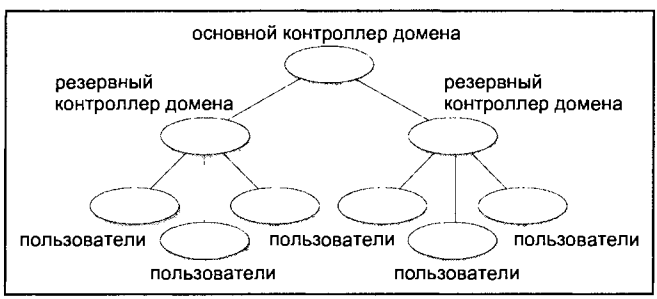


Рис. 5.2. Иерархия основных/резервных контроллеров домена

Если BDC вызывают для замены PDC, ему потребуется текущая версия информации, которой ранее пользовался PDC, наподобие ведущей базы данных пользователей. Когда PDC разделяет свою базу данных с BDC, он синхронизирует ее. Впрочем, между синхронизацией и репликацией есть различия.

В средах, в которых присутствуют службы каталогов, иерархическая модель с участием PDC и BDC не употребляется. Все контроллеры домена в них равноправны. Например, при переходе Microsoft с Windows NT на Windows 2000 (а теперь и на .NET) помимо цветов экрана по умолчанию и шрифтов изменились многие вещи. В частности, ОС Windows 2000 ознаменовала появление в среде Windows контроллеров домена (Domain Controller, DC).

По большей части, как показано на рис. 5.3, обязанности между контроллерами домена распределены поровну. Некоторые контроллеры могут брать на себя дополнительные обязательства (как-то: размещение DNS-серверов и другие задачи), но все они разделяют основные обязанности по сопровождению базы данных сетевых объектов, размещенных в домене. Так как все DC равноправны, процесс координации ими информации о доменах называется *репликацией*. Рассматриваемая сеть показана на рис. 5.4.

В этой сети полдюжины контроллеров домена совместно пользуются каналами как локальной, так и глобальной сети. В каждой области два DC удовлетворяют потреб-

ности локальной сети в службах каталогов. Так как всего контроллеров домена шесть, существует необходимость в обмене информацией между ними через глобальную сеть. Таким образом, контроллер A сверяет свою базу данных с контроллером B; тот координирует свои данные с контроллером C, и т. д., пока согласование информации всех контроллеров не будет завершено.

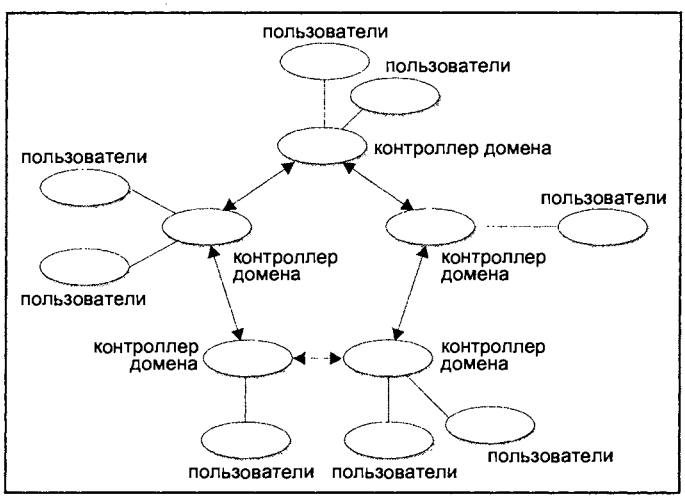


Рис. 5.3. Рабочая нагрузка поровну распределяется между контроллерами домена

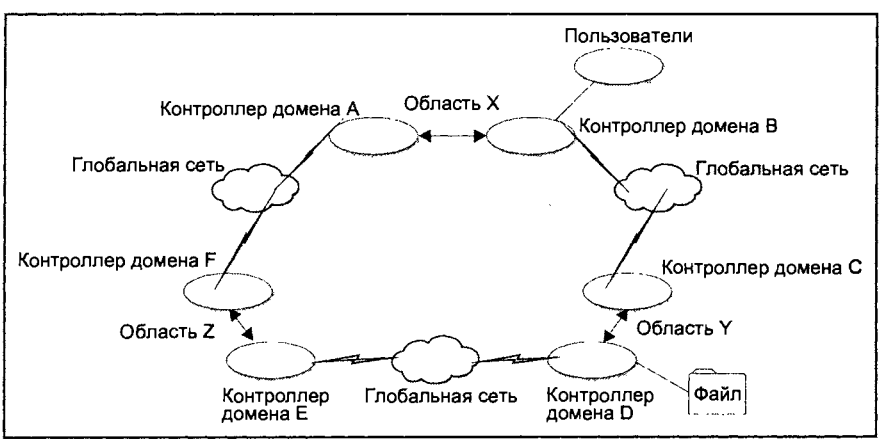


Рис. 5.4. Расположение контроллеров домена и необходимость в репликации

Синхронизация выполняет важную функцию, обеспечивая возможность нахождения объектов (пользователей, файлов, устройств и т. д.) в любой области сети. К примеру, если пользователь в области X попытается обратиться к файлу, который содержится в области Y, он воспользуется услугами локального контроллера домена. Как таковой, этот контроллер домена должен знать, где искать затребованный файл.

Служба Active Directory

Центральной функцией, обеспечивающей управляемость Windows 2000, является служба каталогов под названием Active Directory (AD). Проще говоря, Active Directory — это база данных целой сети. В ней содержатся таблицы данных о различных атрибутах объектов вашей системы.

Преимущества AD

AD представляет собой исключительно ценный метод управления сетевыми ресурсами. Система берет традиционные службы каталогов и позволяет управлять ими со значительно большей степенью контроля и гибкости. Среди прочих преимуществ AD — следующие.

- Управление упрощено благодаря централизованному характеру базы данных Active Directory.
- В Active Directory используется не иерархическая структура, а ряд равноправных контроллеров домена. Это значит, что, если один из серверов, размещающих контроллеры домена, выйдет из строя, другие контроллеры возьмут исполнение его обязанностей на себя, в результате чего воздействие сбоя на работу вашего предприятия будет минимизировано. Средствами резервирования эта функция обеспечивает дополнительный уровень надежности.
- Расширены возможности масштабирования, что позволяет Active Directory хранить миллионы блоков информации без внесения изменений в административную модель.
- Каталоги с возможностью поиска позволяют быстро и с легкостью искать нужные данные среди сетевых ресурсов и служб.
- Active Directory характеризуется расширяемостью. Пользователь или приложение могут без труда добавлять в каталог дополнительные элементы данных.

Структура

Довольно важен способ конструирования Active Directory. Читая или воочию встречаясь со службами каталогов на основе X.500, вы наталкиваетесь на структурированный, иерархический метод организации ресурсов. Язык служб каталогов на основе X.500 включает организационные единицы (Organizational Unit, OU), домены, леса и деревья. Они же являются стандартными блоками не только для Active Directory, но и для других служб каталогов.

На рис. 5.5 изображена схема Active Directory и других служб каталогов. Организационными единицами называются группы людей, компьютеров, файлов, принтеров и других ресурсов, которые нужно объединить в один блок. Домены — это совокупности организационных единиц, деревья — совокупности доменов, леса — совокупности деревьев. Такая сетевая иерархия обеспечивает намного более четкий контроль над сетью и ее атрибутами.

Другим ключевым компонентом Active Directory является ее схема, т. е. внутренняя структура базы данных. Схема определяет взаимоотношения между классами объектов. Так, если возвратиться к примеру с адресной книгой, то в ней может присутствовать класс под названием `Name`, а в его составе — атрибуты, определяющие имя и

фамилию, а следовательно, в объектах класса `Name` обязательно должны содержаться данные об имени и фамилии. Одни классы могут наследовать от других, в результате чего выстраивается иерархия классов.

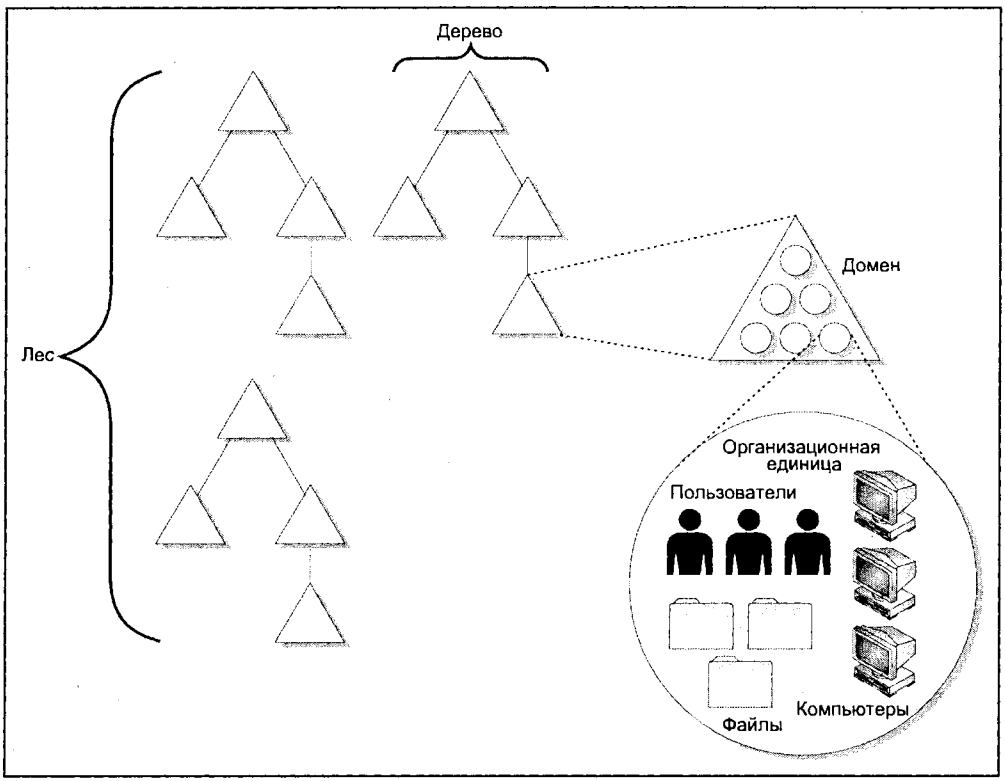


Рис. 5.5. Структура Active Directory

Симптомы неисправностей

Установка и использование Active Directory сопровождаются несколькими часто проявляющимися источниками неисправностей. В следующих разделах показано, как с ними можно бороться.

Симптом 5.1. Продвижение контроллера домена не имеет успеха

При переводе системы в среду Active Directory и при выдвижении PDC или BDC на позицию контроллера в существующем домене есть вероятность вывода сообщения о том, что данный домен не является действительным доменом Active Directory. Как правило, это — результат неполадок в DNS. Чтобы избавиться от этой проблемы, убедитесь в том, что система DNS корректно установлена и надлежащим образом функционирует.

Симптом 5.2. Мастер установки (Installation Wizard) зависает

Если процесс установки Active Directory зависает, проверьте соответствие показаний времени на каждом компьютере. Если часы на ваших компьютерах не синхронизированы, процесс инсталляции может висеть в течение нескольких часов. В данном случае лучше всего прервать установку, синхронизировать серверы и перезапустить мастер установки (Installation Wizard) Active Directory. Эта задача выполняется путем ввода в командной строке команды

```
net accounts /synch
```

Симптом 5.3. Пользователь домена не может войти в сеть

Если новый пользователь не может зарегистрироваться в домене, то происходит это, вероятно, из-за задержки репликации. Другими словами, пользовательская база данных еще не была скопирована в тот контроллер домена, через который осуществляется попытка входа в сеть. Вы можете либо подождать, пока репликация не произойдет сама собой, либо отрегулировать процесс репликации данного контроллера домена, устранив столь серьезное запаздывание. То же самое может произойти с пользователями, чьи пароли переустанавливались.

Примечание

Настройки репликации связаны с балансированием. Разумеется, можно сделать так, чтобы репликация происходила чаще, но вместе с тем в сети увеличатся непроизводительные издержки.

Если проблема все же будет повторяться, проверьте журналы регистрации событий и узнайте, действительно ли репликация контроллеров доменов проходит успешно.

Кроме того, когда пользователь испытывает затруднения при входе в сеть, следует удостовериться в том, что:

- на компьютере клиента все в порядке с конфигурацией TCP/IP;
- контроллер домена доступен;
- сервер с глобальным каталогом работает.

Примечание

Глобальный каталог — это индекс (упорядоченный список) с возможностью поиска, который позволяет пользователям находить объект в сети, не зная о том, в каком конкретно домене он размещен.

Мониторинг Active Directory

В целях отслеживания работы Active Directory и выполнения задач по выявлению неисправностей довольно часто применяются инструментальные средства контроля производительности и анализа. Очень мощной сервисной программой, входящей в состав серверов Microsoft Windows, является Performance Monitor (или System Monitor, как она называется, начиная с версии Windows 2000). Она способна выполнять мониторинг немыслимых объемов информации о вашей Windows-системе. Чтобы осуществить текущий контроль Active Directory, запустите Performance Monitor (для этого можно ввести `PERFMON.EXE` в командной строке), а затем выберите

пункт **NTDS** в списке отслеживаемых объектов. В табл. 5.1 приведены некоторые сервисные программы сторонних разработчиков, которые также могут быть использованы для мониторинга Active Directory.

Таблица 5.1. *Инструментальные средства сторонних разработчиков для мониторинга Active Directory*

Компания	Продукт	Web-сайт
NetPro	DirectoryTroubleshooter	**www.netpro.com**
IBM Tivoli	IBM Tivoli Monitoring	**www.tivoli.com**
NetIQ	NetIQ AppManager	**www.netiq.com**

Если вам придется восстанавливать систему из резервной копии с помощью Мастера восстановления (Restore Wizard), имейте в виду, что Active Directory можно восстановить только в исходное местоположение. Если для файлов состояния системы (System State) определить иное размещение, или же попытаться выполнить восстановление с удаленного компьютера, служба Active Directory восстановлена не будет.

Служба каталогов Novell (NDS)

Компанией Novell было предложено решение под названием eDirectory службы каталогов Novell (Novell Directory Services, NDS). В Novell очень гордятся NDS, утверждая, что этот каталог может содержать миллиард блоков информации и выполнять поиск по LDAP менее чем за секунду. Помимо прочего, NDS закладывает основу таких приложений Novel, как Certificate Server, digitalme, eGuide, iChain, Net Publisher и Single Sign-On.

Спроектированная с расчетом на NetWare, NDS, тем не менее, может работать в операционных системах Windows 2000/NT/XP, Solaris и Linux.

Безопасность

Подобно Active Directory от Microsoft, в состав eDirectory входит набор защитных компонентов, не дающий проходу "плохим парням".

- *Аутентификация.* Первый уровень обеспечения безопасности требует от пользователей подтверждения их прав при входе в сеть. Диапазон средств аутентификации простирается от паролей, кодируемый с помощью SSL (Secure Sockets Layer — протокол защищенных сокетов), до сертификатов X.509v3 и смарт-карт. Дополнительная аутентификация проходит в фоновом режиме, оставаясь незаметной для пользователя.
- *Международная криптографическая инфраструктура Novell* (Novell International Cryptographic Infrastructure, NICI). NICI — это криптографическое средство, которым разработчики могут пользоваться для обеспечения нужного уровня шифрования своих приложений без необходимости внедрения в них криптографии.

Примечание

Уровень шифрования зависит от региона, в котором используется данное приложение.

- *Служба безопасной аутентификации* (Secure Authentication Services, SAS). SAS — это модульная структура, предусматривающая услуги аутентификации следующего поколения. В настоящее время она обеспечивает поддержку SSLv3.

Управление

Novell предоставляет массу инструментов управления, которые призваны помочь вам скоординировать информацию в NDS. Среди них есть такие, которые окажут прямое (Novell Client) или косвенное (NDS Server) воздействие на ваши решения, связанные с интернет-коммерцией. Некоторые из этих инструментов приведены ниже.

- NDS Server. Размещает реплики NDS на основных (PDC) и резервных контроллерах домена (BDC).
- NetWare Administrator и ConsoleOne. Помогает управлять сетевыми пользователями и ресурсами.
- NDS Manager. Управляет разделами, репликами, серверами и схемой NDS.
- Novell Client. Предоставляет пользователям доступ к функциям NDS.
- LDAP. Обеспечивает открытую инфраструктуру для приложений, составленных в соответствии со стандартом Интернета.
- Bulkload Utility. Единовременно добавляет в каталог миллионы объектов.

Симптомы неисправностей

Некоторые аспекты NDS могут стать источниками возникновения проблем. Кое-какие из них могут показаться несущественными (например, временная синхронизация), но многие серьезные проблемы уходят корнями в мелкие детали. Ниже приведены некоторые источники проблем с NDS, относящиеся к самым коварным.

Симптом 5.4. У меня проблемы с синхронизацией серверов NDS

Убедитесь в том, что показания времени на всех серверных NDS синхронизированы. Время имеет большое значение, т. к. NDS отслеживает все изменения в базе данных NDS через временные метки. К примеру, если ваши NDS-серверы не синхронизированы, и при этом вы добавляете объект (скажем, нового пользователя), впоследствии вы будете немало удивлены, не обнаружив его в составе дерева NDS. Проблемы с синхронизацией времени могут возникать по одной из четырех причин:

- служба времени NetWare настроена некорректно;
- взаимодействие серверов может быть прервано вследствие повреждения оборудования;
- сервер был отключен, а показания времени CMOS не совпали с фактическими датой и временем его перезапуска;
- в настройках сервера указан неправильный часовой пояс.

Справиться с этой проблемой, в общем, несложно: просто обеспечьте полную временную синхронизацию ваших серверов друг с другом.

Симптом 5.5. Серверы времени должны быть правильно сконфигурированы

Помимо прочего, вам следует проверить точность конфигурации серверов времени. Это те серверы, к которым другие серверы обращаются в целях синхронизации времени. Службой NDS используются четыре типа таких серверов.

- Простой. Серверы этого типа отвечают на временные запросы от первичных и вторичных серверов времени, но в случае несоответствия между ними не производят изменений.
- Контрольный. Такие серверы отвечают на временные запросы от первичных и вторичных серверов времени, и в случае несоответствия между ними производят изменения.
- Первичный. Эти серверы отвечают на временные запросы от контрольных, других первичных и вторичных серверов времени. Они могут согласовывать незначительные изменения времени с другими первичными серверами.
- Вторичный. В основном, такие серверы получают показания времени от других временных серверов.

Чтобы получить более подробную информацию на тему выбора подходящего типа сервера времени и его конфигурации, зайдите на Web-сайт Novell's Support Connection по адресу **support.novell.com**, и с помощью функции Knowledgebase найдите документ под номером 10058645.

Симптом 5.6. "Сироты" доставляют проблемы

Внося изменения в объект в составе NDS, убедитесь в том, что его репликация выполнена в масштабе всей сети. Если изменение не передано по всей сети, вы рискуете оставить после своих действий "сирот". "Сиротами" называются подобъекты, лишившиеся родительского объекта. К примеру, если сервер печати удален, а принтер оставлен, последний становится "сиротой".

Чтобы проверить наличие" сирот", введите в серверной консоли следующие команды:

```
SET DSTRACE=+SYNCH
SET DSTRACE=*H
```

Если в процессе репликации произойдет ошибка −637, то, вероятно, на ваших серверах присутствует "сирота" (или "сироты"). Чтобы избавиться от нее, следуйте инструкциям документа № 100185121 на сайте **support.novell.com**.

Симптом 5.7. Обмен информацией между серверами нарушен

Если вы сталкиваетесь с нарушениями при взаимодействии серверов, то, может быть, у вас проблемы с "сиротами", или же серверы проводят часы напролет в попытках связаться друг с другом. Чтобы проверить наличие проблем, связанных с обменом информацией, введите в серверной консоли следующие команды:

```
SET DSTRACE=+SYNCH
SET DSTRACE=*H
```

Если произойдет ошибка −625, вам следует проверить каналы связи. Возможно, перегружены каналы глобальной сети или неисправны каналы локальной сети.

Симптом 5.8. Не установлены новейшие заплаты и обновления

Novell пытается решать проблемы с помощью ряда заплат и обновлений. Старайтесь получать их вовремя. Их список опубликован по адресу: **support.novell.com /misc/patlst.htm**.

Службы присваивания имен

У любого компьютера в сети есть уникальный адрес. Он позволяет другим сетевым устройствам определять местонахождение ПК. В дополнение к этому используются службы присваивания имен для того, чтобы сделать процесс нахождения Web-сайта в сети значительно проще, чем с помощью собственной Интернетовской схемы IP-адресации.

В этом разделе вопрос применения служб присваивания имен обсуждается более подробно. Наиболее распространенной службой такого типа является DNS. Она используется в Интернете, но становится популярной и в локальных сетях. К примеру, если набрать **www.whitehouse.gov** или любое другое доменное имя, именно DNS-сервер преобразует его в адрес, понятный для компьютера. DHCP является тем средством, с помощью которого компьютерам, регистрирующимся в сети, динамически назначаются персональные IP-адреса. DHCP полезен в том смысле, что он автоматизирует процесс IP-адресации. Компания Microsoft и здесь приложила руку, создав свою собственную систему именования под названием WINS. WINS — пока еще используемая служба, поддерживаемая ОС Windows, но в Microsoft было принято решение о переходе на DNS вместо WINS. Однако, поскольку WINS еще широко используется в Windows-доменах, здесь объясняется ее функционирование.

Доменная система имен (DNS)

Для того чтобы найти в сети Интернет определенный Web-сайт, вам нужно ввести унифицированный указатель ресурса (Uniform Resource Locator, URL) в адресную строку браузера. Из ряда уникальных доменных имен, объединенных с категорией организации, получаются адреса URL наподобие **www.whitehouse.gov**, **www.cocacola.com**, или **www.harvard.edu**.

Впрочем, URL облегчают жизнь только людям — они не являются настоящими IP-адресами. Чтобы компьютеры могли соединяться друг с другом через Интернет, применяются 32-разрядные IP-адреса, механизм действия которых аналогичен телефонным номерам. Для подсоединения к Web-сайту URL должен быть преобразован в IP-адрес. К примеру, если вы наберете в браузере URL **www.cocacola.com**, соответствующий запрос будет отправлен на ближайший DNS-сервер, который найдет для этого URL соответствие и преобразует его в IP-адрес (в этом случае — 209.98.82.71).

Такое преобразование совершенно необходимо, поскольку маршрутизаторы и коммутаторы не имеют ни малейшего представления о том, что такое доменное имя. На самом деле, даже для подачи запроса на DNS-сервер необходим его IP-адрес. В Интернете каждому адресу соответствует IP-адрес. Не будь DNS-сервера, переход на нужные нам сайты в сети Интернет посредством URL-адресов был бы невозможен.

Примечание

В Windows 2000 была представлена динамическая доменная система имен (Dynamic Domain Name System, DDNS). DDNS позволяет хостам помещать в таблицу DNS новые имена хостов и адреса по мере того, как они добавляются в сеть.

DNS в Windows

Как отмечалось ранее, служба каталогов Microsoft называется Active Directory. Важнейшую роль в обеспечении ее функциональности играет DNS. Наличие инфраструктуры DNS или плана ее инсталляции необходимо еще до начала установки Active Directory. Один из первых этапов планирования перехода на Windows 2000 или .NET состоит в учреждении доменного имени. Оно же будет доменным именем DNS. При разработке сети с Active Directory необходимо учитывать три важнейшие роли DNS, исполняемые в ходе операций с правилами именования, разрешением имен и расположением компонентов.

Примечание

Для установки Active Directory необходима служба DDNS. Старые DNS-серверы работать с Active Directory не будут.

Правила именования

Первая роль связана с тем, что DNS привносит в Active Directory правила именования. К примеру, при разработке решения Active Directory корень домена можно было бы назвать **widgetech.com**. Но это не означает, что домен DNS будет идентичен домену Active Directory. Не забывайте, что Active Directory — это служба каталогов, установленная на контроллерах домена, в то время как DNS является средством разрешения IP-адресов. Локально ваш домен может называться **widgetech.com**, а в Интернете — **www.widgetechnic.com**. Active Directory содержит такие объекты, как принтеры, пользователи, серверы и т. д. Ваш DNS-домен сопровождается DNS-серверами, которые могут быть, а могут и не быть расположены на ваших контроллерах домена. На самом деле они даже могут быть не связаны с семейством Microsoft Windows.

DNS-серверы содержат базу данных (называемую *файлом зоны*), которая включает записи ресурсов, обеспечивающие соответствия между именами хостов и IP-адресами. К примеру, файл зоны может содержать запись, сообщающую нам о возможности связи с машиной domaincontroller5 по IP-адресу 192.168.1.100.

Разрешение имен

Далее, в средах Active Directory DNS предоставляет услуги по разрешению имен. Если одна машина в сети собирается связаться с другой, она отсылает на DNS-сервер DNS-запрос с целью определения IP-адреса второй машины. В Windows NT 4.0 и более ранних системах эта функция выполнялась WINS.

Расположение компонентов

Наконец, DNS помогает AD определять местоположение ее специальных компонентов. Например, если вы войдете в сеть и захотите найти определенный принтер, поскольку AD представляет собой базу данных, содержащую компоненты сети, будет

необходимо определить местонахождение сервера с Глобальным Каталогом. Для обработки запроса этого типа DNS-сервер пользуется ресурсом под названием *запись службы* (service record). Такие записи регистрируются службой NetLogon в контроллере домена во время его запуска.

NSLOOKUP

Для выявления неисправностей, связанных с DNS, можно воспользоваться утилитой nslookup. Это имя программы, которая позволяет администратору или пользователю интернет-сервера ввести имя хоста (например, **osborne.com** или **whitehouse.gov**) и узнать IP-адрес, связанный с этим доменным именем. Кроме того, эта утилита выполняет обратный поиск имени, т. е. выясняет имя хоста, соответствующее указанному IP-адресу.

Утилита nslookup отправляет пакет с запросом доменного имени на DNS-сервер. Выбор сервера зависит от используемой системы. В роли DNS-сервера по умолчанию может выступать сервер, установленный в вашей сети, у поставщика услуг, или в корневой серверной системе, обслуживающей всю иерархию доменных имен. Помимо прочего, с помощью nslookup можно переключиться на DNS-сервер другой организации.

Утилита nslookup поможет вам отследить и другую информацию, связанную с рассматриваемым IP-адресом, включая данные почтовых служб. Она входит как в состав Windows, так и в операционные системы на основе UNIX.

Кроме того, утилита nslookup умеет запрашивать серверы, на которых работают DNS-приложения наподобие BIND (Berkley Internet Name Domain — служба доменных имен в сети Интернет). Для составления DNS-запроса с помощью nslookup необходимы три элемента:

- имя или адрес DNS-сервера;
- запрашиваемый интернет-адрес;
- тип записи, для которой производится поиск.

Применение nslookup

В среде UNIX нужно лишь ввести `nslookup` в командной строке. Находясь в Windows, введите `nslookup.exe`. Любая из этих команд запускает утилиту nslookup.

Программа nslookup полезна в ситуациях, когда существует необходимость в сборе различных типов информации о хостах в сети. К примеру, можно получить данные о почтовых записях, IP-адресах, канонических именах и т. д.

Вызвав программу nslookup, вы увидите следующее приглашение:

```
>
```

После его появления можно ввести DNS-запрос. К примеру, при необходимости выяснить IP-адрес определенного сайта нужно задать его имя следующим образом:

```
>osborne.com
```

В результате будет возвращен IP-адрес:

```
198.45.24.162
```

Стоит ввести IP-адрес, и в ответ вы получите каноническое имя.

Примечание

Каноническим именем является имя хоста — к примеру, **osborne.com**.

Другой полезной характеристикой nslookup является способность получать листинг хостов, которые выполняют почтовые (Mail Exchange, MX) функции в данном домене.

Примечание

Ввод символа ? после приглашения > приведет к появлению списка функций, выполняемых nslookup.

Если вы ищете определенный тип записи (к примеру, почтовую запись), сообщить об этом nslookup можно с помощью команды `set type`.

Примечание

В средах Windows команду `set type` можно заменить `set q`. В данном случае под "q" подразумевается запрос (query). Термины "type" и "q" взаимозаменяемы.

К примеру, чтобы произвести поиск почтовой информации, введите следующую команду:

```
>set type=mx
```

Определив тип искомой записи, введите нужный интернет-адрес. К примеру, если ввести:

```
>osborne.com
```

результаты будут таковы:

```
Server:  ra.visi.com
Address:  209.98.98.98
osborne.com      MX preference = 0, mail exchanger = mail.eppg.com
osborne.com      nameserver = NS1.MHEDU.com
osborne.com      nameserver = NS2.MHEDU.com
NS1.MHEDU.com    internet address = 198.45.24.13
NS2.MHEDU.com    internet address = 198.45.24.14
```

Отсюда видно, что **mail.eppg.com** является зарегистрированным почтовым адресом для всей входящей почты на **osborne.com**. Сбор результатов был проведен посредством DNS-сервера **ra.visi.com**.

Если вы хотите выполнить проверку посредством DNS-сервера, являющегося авторитетным источником для другого домена, с помощью команды `server` его можно определить в качестве первичного DNS-сервера.

```
> server ns1.mhedu.com
Default Server: ns1.mhedu.com
Address:  198.45.24.13
```

Более подробную информацию о почтовой записи можно получить, выполнив поиск записи другого типа. В данном случае мы вновь воспользуемся командой `set type` — в этот раз для поиска записи хостовой информации (HINFO):

```
> set type=hinfo
```

Теперь, стоит нам ввести имя **osborne.com**, мы получим приведенные ниже подробные данные о хосте:

```
Server: ns1.mhedu.com
Address:  198.45.24.13

osborne.com
        primary name server = osborne.com
        responsible mail addr = hostmaster.eppg.com
        serial  = 200204152
        refresh = 3600 (1 hour)
        retry   = 900 (15 mins)
        expire  = 604800 (7 days)
        default TTL = 1800 (30 mins)
```

Если желаете просмотреть все подробности, касающиеся данного домена, установите тип `all`. В результате, как показано в следующем примере, будут возвращены все данные об указанном домене:

```
>set type=all
>osborne.com
Server:  ns1.mhedu.com
Address:  198.45.24.13

Non-authoritative answer:
osborne.com     nameserver = NS1.MHEDU.com
osborne.com     nameserver = NS2.MHEDU.com
osborne.com     MX preference = 0, mail exchanger = mail.eppg.com

osborne.com     nameserver = NS1.MHEDU.com
osborne.com     nameserver = NS2.MHEDU.com
NS1.MHEDU.com   internet address = 198.45.24.13
NS2.MHEDU.com   internet address = 198.45.24.14
mail.eppg.com   internet address = 198.45.24.13
```

Что может привлечь ваше внимание во время просмотра информации nslookup, так это запись "non-authoritative answer" (неответственный отклик). Для примера рассмотрим следующие листинги:

```
> whitehouse.gov
Server:  ns1.mhedu.com
Address:  198.45.24.13

Name:    whitehouse.gov
Address:  198.137.240.92
```

```
> whitehouse.gov
Server:  ns1.mhedu.com
Address:  198.45.24.13

Non-authoritative answer:
Name:    whitehouse.gov
Address:  198.137.240.92
```

В каждом случае мы произвели простой поиск nslookup на предмет Web-сайта Белого дома. В первый раз мы получили совершенно неинтересный ответ в форме IP-адреса Белого дома. Впрочем, когда мы ввели команду второй раз, перед строкой с IP-адресом Белого дома был поставлен классификатор "non-authoritative answer" (неответственный отклик). Не волнуйтесь: это не значит, что мы получили фальшивые данные. В первый раз, когда мы запросили информацию nslookup, результаты запросов были возвращены программе непосредственно с DNS-сервера Белого дома и были кэшированы нашим DNS-сервером. При выполнении второго запроса nslookup результаты были извлечены из кэша. Чтобы обозначить кэш как источник наших результатов, nslookup и добавляет классификатор "non-authoritative answer" перед листингом.

Ошибки nslookup

Пользуясь nslookup, вы можете столкнуться с различными типами ошибок. Их перечень приведен ниже.

- Превышение лимита времени (Timed out). Сервер не ответил на запрос nslookup по прошествии определенного периода времени и после совершения некоторого количества повторных попыток. Этот период времени можно отрегулировать с помощью подкоманды `set timeout`. Количество повторных попыток регулируется посредством подкоманды `set retry`.
- Сервер не отвечает (No Response From Server). На серверной машине не задействован ни один DNS-домен.
- Записи отсутствуют (No Records). На сервере имен DNS нет записей ресурсов, соответствующих текущему типу запроса для данного компьютера, хотя имя действительно.
- Несуществующий домен (Nonexistent Domain). Компьютер или DNS-домен не существует.
- В соединении отказано (Connection Refused). Соединение с сервером имен DNS установить не удалось.
- Сеть недостижима (Network is Unreachable). Соединение с сервером имен DNS установить не удалось.
- Сбой сервера (Server Failure). Сервер имен DNS обнаружил в своей базе данных несовпадение, и не смог возвратить ответ.
- Отказано (Refused). Сервер имен DNS отказал в исполнении запроса nslookup.
- Ошибка формата (Format Error). Пакет запроса, отправленный на сервер имен DNS, находился в неправильном формате. Это согласуется с ошибкой в nslookup.

Протокол динамической конфигурации хоста (DHCP)

Протокол DHCP упрощает процедуры предоставления и управления подключениями компьютеров к сети TCP/IP. DHCP автоматически присваивает компьютерам и другим сетевым устройствам IP-адреса из пула доступных адресов.

Настроенный DHCP-сервер предоставляет базу данных доступных IP-адресов и может устанавливаться с учетом дополнительных настроек для клиентов, включая адреса DNS-серверов, шлюзов и другую информацию. Как правило, DHCP-серверы используются в крупных организациях и поставщиках услуг Интернета, т. к. они предусматривают свободное назначение и повторное применение IP-адресов.

При запуске DHCP-клиент запрашивает информацию у DHCP-сервера. Это позволяет автоматически распределять IP-адреса вместе с масками подсети и другими данными. IP-адрес присваивается каждому клиенту на ограниченный период времени. Это называется "арендой". Время от времени периоды аренды можно продлевать, в результате чего сеанс становится беспрерывным. Аренда продлевается примерно в середине первоначального срока ее действия. Если обновление прошло успешно, IP-адрес остается за клиентом. Если же попытка обновления была неудачной, IP-адрес возвращается в пул и становится доступен другим клиентам.

Симптомы неисправностей

Если на вашем DHCP-сервере появились проблемы, вот вам несколько сценариев, которые часто встречаются и легко исправляются.

Симптом 5.9. DHCP-сервер остановился

Если ваш DHCP-сервер остановился, для начала необходимо проверить, уполномочен ли он для работы в данной сети. Кроме того, совсем не сложно упустить из виду какую-нибудь деталь конфигурации, особенно если вы только что настроили или завершили администрирование DHCP-сервера. Проверяйте настройки дважды, чтобы ничего не упустить.

Проанализируйте журнал регистрации событий вашей системы и контрольные журналы DHCP-сервера. В случае если служба запускается и останавливается, объяснение обычно фиксируется в таком журнале.

Симптом 5.10. DHCP-сервер не может обслужить клиентов

Если ваш DHCP-сервер является многоместным (Multihomed) компьютером, и при этом не предоставляет службу DHCP по одному или нескольким сетевым соединениям, проверьте привязки протоколов сервера. Посмотрите, как они конфигурируют TCP/IP для каждого из установленных на сервере соединений: статически или динамически?

Примечание

"Многоместность" подразумевает установку на сервере более одной сетевой платы и его работу в нескольких подсетях.

Если области или суперобласти не были настроены или активизированы, обеспечьте их правильную конфигурацию, а также все специальные опции, которые необходи-

мы для вашей системы. Если область полностью занята, и выделение адресов запрашивающим клиентам невозможно, DHCP-сервер возвращает им сообщения с отрицательным подтверждением (Negative ACKnowledgement, DHCPNACK). В такой ситуации в целях расширения пула IP-адресов можно предпринять четыре действия:

- расширить диапазон IP-адресов, увеличив конечный IP-адрес текущей области;
- создать дополнительную область и суперобласть, а затем включить в эту суперобласть существующую и новую области;
- дезактивировать существующую область и создать новую;
- уменьшить продолжительность периодов аренды.

Примечание

Областью называется пул доступных IP-адресов.

Кроме того, может оказаться, что диапазон IP-адресов, предлагаемый одним из ваших DHCP-серверов, конфликтует с диапазоном другого DHCP-сервера в сети. Чтобы избавиться от этой проблемы, измените пределы адресных пулов на каждом сервере таким образом, чтобы они не перекрывали друг друга. Вы даже можете аннулировать аренды, предоставленные клиентам, и временно задействовать обнаружитель конфликтов на стороне сервера — это поможет уладить проблему.

Симптом 5.11. На DHCP-сервере произошла потеря или разрушение данных

Если DHCP-сервер сообщает об ошибке базы данных Jet, или вы подозреваете, что база данных повреждена, не забывайте, что средства восстановления данных DHCP-сервера существуют для восстановления базы данных и исправления любых ошибок, о которых поступают сообщения. Чтобы проверить и отрегулировать любые проблемы в базе данных, вы можете воспользоваться функцией **Reconcile** в консоли DHCP.

Проблемы DHCP-клиента

Если DHCP-сервер работает безошибочно, но проблемы продолжают появляться, логично будет проанализировать DHCP-клиента. Существует несколько общих клиентских проблем, которые следует рассмотреть.

Перезагрузка

Начать можно с простой перезагрузки клиента. Если настройки DHCP на клиентской машине выполнены правильно, то, быть может, перезагрузки будет достаточно для того, чтобы избавиться от всех трудностей. Программное обеспечение DHCP до сих пор сталкивается с проблемами надежности, которые лучше всего решатся путем простой перезагрузки.

Подсоединение к другой сети

Если вы подсоединяетесь к другой сети и не можете получить доступ к DHCP-серверу, опять же, выполнение перезагрузки может оказаться всем, что вам нужно.

Освобождение и обновление

Еще один действенный способ избавиться от проблем с DHCP состоит в применении команд `ipconfig/release`, а затем `ipconfig/renew` (в среде Windows NT/XP), или `winipcfg` (в среде Windows 9x).

Дефектные DHCP-серверы

Убедитесь в том, что клиенты подсоединяются к правильному DHCP-серверу. Если они пытаются подключиться к так называемому *дефектному* DHCP-серверу, он может выдавать ошибочную информацию.

Служба имен Интернета для Windows (WINS)

WINS — это служба разрешения имен, разработанная Microsoft, но в операционных системах, начиная с Windows 2000, она, в основном, не используется. Тем не менее в целях обеспечения обратной совместимости она до сих пор поставляется вместе с системами Windows. Более того, поскольку среда Windows NT достаточно распространена, WINS все еще применяется многими организациями. WINS обеспечивает совместимость со службами и приложениями, которые требуют разрешения адресов из NetBIOS в IP.

Примечание

NetBIOS расшифровывается как Network Basic Input/Output System (Сетевая базовая система ввода/вывода) и представляет собой программу, позволяющую приложениям на разных компьютерах обмениваться информацией в рамках локальной сети

Основы WINS

WINS содержит два компонента высокого уровня: это WINS-сервер и WINS-клиент. WINS-клиент выполняет две функции: впервые появляясь в сети, он регистрируется на WINS-сервере, и ему же он посылает запросы на разрешение имен из IP в NetBIOS. WINS-сервер принимает и обрабатывает регистрационные данные и запросы от WINS-клиентов, и передает эту информацию другим WINS-серверам путем совместного использования ее базы данных в процессе репликации.

Примечание

В сети Windows NT может содержаться несколько WINS-серверов. В случае, если первичный WINS-сервер недостижим, клиенты могут попытаться установить связь с вторичным сервером. WINS-серверы регулярно согласовывают свои базы данных имен; период времени между этими согласованиями называется интервалом репликации.

Регистрация, обновление и освобождение

Стек TCP/IP инициализируется при первой связи между WINS-клиентом и WINS-сервером. Клиент инициирует запрос, отсылая WINS-серверу *запрос на регистрацию имени* (Name Registration Request). После этого WINS-сервер просматривает свою базу данных, выясняя, не занято ли указанное имя. Если оно свободно, регистрация принимается и фиксируется в базе данных для будущих поисков. Оставаясь подключенным к сети, клиент периодически обращается к серверу с целью обновления аренды, т. е. он пытается гарантировать дальнейшее использование регистрации на WINS-сервере. При выключении клиент связывается с сервером для того, чтобы освободить занимаемое имя. В последующих разделах процесс регистрации, обновления и освобождения рассматривается более подробно.

Регистрация

Когда WINS-клиент отсылает запрос на WINS-сервер, последний считывает запрос и принимает решение о его принятии или отклонении. Отказ в исполнении запроса в значительной степени мотивируется тем, что указанное имя уже применяется другим сетевым клиентом. Если имя уже зарегистрировано, сервер проверяет IP-адрес инициатора запроса. Если имя зарегистрировано, находится в активном состоянии, а у инициатора другой адрес, WINS-сервер отправляет сообщение текущему обладателю IP-адреса. Этот процесс начинается с сообщения "ожидание подтверждения" (Wait for Acknowledgement, WACK), согласно которому клиент должен подождать, пока сервер закончит обработку его запроса имени. Если текущий обладатель адреса отвечает, WINS-сервер сообщает первому запрашивающему клиенту о том, что указанное имя уже зарегистрировано и используется. Сразу после того, как WINS-сервер определяет наличие или отсутствие другого клиента с этим именем, он отсылает запрашивающему клиенту либо положительный (Positive), либо отрицательный (Negative) ответ на запрос о регистрации имени (Name Registration Response).

Обновление

Чтобы база данных имен на сервере не засорялась неиспользуемыми именами, они присваиваются клиентам на ограниченный период времени. Таким образом, периодически имена нужно обновлять. В ходе процесса регистрации клиенту предоставляется интервал обновления. По прошествии половины этого интервала клиент должен выполнить повторную регистрацию на сервере. Если к концу интервала возобновления клиенту не удалось это сделать, сервер освобождает его имя.

Примечание

Клиенты Windows продлевают аренду по прошествии половины интервала. Другие клиенты могут выполнять действия по возобновлению в другое время.

Освобождение

Существует два пути освобождения имени клиента.

- *Явное освобождение.* Выполняется при нормальном отключении клиента. Отправляя запрос об освобождении имени (Name Release Request), клиент сообщает WINS-серверу о прекращении своей работы и о том, что имя ему больше не нужно.
- *Необъявленное освобождение.* Происходит при внезапном отключении клиента. В данном случае запрос об освобождении имени не отсылается, и по прошествии интервала возобновления имя освобождается.

Воздействие WINS

При внедрении WINS в сети имеет смысл придерживаться настроек, принимаемых по умолчанию; для того чтобы изменять их, нужна очень веская причина. В большинстве своем параметры WINS прекрасно работают сами по себе. Постарайтесь приравнять интервал репликации между WINS-серверами к 15 минутам в локальной сети, 60—90 минутам во внутригосударственном сетевом соединении, к 2—12 часам в международном сетевом соединении. В зависимости от динамических свойств ва-

шей сети, возможно, эти значения будет разумно подрегулировать в ту или иную сторону.

WINS в локальной сети

Размещая WINS-сервер в своей локальной сети, окажите себе услугу: найдите время и поработайте над организацией первичного и вторичного WINS-серверов. В этом случае, если первичный сервер выйдет из строя, вам не придется слышать хор из ворчащих пользователей, недовольных работой сети. Более того, неплохо бы расположить WINS-серверы в географически разнородных областях; это позволит физическими методами повысить надежность WINS-серверов.

Примечание

Географическая разнородность отнюдь не подразумевает размещения серверов в разных странах. Они могут находиться в разных зданиях кампуса или на разных этажах одного здания.

WINS в глобальной сети

При установке WINS в глобальной сети имеет смысл организовать несколько WINS-серверов. Для примера рассмотрим сеть, схематически изображенную на рис. 5.6.

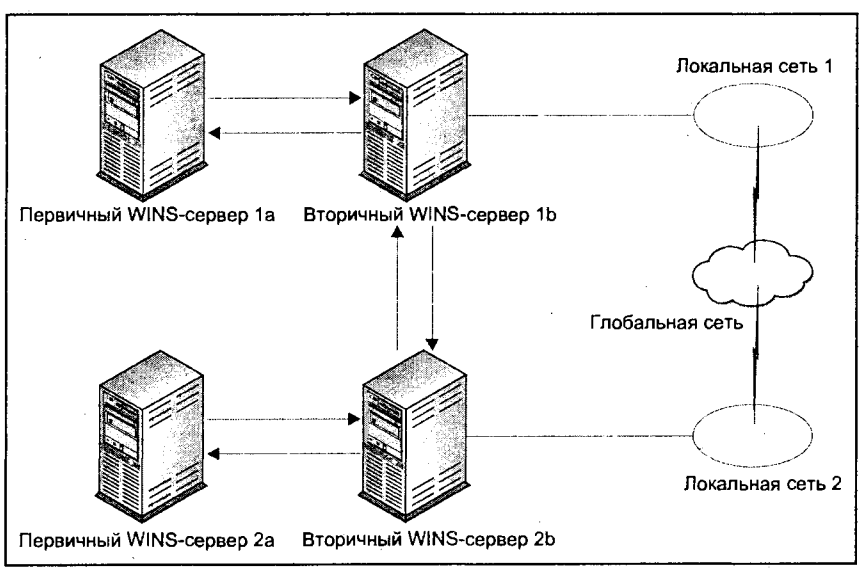


Рис. 5.6. Реализация WINS в глобальной сети

В данном случае первичный и вторичный WINS-серверы установлены с обоих краев глобальной сети. WINS-серверы 1a и 1b являются репликационными партнерами, так же как серверы 2a и 2b. В больших сетях может потребоваться отправить одну половину трафика локальной сети на первичный WINS-сервер 1a, а другую половину — на WINS-сервер 1b. Таким образом, нагрузка будет выровнена между ними. Аналогичная ситуация складывается на другой стороне глобальной сети, где поло-

вина трафика идет на 2a, а другая половина — на 2b. С каждой стороны глобальной сети серверы выполняют репликацию своих баз данных каждые 15 минут.

Впрочем, в этой ситуации интенсивность использования канала глобальной сети высока, и нам совершенно не нужно засорять его излишним трафиком. Так как пользователи по каждую сторону глобальной сети, в основном, обращаются к ресурсам своих собственных локальных сетей, мы можем быть достаточно уверенными в том, что данные WINS на обеих сторонах объединятся менее чем за час. Чтобы вычислить максимально допустимый период репликации между 1a и 2a, мы сложим периоды репликации каждой пары WINS-серверов (в данном случае 15 + 15 = 30). Эту сумму мы вычтем из максимально допустимого периода объединения, который равен 60 минутам (наша цель); в результате получим максимальный период репликации. В данном случае мы вычитаем 30 минут из 60, и получаем 30 минут — максимальный период времени, в течение которого запись передается с WINS-сервера 1a на WINS-сервер 2a.

Поиск и устранение неисправностей в WINS

Нижеследующие сценарии помогут справиться с поиском и устранением неисправностей WINS. Как отмечалось ранее, в системе WINS задействовано два компонента: клиенты и серверы.

В большинстве случаев, если сервер не справляется с задачей разрешения имен для своих клиентов, имеет смысл пересмотреть конфигурацию WINS и удостовериться в правильности всех установок. Большинство проблем WINS начинаются как неудачные клиентские запросы.

Проблемы с WINS-сервером

В случае возникновения неисправностей на WINS-сервере в первую очередь следует убедиться в том, что он работает. Откройте **Event Viewer** (Просмотр событий) или WINS-консоль, и посмотрите, запущена ли служба WINS. Для выполнения этой задачи, кроме прочего, можно воспользоваться пунктом **Services** (Службы) в Control Panel (Панель управления). Если WINS работает, выполните поиск ранее запрошенного имени, и убедитесь в том, что оно есть в базе данных.

Если имени в базе данных WINS нет, проверьте правильность настройки репликации между WINS-серверами. Кроме того, нужно узнать, не выдает ли сервер клиентам устаревшую информацию. Это может происходить из-за того, что статические сопоставления блокируют динамическую регистрацию правильных сопоставлений имя — адрес. Чтобы разрешить эту ситуацию, лучше всего отказаться от применения статических сопоставлений в отношении клиентов, которые для обновления данных об именах и адресах используют WINS динамическим способом. Если вы встретитесь с устаревшей информацией, проверьте, не была ли запись имени в базе данных WINS-сервера введена статически. Если это так, для обновления статически введенной записи выберите один из следующих методов:

- задействуйте миграцию в **Replication Partners Properties** (Свойства репликационных партнеров);
- в целях отражения измененной информации отредактируйте статическое соответствие;
- удалите статическую запись.

Если репликация между вашими WINS-серверами затруднена, проверьте репликационные партнерства. Если они однонаправленны (например, в них выполняется только проталкивание или только выталкивание), репликация базы данных может не распространяться на все серверы.

Если проблемы с разрешением имен на вашем WINS-сервере происходят не регулярно, то, вероятно, он регистрирует свои имена на других WINS-серверах. Такая ситуация складывается, когда настройки WINS-сервера, определенные в свойствах TCP/IP клиента, указывают на IP-адрес не локального, а удаленных WINS-серверов. В этом случае вам следует перенастроить свойства TCP/IP клиента таким образом, чтобы они указывали на локальные WINS-серверы.

Если WINS-серверу не удается выполнить репликацию проталкивания или выталкивания с другим WINS-сервером, воспользуйтесь утилитой Ping, чтобы убедиться, что оба этих сервера работают, и соединение с ними возможно. Кроме того, проверьте точность их настроек в качестве партнеров как проталкивания, так и выталкивания. Это можно сделать, просмотрев ключи `Push` и `Pull` системного реестра.

База данных WINS-сервера

Если вы выяснили, что служба WINS на WINS-сервере запущена, но, несмотря на это, вам не удается установить соединение с помощью WINS Manager (Диспетчер WINS), это значит, что база данных WINS либо недоступна, либо повреждена. В этой ситуации лучше всего восстановить базу данных с помощью ее резервной копии. Это можно сделать либо вручную, либо с помощью WINS Manager.

Чтобы восстановить базу данных WINS вручную, нужно в первую очередь создать резервную копию существующего файла базы. Даже если вы подозреваете, что она неисправна, резервирование не представит сложности, а впоследствии оно сможет избавить вас от головной боли, если выяснится, что на самом деле с базой данных все нормально.

Затем зайдите в папку \%Systemroot%\System32\Wins и удалите следующие файлы:

- J50.log;
- J50#####.log;
- Wins.tmp.

Скопируйте неповрежденную версию Wins.mdb в папку \%Systemroot%\System32 \Wins; после чего перезапустите WINS на вашем WINS-сервере. Перезагрузка WINS-сервера выполняется следующим образом.

1. Выключите сервер и подождите не меньше минуты.
2. Включите питание, перезагрузите Windows NT Server, и войдите в систему в качестве администратора.
3. Откройте командную строку, введите команду `NET START WINS` и нажмите клавишу <Enter>.

В случае если работоспособность вашего WINS-сервера нарушена из-за аппаратных сбоев, лучше всего полностью перенести WINS на другой физический сервер. Для этого потребуется выполнить перекомпоновку WINS-сервера. Этапы перекомпоновки приводятся ниже.

1. Если это возможно, перезапустите WINS-сервер и создайте резервные копии всех файлов в папке \%Systemroot%\System32\Wins. В случае необходимости вы можете воспользоваться либо графическим интерфейсом Windows, либо командной строкой MS-DOS. Если ни один из этих вариантов вам не подходит, придется воспользоваться резервной версией базы данных WINS.
2. Установите версию Windows, которая вам подходит, а затем стек TCP/IP (он инсталлируется вместе с Windows 2000 и Windows .NET). Создайте новый WINS-сервер, используя то же расположение жесткого диска и ту же папку \%Systemroot%, что присутствовали на вашем старом WINS-сервере.
3. Приостановите службу WINS на новом сервере, а затем с помощью Registry Editor (Редактор реестра) выполните восстановление ключей WINS из резервных копий.
4. Воспроизведите резервные копии в каталоге \%Systemroot%\System32\Wins.
5. Перезагрузите компьютер.

Если нужно переместить базу данных WINS с одного сервера на другой, сделайте следующее:

1. Остановите службу WINS.
2. Скопируйте файлы из папки \%Systemroot%\System32\Wins на новый компьютер. Лучше всего разместить их по тому же пути, что и на исходном компьютере; впрочем, если это не представляется возможным, скопируйте файл Wins.mdb, но не трогайте файлы с расширениями chk или log.
3. Запустите службу WINS на новом сервере.

Проблемы с WINS-клиентом

Если разрешения имен нарушено на клиентском компьютере, вероятно, применяется неверный тип разрешения. Вам следует проверить, какая служба разрешения имен используется в сети: WINS или DNS. Кроме того, установите, относится ли сбой к имени NetBIOS, или же к полностью определенному (полному) доменному имени (Fully Qualified Domain Name, FQDN).

Имена NetBIOS могут составлять до 15 символов в длину (к примеру, DAVESCOMPUTER), а применяются они в WINS. FQDN сильно напоминают интернет-адреса (например, **davescomputer.accounting.widgetech.com**) и применяются в DNS. Посмотрев на имя компьютера, можно сделать вывод о том, какой тип службы нужен в вашей сети.

Далее, ваш клиент может использовать приложение или версию Windows, в которой для разрешения имен необходимо применение WINS. К примеру, если разрешение имен закончилось неудачей при попытке найти Web-сайт в сети Интернет, вероятно, проблема относится к DNS, а не к WINS. Один из способов обойти это препятствие — воспользоваться DNS вместо WINS, но это возможно лишь в том случае, если вы находитесь в несмешанном окружении Windows 2000 или .NET (т. е. на всех клиентах и серверах установлены ОС Windows XP, 2000 или .NET). Если на каких-либо серверах применяются системы Windows NT или MS-DOS, это окружение, вероятнее всего, является смешанным.

Если вы находитесь в смешанном окружении, разрешение имен может окончиться неудачей в случае, когда клиенту нужен доступ к совместно используемому ресурсу,

который не был опубликован средствами Active Directory. Примером приложения, которому для разрешения имен необходима служба WINS, выступает **Map Network Drive** (Подключить сетевой диск) в составе Windows Explorer.

При появлении проблем с WINS важно рассмотреть конфигурацию клиента. Для начала нужно выяснить, настроен ли клиент на применение TCP/IP вместе с WINS. Эти настройки можно проверить вручную, просмотрев конфигурацию TCP/IP клиента, или динамически с помощью DHCP-сервера, который и обеспечивает клиента настройками TCP/IP. В операционных системах Windows до версии 2000 клиенты имеют возможность работать с WINS сразу после установки и конфигурации TCP/IP. В клиентских системах, начиная с версии Windows 2000, для каждого клиента можно блокировать NetBIOS через TCP/IP (NetBT). В случае отключения NetBT клиент не может пользоваться WINS.

Для проверки конфигурации IP клиента вам также следует воспользоваться командой `ipconfig/all`. При отображении настроек проверьте конфигурацию следующих параметров:

- IP-адрес;
- маска подсети;
- шлюз по умолчанию;
- первичный и вторичный WINS-серверы.

Если эти настройки недействительны, можно либо переустановить их вручную, либо с помощью команды `ipconfig/renew` запросить новые детали конфигурации с DHCP-сервера.

Клиент может испытывать затруднения из-за отсутствия возможности соединения с WINS-серверами. Первое, что нужно сделать в этой ситуации, — отправить на IP-адрес WINS-сервера ping-запрос. Если IP-адрес WINS-сервера вам неизвестен, команда `ipconfig/all` поможет его отыскать. Если WINS-сервер ответил на ping-запрос, необходимо применить команду `nbtstat -RR` в отношении как WINS-клиента, так и ресурсного сервера, к которому клиент пытается обратиться. Команда `nbtstat -RR` переустановит имена клиента и ресурсного сервера. В случае если WINS-сервер не отвечает на ping-запрос, можете смело делать вывод о наличии проблем со связью в сети, и на очереди у вас пересмотр настроек TCP/IP и процедуры выявления неисправностей.

Интернет-службы

В основном, пользователи представляют себе Интернет как один гигантский организм. Они думают, что электронная почта, Web-страницы и все остальное появляется лишь потому, что они обратились к Internet Explorer или Outlook. На самом деле, для всех функций, выполнение которых делает возможным сеть Интернет, необходимы разнообразные приложения, сервисные программы и протоколы.

В этом разделе рассматриваются различные компоненты, применяемые для передачи Web-страниц, электронной почты, передачи файлов, сетевого теледоступа и рассылки новостей.

Протокол передачи гипертекста (HTTP)

Протокол передачи гипертекста (Hypertext Transfer Protocol, HTTP) используется для передачи компонентов Web-сайта (текста, графики и других мультимедийных файлов) по сети Интернет. Являясь не только средством совместного использования информации во Всемирной паутине, HTTP обеспечивает страницам возможность содержать ссылки на другие страницы с данными. К примеру, когда вы идете на сайт **www.whitehouse.gov** и щелкаете мышью на фотографии президента, именно HTTP применяется для доставки другой страницы о президенте.

Любой компьютер, на котором размещается Web-сервер, называется HTTP-демоном. Это программа, которая ожидает поступления HTTP-запросов, а затем выполняет задачу поиска связанных страниц. Браузер, которым вы пользуетесь для поиска информации в Интернете, является HTTP-клиентом, который отправляет запросы на HTTP-сервер. Когда вы отсылаете запрос на сервер (либо вводя URL, либо переходя по ссылке), браузер формирует HTTP-запрос, который отсылается на IP-адрес, указанный в URL. HTTP-демон на Web-сайте назначения получает запрос и предоставляет запрошенный файл.

Протокол передачи файлов (FTP)

Протокол передачи файлов (File Transfer Protocol, FTP) — это интернет-протокол, который обеспечивает простой способ обмена файлами между компьютерами. FTP напоминает HTTP тем, что тоже осуществляет передачу Web-страниц и связанных с ними файлов; кроме того, он схож с протоколом SMTP (рассматривается далее в этом разделе), который отвечает за отправку электронной почты; впрочем, FTP для передачи файлов задействует стек протоколов TCP/IP. В основном, FTP-сервер используется для передачи файлов из пунктов их исходного местонахождения на компьютеры во всем мире.

Для пользователей FTP доступен либо через простой интерфейс командной строки (к примеру, в MS-DOS), либо через программу, которая предоставляет графический интерфейс пользователя и массу дополнительных возможностей, выходящих за рамки простой передачи файлов. Web-браузеры также имеют возможность делать FTP-запросы на файлы. С помощью FTP пользователь (располагающий соответствующими полномочиями) может удалять, переименовывать, перемещать и копировать файлы на сервере. Для доступа на FTP-сервер необходимы определенные полномочия, но в ситуациях, когда к серверу предполагается общий доступ, вход на него может быть анонимным.

Сетевой протокол передачи новостей (NNTP)

Сетевой протокол передачи новостей (Network News Transfer Protocol, NNTP) — это основной протокол, применяемый клиентами и серверами для управления публикацией объявлений в новостных группах Usenet. Серверы, применяющие NNTP, координируют всемирную сеть новостных групп Usenet. Для доступа к новостным группам, хранящимся на таких серверах, необходим NNTP-клиент. Они включены в большинство ведущих Web-браузеров, но могут выступать и в качестве отдельных продуктов с дополнительными функциями, наподобие Agent или Free Agent. Эти

автономные клиенты называются программами чтения новостей. По умолчанию NNTP действует через порт 119.

Telnet

Если вы располагаете всеми необходимыми полномочиями, то можете воспользоваться Telnet для доступа к другому компьютеру (который называется хостом). Если точнее, Telnet представляет собой пользовательскую команду, часть протокола TCP/IP для доступа к удаленным компьютерам. В сети Интернет применение HTTP и FTP позволяет отправлять и получать файлы с определенных удаленных компьютеров, но для этого вы должны быть зарегистрированы на них. С помощью Telnet вы получаете возможность зарегистрироваться на хосте как его пользователь. Входя в систему хоста посредством Telnet, вы делаете это, как обычный пользователь, располагая любыми правами доступа, которые вам предоставлены. К примеру, Telnet может быть полезен разработчикам программного обеспечения и любым другим людям, испытывающим необходимость в применении определенного приложения или данных, хранящихся на хосте.

Но протокол Telnet — это не только средство доступа к другим компьютерам, но и очень полезный инструмент выявления неисправностей. Telnet работает поверх TCP/IP, так что он с большей степенью надежности, чем команда `Ping`, указывает на доступность. Более того, Telnet способен тестировать высокоуровневые функции компьютера назначения. К примеру, если вы испытываете затруднения при обращении к многопользовательской машине, можете отправить ей ping-запрос, и, скорее всего, вы получите ответ. Тем не менее есть вероятность, что ping-ответ поступит, а машина все равно будет недоступна. Дело в том, что ответ на ping-запрос может прийти от ядра операционной системы. Ядро может принять и TCP-соединение, которым пользуется Telnet (им также оперирует ядро ОС), но другие проблемы, возможно, воспрепятствуют появлению приглашения на вход в систему.

Более того, Telnet-клиенты позволяют применять порты, отличные от того, который является портом Telnet по умолчанию. Например, можно установить порт 25, чтобы проверить работоспособность почтового сервера, или порт 80, чтобы проделать аналогичную операцию с Web-сервером.

Простой протокол электронной почты (SMTP)

Простой протокол электронной почты (Simple Mail Transfer Protocol, SMTP) — это протокол TCP/IP, предназначенный для отправки и получения электронных почтовых сообщений. Как правило, вследствие ограниченности возможностей SMTP по организации очереди из сообщений на принимающем конце, этот протокол применяется в сочетании с одним или двумя другими протоколами: POP3 (Post Office Protocol v3 — почтовый протокол версии 3) или IMAP (Internet Message Access Protocol — протокол доступа к сообщениям в Интернете). При использовании одного из этих двух последних протоколов пользователи получают возможность сохранять сообщения в почтовом ящике на сервере, а затем загружать их с него. На практике пользователи обычно применяют SMTP для отправки электронной почты, а POP3 или IMAP — для ее получения с почтового сервера.

Чтобы скомпоновать эти протоколы электронной почты, большинство почтовых программ позволяют определить как SMTP-сервер, так и POP-сервер. В основном

SMTP работает через порт 25 протокола TCP. В Европе существует альтернатива SMTP под названием X.400.

Симптомы неисправностей

При распространении Web-решений вы можете столкнуться с некоторыми трудностями, описанными ниже.

Симптом 5.12. Возникают ошибки паролей FTP

Так как для предоставления доступа по FTP применяются пароли, с ними могут возникать проблемы. В первую очередь необходимо проверить правильность ввода паролей (сделать это легче всего). Убедитесь в том, что режим <Caps Lock> отключен. Если сообщение об ошибке, тем не менее, появляется, убедитесь в том, что пароль не был изменен ни вами, ни администратором. Если ошибка появляется при попытке войти на сайт FTP с анонимным доступом, скорее всего, вы вводите неправильные данные, или же анонимный доступ на самом деле не разрешен. Чтобы разобраться в проблеме, свяжитесь с администратором сайта.

Примечание

Пароли Telnet и FTP отсылаются в виде открытого (читаемого) текста, поэтому их нужно тщательно подбирать.

Симптом 5.13. Возникают проблемы с полномочиями FTP

Полномочия FTP выходят за рамки парольной защиты сайта. Вы можете столкнуться со следующей ошибкой:

```
Server response:имя_файла:Permission denied
```

Даже если у вас есть пароль, необходимый для входа на сайт, вы можете не располагать полномочиями для доступа к конкретному файлу или папке. При попытке выполнить с файлом какую-либо операцию (например, переместить, удалить или переименовать его), на которую у вас нет разрешения, будет выведено сообщение об ошибке, схожее с предыдущим:

```
Server file error:имя_файла:Permission denied
```

На большинстве FTP-сайтов вы сможете копировать файлы, но по соображениям безопасности (и здравого смысла) лишь на немногих сайтах вы получите возможность переписывать или редактировать их. В любом из вышеупомянутых случаев, если возможность вашего доступа к данному файлу или папке подразумевается, следует связаться с администратором FTP-сайта — для того, чтобы он решил возникшую проблему с полномочиями.

Симптом 5.14. FTP-хост отсутствует

При попытке связаться с FTP-хостом вы можете получить сообщение с таким текстом:

```
Error Prompt: Could not find host entry
```

Это означает, что хоста, к которому вы пытаетесь подсоединиться, не существует. Проверьте правильность ввода имени хоста. Если в этом плане все нормально, воз-

можно, все объясняется тем, что сайт прекратил свое существование или был перемещен.

Симптом 5.15. FTP-соединение было прервано

После получения доступа к FTP-сайту может появиться сообщение об ошибке с уведомлением о разрыве соединения. Чаще всего это происходит потому, что FTP-клиент слишком долго бездействовал. Вам следует попытаться установить повторное соединение с этим FTP-сайтом. Кроме того, имеет смысл проверить настройки вашего FTP-клиента и изменить ту из них, которая относится к "разрыву соединения при простое" (или чему-нибудь в этом роде).

Продолжайте попытки подсоединения. Если единожды это удалось, велика вероятность того, что удастся и еще раз. Убедитесь в том, что настройки вашего компьютера не предписывают отключение по прошествии некоего периода бездеятельности, и пытайтесь дальше.

Симптом 5.16. Система доставки почты терпит неудачу

В случае, когда при доставке почты происходит сбой, sendmail — преобладающая реализация SMTP — помещает сообщение в очередь, чтобы через некоторое время попытаться доставить его еще раз. Впрочем, даже при использовании алгоритма отсрочки механизм опроса всех интернет-хостов на предмет почты отсутствует. В действительности, если хост расположен таким образом, что обращения к нему осуществляются по ненадежным соединениям (например, с помощью удаленного доступа через модем), SMTP не является оптимальным вариантом. Лучше настроить почтовые ящики POP и POP-сервер на хосте почтового обмена, а затем разрешить всем пользователям выступать в качестве почтовых клиентов с применением POP. Другое решение заключается в том, чтобы организовать периодическую передачу почты с помощью SMTP с хоста почтового обмена на другой, локальный хост почтового обмена SMTP, который ранее выстраивал очередь из исходящей почты.

Симптом 5.17. Существуют проблемы отправки и получения электронной почты

Если пользователь сообщает о проблемах с отправкой или получением электронной почты, нужно в первую очередь удостовериться в том, что серверы входящей и исходящей почты в его почтовой программе настроены надлежащим образом. К примеру, входящая почта обычно доставляется с POP3-, IMAP- или HTTP-сервера. SMTP-сервер, напротив, применяется для доставки исходящей почты.

Обычно в организациях почтовые серверы настраиваются с применением простой схемы именования, в которой неизменны только имена доменов. К примеру, в воображаемой компании Widgetech Inc. **pop.widgetech.com** был бы сервером входящих сообщений, а **smtp.widgetech.com** выступал бы в качестве сервера исходящих сообщений. Эту ошибку совершают довольно часто, но при этом ее легко исправить.

Симптом 5.18. Существуют проблемы с номерами портов

Все службы TCP/IP (включая HTTP, SMTP, Telnet, FTP и NNTP) обращаются к серверам с использованием определенных номеров портов. Номер порта применяется для того, чтобы дифференцировать одну службы TCP/IP от другой. Наиболее часто употребляемый номер порта для HTTP — 80; он по умолчанию используется

для доступа к данным из Web-браузера. Номером порта службы NNTP по умолчанию является 119. При возникновении проблем с номерами портов убедитесь в том, что номер порта вашей интернет-службы соответствует номеру порта этой службы на тех серверах, к которым вы пытаетесь подсоединиться.

Симптом 5.19. Система Telnet блокируется по времени

Если при работе с Telnet вы получаете сообщение о том, что "лимит времени соединения превышен", проверьте, действительно ли вы находитесь в сети и подсоединены к Интернету. Для соединения попытайтесь воспользоваться IP-адресом компьютера назначения.

Симптом 5.20. Не удается установить соединение Telnet

Если при попытке подсоединиться к другому компьютеру с помощью Telnet появляется сообщение об ошибке при установлении соединения, в первую очередь проверьте правильность ввода имени хоста. Если в этом плане все нормально, вероятнее всего, проблемы возникли именно на хосте. Попытайтесь подсоединиться позже.

Симптом 5.21. Я не могу подключиться к Web-сайту

Это очень обширная проблема, причины появления которой могут быть разными. Во-первых, проверьте соединение с Интернетом. Вполне возможно, что вы забыли войти в сеть, или после длительного простоя соединение было прервано. Если соединение активно, и вам известен IP-адрес сайта, попытайтесь ввести его. Если с помощью IP-адреса соединение пройдет успешно, вы будете знать, что проблема — в вашем DNS-сервере.

Дополнительные ресурсы

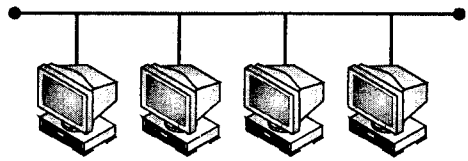
Active Directory:
http://www.microsoft.com/windows2000/technologies/directory/ad/default.asp.

Служба каталогов Novell eDirectory: **http://www.novell.com/products/edirectory/**.

DHCP: **http://www.dhcp.org**.

WINS: **http://www.microsoft.com/windows2000/techinfo/howitworks/communications/nameadrmgmt/wins.asp**.

DNS: **http://www.ludd.luth.se/~kavli/BIND-FAQ.html.**



ГЛАВА 6

Основы беспроводных технологий

В этой главе мы обратимся к теме организации сетей без проводов. Таким образом, сначала вы получите общее представление о характере функционирования разнообразных беспроводных приложений, а также о том, как они могут дополнить традиционные сети. Как только этот материал будет усвоен, мы перейдем к рассмотрению беспроводных локальных сетей, проведем обзор основных принципов их организации и познакомимся с семейством стандартов IEEE 802.11 (Institute of Electrical and Electronics Engineers, IEEE — Институт инженеров по электротехнике и электронике).

Введение в беспроводные технологии

Фактически под беспроводными сетями подразумевается ряд технологий передачи информации через воздушную среду, некоторые из которых восходят к началу телевещания, а другие основываются на последних достижениях в области проектирования кристаллов. Общим для всех беспроводных технологий является использование предопределенных частот, которые обеспечивают их функциональность. Таким образом, прежде чем переходить к рассмотрению различных беспроводных приложений, мы остановимся на трех взаимосвязанных понятиях: частоте, длине волны и полосе пропускания.

Частота

Термин "частота" применяется для обозначения количества периодических колебаний, или волн, в единицу времени. На рис. 6.1 изображены две синусоидальные волны, колеблющиеся на разных частотах. В верхней части рисунка приводится синусоидальная волна с частотой 1 цикл в секунду. Обратите внимание на то, что термин "цикл в секунду" в большинстве случаев заменяется синонимичным термином "герц", который, в свою очередь, сокращается до "Гц". В нижней части рис. 6.1 показана та же синусоидальная волна после удвоения частоты ее колебания до 2 Гц.

Время, необходимое для передачи сигнала на расстояние одной длины волны, обозначается как "период сигнала". Период, представляющий продолжительность цикла, также называется длиной волны, которая обозначается греческим символом

"лямбда" (λ). Период, или длину волны, можно выразить как функцию частоты. Таким образом, если λ обозначает период сигнала, а f — его частоту, то

$$\lambda = \frac{1}{f}$$

Кроме того, частоту можно выразить как период, или длину волны, сигнала. В результате получится

$$f = \frac{1}{\lambda}$$

Исходя из показанного выше, мы можем подсчитать, что синусоидальная волна, изображенная на рис. 6.1, с периодом сигнала 1 секунда, характеризуется частотой 1/1, или 1 Гц. Аналогичным образом вычисляем, что частота второй синусоидальной волны, чей период был сокращен наполовину, т. е. до 0,5 секунды, равен 1/0,5 или 2 Гц. Итак, мы видим, что между частотой и периодом, или длиной волны сигнала, существует обратная зависимость. Следовательно, когда период сигнала уменьшается, его частота увеличивается. Аналогично, когда длина волны сигнала возрастает, его частота убывает.

Длина волны

Как уже говорилось, период колебания сигнала также называется длиной волны (λ). Длину волны в метрах можно получить, разделив скорость света (приблизительно 3×10^8 м/с) на частоту сигнала в герцах. Таким образом,

$$\lambda(\text{м}) = \frac{3\times10^8}{f(\text{Гц})}.$$

Числитель и знаменатель предыдущего уравнения можно изменить и тем самым перевести частоту из герц в килогерцы, мегагерцы или гигагерцы, и уже в этих показателях вычислять длину волны:

$$\lambda(\text{м}) = \frac{3\times10^8}{f(\text{Гц})} = \frac{3\times10^5}{f(\text{кГц})} = \frac{300}{f(\text{МГц})} = \frac{0,3}{f(\text{ГГц})}.$$

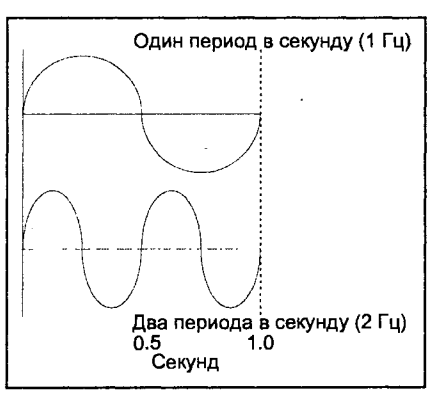


Рис. 6.1. Знакопеременные синусоидальные сигналы на разных частотах

Так как длину волны можно выразить как отношение скорости света к частоте, частота будет равняться скорости света, разделенной на длину волны:

$$f(\text{Гц}) = \frac{3 \times 10^8}{\lambda(\text{м})}.$$

Аналогично тому, как длина волны вычисляется через разные единицы измерения частоты, можно получить варианты вычисления частоты для длины волны в метрах:

$$f(\text{Гц}) = \frac{3 \times 10^8}{\lambda(\text{м})}, \quad f(\text{кГц}) = \frac{3 \times 10^5}{\lambda(\text{м})}.$$

$$f(\text{МГц}) = \frac{300}{\lambda(\text{м})}, \quad f(\text{ГГц}) = \frac{0,3}{\lambda(\text{м})}.$$

Для метрических вычислений можно аппроксимировать длину волны в сантиметрах следующим образом:

$$\lambda(\text{см}) = \frac{30}{f(\text{ГГц})}.$$

К примеру, предположим, что беспроводная система функционирует на частоте 5 ГГц. Тогда ее длина волны приблизительно равна 30/5, или 6 см. Работая с английской системой мер, можно вычислить длину волны в футах:

$$\lambda(\text{фут}) = \frac{1}{f(\text{ГГц})}.$$

Возвращаясь к нашему предыдущему примеру, где частота равнялась 5 ГГц, получим длину 1/5, или 0,2 фута. Длина волны сигнала сильно влияет на размер антенны, необходимой для работы данной беспроводной системы. Большинство антенн для беспроводной связи изготавливаются в четверть или половину длины волны, выраженной в единицах физической длины. Это объясняет, почему на погруженных подводных лодках, связь с которыми осуществляется на очень низких частотах, разматывают шлейф проводов: длина антенны может составлять тысячи футов. Для сравнения, сотовые телефоны и беспроводные локальные сети работают в мегагерцевых и гигагерцевых диапазонах и характеризуются сравнительно короткой длиной волны. Именно поэтому сотовые телефоны и платы сетевых адаптеров для беспроводных локальных сетей производятся с довольно небольшими антеннами.

Полоса пропускания

Полоса пропускания является мерой диапазона частот, но не самих частот. К примеру, если мы примем самую низкую частоту диапазона за f_1, а самую высокую — за f_2, доступная полоса пропускания будет равна $(f_2 - f_1)$. Хотя многие беспроводные системы функционируют на точно установленной частоте, она является центральной частотой, вокруг которой модулируется голос или данные, и может меняться в зависимости от конкретного беспроводного приложения. Например, при перемещении абонента от одной соты к другой частота работы сотового телефона может меняться автоматически и незаметно для владельца. Это объясняется тем, что системы сотовой связи в рамках каждой соты поддерживают некий диапазон частот, который

не может применяться в других сотах, и это позволяет избежать помех от сеансов связи в смежных сотах.

Теперь, когда вы имеете некоторое представление о частоте, длине волны и полосе пропускания, давайте кратко познакомимся с тем, какие позиции частотного спектра занимают беспроводные системы.

Беспроводные системы и частотный спектр

Любое исследование беспроводных систем требует хотя бы поверхностного обсуждения национальных и международных организаций, ответственных за регламентирование применения частотных спектров. Таким образом, в этом разделе мы вкратце ознакомимся с ролью двух американских федеральных правительственных организаций и одной международной.

Управляющие организации

В большинстве стран беспроводные средства связи регулируются правительственными организациями, ответственными за использование частотного диапазона. В Соединенных Штатах, в соответствии с Законом о системах связи (Communications Act) 1934 года и внесенными в него поправками, полномочия по координации применения радиочастотного спектра были разделены между Государственным управлением по телекоммуникациям и информации (National Telecommunications and Information Administration, NTIA) Министерства торговли США, с одной стороны, и Федеральной комиссией связи (Federal Communications Commission, FCC), с другой. NTIA осуществляет руководство частотным диапазоном, предназначенным для применения федеральными правительственными учреждениями. Для сравнения, FCC, являясь независимой регулирующей организацией, заведует частотным диапазоном, отведенным для использования нефедеральными правительственными структурами.

Для того чтобы самолеты, находясь в воздушном пространстве разных стран, могли связываться с наземными станциями, а спутники имели возможность передавать телевизионные сигналы, не испытывая воздействие и не создавая взаимные помехи, Международный союз телекоммуникаций (International Telecommunications Union, ITU) исполняет роль всемирного органа по контролю над использованием частотного диапазона. По условиям договоров ITU с большинством государств, подписывающие стороны обязуются соблюдать правила распределения радиочастотного диапазона, отведенного ITU для международного применения.

Теперь, когда вы понимаете, что частоты функционирования беспроводных систем подвержены регулированию, мы обратимся к рассмотрению некоторых простых систем и выделенных для них частот.

Беспроводные системы

В табл. 6.1 перечислены частотные диапазоны для 20 распространенных и развивающихся беспроводных систем. Применительно к этой главе особого внимания заслуживают сотовые системы, беспроводные локальные сети и фиксированные частотные диапазоны беспроводных технологий.

Таблица 6.1. *Распространенные и развивающиеся беспроводные приложения*

Приложение	Частота
AM-радио	535—1635 кГц
Аналоговый беспроводной телефон	44—49 МГц
Телевидение	54—88 МГц
FM-радио	88—108 МГц
Телевидение	174—216 МГц
Телевидение	470—806 МГц
RF-беспроводной модем	800 МГц
Сотовый телефон	806—890 МГц
Цифровой беспроводной телефон	900 МГц
ISM-диапазон	900—929 МГц
Общенациональная пейджинговая связь	929—932 МГц
Спутниковая телефонная связь (восходящая линия)	1610—1626,5 МГц
Сотовый телефон (PCS)	1850—1990 МГц
ISM-диапазон (802.11, 802.11b)	2,4—2,4835 ГГц
Спутниковая телефонная связь (нисходящая линия)	2,4835—2,5 ГГц
Многоканальная многоточечная система распространения	2,5—2,7 ГГц
Спутниковое телевидение (большая тарелка)	4—5 ГГц
UNII-диапазон (802.11a)	5,15—5,35; 5,725—5,825 ГГц
Спутниковое телевидение (малая тарелка)	11,7—12,7 ГГц
Беспроводное кабельное телевидение и LMDS	28—31 ГГц

Сотовые диапазоны

В Соединенных Штатах сотовая связь изначально заняла частотный диапазон 806—890 МГц, который до сих пор используется как исходными аналоговыми системами, так и основанными на множественном доступе с временным разделением (Time Division Multiple Access, TDMA). Более современные системы сотовой телефонии работают в частотном диапазоне 1850—1990 МГц, который называется диапазоном системы персональной связи (Personal Communications System, PCS). Заметим, что диапазон PCS размещен в области более высоких частот, чем исходный сотовый диапазон. Высокие частоты затухают намного быстрее, чем низкие. Вот почему двухрежимные сотовые телефоны, работающие в обоих частотных диапазонах, зачастую прибегают к аналоговым частотам. Поскольку в цифровой сотовой телефонии используются более высокие, чем в аналоговой, частоты, дальность передачи оказывается меньше. Таким образом, для обслуживания каждой отдельной геогра-

фической области при использовании частотного диапазона 1850—1990 МГц требуется больше сот, чем в случае аналогового диапазона 806—890 МГц. Хотя сотовые операторы обеспечивают довольно приличный цифровой охват вдоль межштатных автомагистралей, в крупных городах и многих пригородных областях, в сельской местности передача сотовых сигналов, как правило, осуществляется за счет старых аналоговых станций. Поскольку установка в сельских районах большого числа цифровых базовых станций взамен старых аналоговых слишком дорога, в обозримом будущем актуальность старых аналоговых технологий в двухрежимных сотовых телефонах сохранится.

ISM-диапазоны

Другой набор частотных диапазонов, который заслуживает упоминания, — это Промышленные, Научные и Медицинские (Industrial, Scientific and Medical, ISM) диапазоны 900—929 МГц и 2,4—2,4835 ГГц, а также диапазон Нелицензируемой национальной информационной инфраструктуры (Unlicensed National Information Infrastructure, UNII) на частотах 5,15—5,35 ГГц и 5,75—5,825 ГГц. Эти три диапазона представляют нелицензируемые частотные диапазоны в почти глобальном масштабе. В данном случае термин "нелицензируемый" обозначает, что для эксплуатации беспроводного оборудования в этих диапазонах от его пользователя не требуется лицензии. Тем не менее такое оборудование должно соответствовать разнообразным национальным спецификациям, которые варьируют в зависимости от конкретного государства. К примеру, в Соединенных Штатах FCC определяет максимальную мощность излучения устройства, а также регламентирует метод модуляции, применяемый оборудованием, работающим в нелицензируемом частотном диапазоне.

Первый ISM-диапазон, показанный в табл. 6.1 (900—929 МГц), применяется различными устройствами для присоединения множества беспроводных локальных сетей со специализированными методами передачи. Поскольку для использования доступны лишь 29 МГц полосы пропускания, специализированные беспроводные локальные сети, функционирующие в ISM-диапазоне 900—929, довольно медленны: скорость их работы обычно не превышает 1 Мбит/с.

Второй частотный диапазон ISM, показанный в табл. 6.1 (2,4—2,4835 ГГц), обеспечивает полосу пропускания 83,5 МГц. В этом диапазоне действуют микроволновые печи, беспроводные телефоны некоторых типов, а также (что представляет для читателей больший интерес) две версии беспроводных локальных сетей от IEEE, которые формально обозначаются как 802.11 и 802.11b. Стандарт IEEE 802.11 для беспроводных локальных сетей определяет, что метод управления доступом (MAC) может быть транспортирован одним из трех способов, каждый из которых работает со скоростью 1 или 2 Мбит/с. В числе поддерживаемых методов транспортировки — инфракрасное излучение, расширенный спектр со скачкообразной перестройкой частоты (Frequency Hopping Spread Spectrum, FHSS) и расширенный спектр с прямой последовательностью (Direct Sequence Spread Spectrum, DSSS).

Как FHSS, так и DSSS являются широкополосными методами передачи, изначально разработанными для военного применения в качестве механизмов преодоления радиопомех. В FHSS используется псевдослучайная последовательность частот, при которой передатчик перескакивает с одной частоты на другую по прошествии небольшого времени пребывания на частоте для передачи данных. В среде беспроводной локальной сети каждое устройство знает последовательность скачкообразной

перестройки, а применение относительно короткого интервала пребывания на частоте гарантирует, что взаимные пересечения, возникающие при работе нескольких передатчиков на одной или даже нескольких частотах, окажут минимальное влияние на итоговую передачу.

В DSSS к каждому информационному разряду применяется код расширения, так что каждый бит заменяется на несколько. К примеру, предположим, что код расширения — 10100. Он "усиливает" информационные разряды так, что для каждого из них будут переданы пять бит. Например, если информационный разряд представлял собой двоичную единицу, передаваться будет 01011. В приемнике тот же самый код расширения, который применялся отправителем, используется для "сужения", т. е. для восстановления исходного информационного разряда. Соответственно, если принята битовая последовательность 01011 и код расширения 10100, в результате их сложения получится последовательность 11111. Она будет означать, что расширенным информационным разрядом была двоичная единица. В случае возникновения ошибки приемник проверит набор из этих пяти бит, и с помощью стандартного мажоритарного правила (по большинству) восстановит переданный бит. Так, при использовании 5-разрядного кода расширения повторение одного и того же значения 3 или более раз в "суженном" коде будет представлять желаемое значение. Поскольку DSSS передает энергию, или мощность, сигнала в большой полосе пропускания, он также является механизмом минимизации помех, среди которых может быть и глушение. В случае инфракрасного излучения передача информации происходит в приближенном к видимой области спектре. Так как при этом не задействуется радиосигнал, нет таких организаций, которые регулировали бы применение инфракрасного излучения. Впрочем, из-за ограниченной протяженности передачи инфракрасного излучения эта технология, определенная стандартом IEEE 802.11, нуждается в дальнейшей разработке производителями, которые должны превратить ее в жизнеспособные продукты.

Возвращаясь к нашему обсуждению стандартов беспроводных локальных сетей, отметим, что расширение стандарта IEEE 802.11b специфицировало применение DSSS на физическом уровне для поддержки скоростей передачи данных в 1, 2, 5,5 и 11 Мбит/с. Третий ISM-диапазон относится к частотному диапазону Нелицензируемой национальной информационной инфраструктуры (UNII). В настоящее время в этом диапазоне работает оборудование стандарта IEEE 802.11a, в соответствии с которым для получения скоростей передачи данных до 54 Мбит/с нужно применить ортогональное частотное уплотнение (Orthogonal Frequency Division Multiplexing, OFDM). Из нашего экскурса в физику вспомним, что высокие частоты затухают намного быстрее, чем низкие, и получим, что дальность передачи 802.11a-совместимого оборудования намного ниже, чем у продуктов стандарта 802.11b. Это значит, что для организации, монтирующей в своем здании беспроводную локальную сеть на основе стандарта 802.11a, может потребоваться значительно больше точек доступа, чем для поддержки беспроводной сети, действующей в более низком частотном диапазоне 2,4—2,4835 ГГц.

Фиксированная радиосвязь

В рамках нашего обзора беспроводных систем уместно отметить еще два частотных диапазона: 2,5—2,7 ГГц, используемый задачами многоканальной многоадресной распределительной системы (Multichannel Multipoint Distribution System, MMDS), и 28—31 ГГц для задач местной многоадресной распределительной системы (Local

Multipoint Distribution System, LMDS). Как MMDS, так и LMDS являются представителями фиксированной беспроводной технологии, разработанной с целью обеспечения высокоскоростной широкополосной передачи данных. MMDS — это фиксированная беспроводная технология, чей частотный спектр 2,5—2,7 ГГц позволяет гарантировать скорость передачи данных до 10 Мбит/с. Для сравнения, LMDS представляет собой работающую в пределах прямой видимости технологию беспроводного широкополосного доступа. В Соединенных Штатах полоса пропускания, выделяемая LMDS, составляет 150 либо 1150 МГц, что гораздо больше, чем у всех прочих методов беспроводной передачи.

При использовании LMDS сота теоретически может обеспечивать скорость передачи данных до 3,5 Гбайт/с. В конце 1990-х годов осуществлялись значительные инвестиции в технологии MMDS и LMDS, когда несколько ведущих коммуникационных компаний скупали лицензии на работу с абонентским телевидением у колледжей и университетов, чтобы получить достаточную полосу пропускания и проектировать системы. К сожалению, как технические проблемы (включая отражения от зданий, создающие многолучевые помехи), так и имевшие место финансовые проблемы в телекоммуникационном секторе задержали потенциальный рост этой технологии. Теперь, когда вы имеете представление о фиксированных широкополосных беспроводных технологиях, в оставшейся части этой главы мы сосредоточим внимание на беспроводных локальных сетях, а начнем с анализа ряда стандартов IEEE, регламентирующих применение таких сетей.

Стандарты беспроводных локальных сетей

В дополнение к базовому стандарту IEEE 802.11 было разработано несколько расширений, два из которых (802.11b и 802.11a) мы вкратце упомянули. В табл. 6.2 приведены существующие на сегодняшний день стандарты IEEE.

Таблица 6.2. *Стандарты IEEE 802.11*

Стандарт	Описание
802.11	Исходный стандарт для беспроводных локальных сетей; 1/2 Мбит/с
802.11b	Расширение DSSS с поддержкой 1, 2, 5,5 и 11 Мбит/с
802.11a	Функционирует в 5-гигагерцевом диапазоне со скоростью 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с
802.11c	Операции по организации мостов
802.11d	Спецификация для распорядительных областей
802.11e	Качество обслуживания (в мае 2001 года перемещено в 802.11i)
802.11f	Возможность взаимодействия точек доступа
802.11g	Операции в 2,4/5-гигагерцевом диапазоне
802.11h	Помехи
802.11i	Функции обеспечения безопасности

Базовый стандарт 802.11

Как указывалось выше, IEEE 802.11 — это первоначальный стандарт беспроводных локальных сетей, пропагандируемый Институтом инженеров по электротехнике и электронике (IEEE). В соответствии с этим стандартом, операции инфракрасного излучения, FHSS и DSSS, на физическом уровне должны проходить со скоростью 1 или 2 Мбит/с. В качестве его компонента в исходном стандарте IEEE 802.11 присутствовал механизм обеспечения безопасности — эквивалентная проводной конфиденциальность (Wired Equivalent Privacy, WEP). WEP задумывался как способ предоставления пользователям беспроводных локальных сетей уровня конфиденциальности, эквивалентного уровню, получаемому при передаче незашифрованных данных по проводной локальной сети.

WEP

У WEP есть несколько недостатков, которые были унаследованы расширениями IEEE 802.11b и 802.11a от базового стандарта 802.11. Так как для большинства организаций безопасность крайне важна, сначала мы сосредоточимся на обсуждении механизма WEP и его слабых мест, а потом уже перейдем к другим стандартам 802.11.

Эквивалентная проводной конфиденциальность (WEP) представляет собой метод шифрования, применяемый на покадровой основе. В методе WEP вектор инициализации (Initialization Vector, IV), состоящий из 24 разрядов, применяется в сочетании с секретным ключом, который используется на каждой беспроводной станции в качестве начального числа при генерации псевдослучайной числовой последовательности. Эта последовательность объединяется по схеме XOR (исключающее ИЛИ) с открытым текстом для формирования зашифрованных данных. Вектор IV обеспечивает для каждого кадра данных возможность шифрования независимо от предшествующего и последующего кадров. Чтобы получатель смог должным образом расшифровать данные, IV, как показано на рис. 6.2, передается в незашифрованном виде. Поскольку каждая станция, применяющая WEP, сконфигурирована с одним и тем же секретным ключом, принимающая станция связывает полученный вектор IV со своим секретным ключом, в результате чего получает начальное число для генерации псевдослучайной последовательности чисел, которая по схеме "исключающее ИЛИ" объединяется с зашифрованными данными с целью воссоздания открытого текста. Величина контрольной суммы (Integrity Check Value, ICV) представляет собой результат выполнения проверки при помощи 32-разрядного циклического избыточного кода (CRC) и позволяет приемнику определить наличие ошибок в одном или нескольких разрядах принятого кадра.

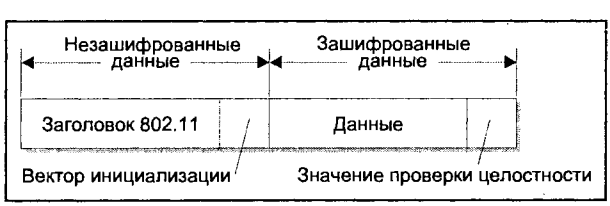


Рис. 6.2. WEP-шифрование

Слабые места

Псевдослучайным генератором, применяемым в WEP, является алгоритм RC4; он используется во многих продуктах, от браузеров до баз данных. Хотя в других продуктах RC4 является средством базовой безопасности, он генерирует некоторые слабые ключи, которые в сочетании с обоснованными предположениями относительно первого байта зашифрованных данных могут позволить математически восстановить секретный ключ. Среди других проблем, связанных с WEP, присутствует тот факт, что по умолчанию он отключен, длина вектора IV составляет лишь 24 разряда (а это значит, что он довольно часто повторяется), а процесс создания ICV носит линейный характер. Каждый из этих недостатков был описан в течение нескольких последних лет в различных публикациях, которые обращали внимание на небезопасность WEP. Из-за крайней важности обеспечения безопасности мы обсудим ненадежность WEP, а также текущие и планируемые меры по повышению степени его защищенности.

Настройка по умолчанию

В большинстве продуктов производителей метод WEP отключен. Пример этой настройки по умолчанию показан на рис. 6.3, на котором изображена вкладка **Encryption** диалогового окна конфигурации беспроводной локальной сети Orinoco (компания Agere System) для профиля по умолчанию. Обратите внимание, что флажок, находящийся слева от метки **Enable Data Security** (Разрешить защиту данных), не установлен. Чтобы задействовать WEP, пользователь должен сначала пометить его, а затем ввести либо буквенно-цифровые, либо шестнадцатеричные символы одного секретного ключа шифрования. Диалоговое окно конфигурации Agere Orinoco аналогично соответствующим настройкам других продуктов в том отношении, что оно позволяет задавать до четырех ключей шифрования; впрочем, единовременно может использоваться лишь один из них.

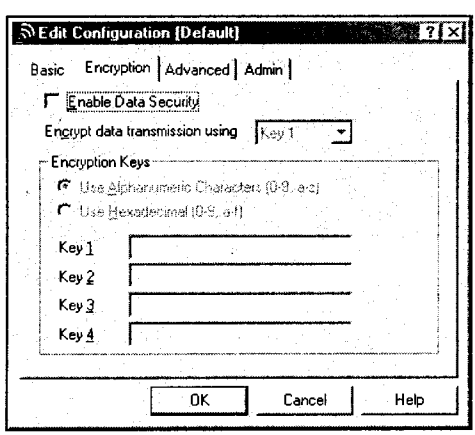


Рис. 6.3. WEP-шифрование в большинстве продуктов для беспроводных локальных сетей по умолчанию отключено

Именно тот факт, что в большинстве продуктов для беспроводных локальных сетей WEP-шифрование по умолчанию отключено, объясняет появление в 2001 году со-

общений в New York Times, Wall Street Journal и других изданиях о проникновениях, совершенных двумя господами в фургоне. Этим двоим удалось, переезжая от парковки к парковке в Кремниевой долине в 2001 году, перехватить сетевые передачи и разобраться в них. Они воспользовались тем, что, в соответствии с настройками по умолчанию, метод WEP находится в отключенном состоянии. С помошью портативного компьютера и направленной антенны они смогли перехватить трафик локальной сети более чем из половины зданий, фасадами обращенных к тем парковкам, на которых они побывали.

Другие пассивные атаки

Из-за того что большую часть трафика локальной сети составляют IP-пакеты, довольно просто угадать первые несколько байт, передаваемых в каждом кадре беспроводной локальной сети. Имеется в виду, что после начала заголовка кадра в нем размещаются определенные поля, которые обозначают тип передаваемого кадра. К примеру, IP передается в кадре протокола доступа к подсети (Sub Network Access Protocol, SNAP), который идентифицируется шестнадцатеричными символами AA. Благодаря взаимосвязи между слабыми ключами, генерируемыми алгоритмом RC4 и применяемыми WEP, с одной стороны, и первым байтом зашифрованных данных, с другой, нескольким исследователям удалось установить методы восстановления секретного ключа посредством пассивного мониторинга и сбора от 4 до 5 миллионов кадров зашифрованных данных. Другие исследователи заявляли о том, что могут восстановить секретный ключ, выполнив мониторинг 1—2 миллионов кадров, и их достижениями воспользовались другие люди, опубликовавшие в сети Интернет две популярные программы. Обе эти программы, называющиеся AirSmart и WEPCrack, позволяют третьему лицу проводить пассивный мониторинг беспроводной локальной сети и восстанавливать применяемый в ней секретный ключ. Как только ключ выявлен, становится довольно просто воспользоваться одной из нескольких программ декодирования локальных сетей, которые предоставляют пользователю возможность ввести секретный ключ, и, следовательно, расшифровать данные, передаваемые в каждом захваченном кадре.

В дополнение к публикациям и программам, обеспечивающим возможность восстановления секретного ключа, было написано несколько статей на тему слабых мест WEP, связанных с применением 24-разрядного вектора IV. Использование относительно короткого IV приводит к тому, что довольно регулярно он повторяется. Эта ситуация называется "конфликтом векторов инициализации", и, когда она происходит, захват нескольких одинаковых IV позволяет провести статистический анализ зашифрованных данных и, в конечном итоге, восстановить открытый текст.

Третье слабое место WEP имеет отношение к линейной природе контрольной суммы (ICV). Такая линейная зависимость делает возможной атаку типа "человек посередине" (man-in-the-middle), в ходе которой неуполномоченная третья сторона может перехватить кадр, отобразить зеркально разряды зашифрованных данных и полей ICV, а затем переадресовать пакет в место его назначения. В результате получатель расшифрует пакет и после повторного вычисления ICV обнаружит, что это значение действительно соответствует ICV в полученном поле. Таким образом, третья сторона способна изменить данные так, что это не будет замечено получателем.

Усиление WEP

В связи с наличием в WEP слабых мест при институте IEEE была создана рабочая группа "Task Group i", вошедшая в подчинение Рабочей группы 802.11, которая должна была разработать стандарт, повышавший уровень безопасности в беспроводных локальных сетях. Этот стандарт известен как 802.11i. Впоследствии в IEEE был также разработан стандарт 802.1x для идентификации на основе портов; оба они будут рассмотрены далее в этом разделе.

Не ожидая появления новых стандартов, которые должны были заделать существующие дыры в системе безопасности WEP, несколько производителей представили на суд публики свои собственные решения проблемы слабых мест WEP. Большинство из этих решений базируются на динамическом изменении секретного ключа WEP. Некоторые производители дают пользователю возможность определять частоту изменения ключа WEP, а другие — нет. Впрочем, поскольку периодичность изменения ключей WEP не превышает миллиона кадров, этого должно быть вполне достаточно, чтобы предотвратить восстановление секретного ключа. Теперь, когда мы ознакомились со степенью уязвимости WEP, следует вновь обратить внимание на другие расширения стандарта IEEE 802.11.

802.11B

Расширение 802.11b стандарта 802.11 ограничено использованием DSSS на физическом уровне. Тем не менее рабочая скорость оборудования была увеличена с 1 и 2 Мбит/с до 5,5 и 11 Мбит/с. Как исходный стандарт 802.11, так и расширение 802.11b функционируют в частотном диапазоне 2,4 ГГц.

802.11A

Расширение 802.11a стандарта 802.11 можно считать представляющим высокоскоростные беспроводные локальные сети. В этом расширении были внедрены скорости передачи данных в 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с; впрочем, обязательной является только поддержка скоростей в 6, 12 и 24 Мбит/с. В отличие от расширения 802.11b, оборудование, которое поддерживает 802.11a, функционирует в частотном диапазоне 5 ГГц. Как указывалось ранее в этой главе, из-за того, что высокие частоты затухают быстрее низких, радиус действия 802.11a-совместимого оборудования меньше, чем дальность продуктов беспроводных локальных сетей, действующих в 2,4-гигагерцевом частотном диапазоне.

802.11C

Расширение 802.11c стандарта 802.11 разграничивает операции по организации мостов. Так как точка доступа исполняет роль моста между беспроводной и проводной сетевыми инфраструктурами, это расширение определяет методы, благодаря которым точка доступа узнает адреса в каждой из них.

802.11D

Расширение 802.11d стандарта 802.11 представляет собой дополнение к уровню управления доступом к среде (MAC-уровню), создающее благоприятные условия для

применения беспроводных локальных сетей 802.11 по всему миру. Цель этой работы заключается в том, чтобы обеспечить для точек доступа возможность функционирования на допустимых радиоканалах; эта задача реализуется посредством внедрения функций, дополняющих стандарт, в результате чего оборудование получает возможность законно функционировать в определенных странах.

802.11E

Расширение 802.11e уровня управления доступом к среде представляет собой развивающийся стандарт, назначение которого заключается в обеспечении беспроводных локальных сетей функцией качества обслуживания (Quality of Service, QoS). Она позволяет задавать приоритеты при передаче голосового, информационного и видеотрафика по беспроводным локальным сетям. В мае 2001 года эти работы были переведены в область 802.11i.

802.11F

Расширение 802.11f стандарта 802.11 формулирует "рекомендованную практику" и разрабатывается с целью обеспечения межоперабельности точек доступа от различных поставщиков. Этот стандарт будет определять порядок взаимодействия точек доступа разных производителей в рамках мобильной среды, и к моменту вашего, уважаемый читатель, ознакомления с этим текстом будет доступен в качестве группового обновления для существующего оборудования.

802.11G

Так как подавляющее большинство продуктов для беспроводных локальных сетей функционируют в 2,4-гигагерцевом частотном диапазоне, организация, обновляясь до высокоскоростной беспроводной локальной сети с 5-гигагерцевым частотным диапазоном, рискует не извлечь пользы из инвестиций в точки доступа. Стандарт 802.11g разрабатывался как раз с той целью, чтобы обеспечить организациям варианты перехода и совместимость со старым оборудованием. Оборудование, поддерживающее стандарт 802.11g, может работать в 2,4-гигагерцевом диапазоне со скоростью 11 Мбит/с или в 5-гигагерцевом диапазоне со скоростью до 54 Мбит/с.

802.11H

В Европе стандарт 802.11a может провоцировать появление помех, т. к. он делит 5-гигагерцевый диапазон с некоторыми видами радиолокационных и спутниковых средств связи. Спецификация 802.11h объединяет функции регулирования мощности передачи (Transmission Power Control, TPC) и динамического подбора частоты (Dynamic Frequency Selection, DFS). TPC позволяет пользователям, находящимся неподалеку от точки доступа, снижать мощность, а DFS дает возможность устройствам, выявляющим другие сигналы, переключаться на альтернативный канал передачи.

802.11I

Как указывалось выше, WEP олицетворяет основной недостаток системы безопасности беспроводных локальных сетей IEEE. Расширение IEEE 802.11i является на-

бором функций безопасности, среди которых фигурируют протокол целостности временного ключа (Temporal Key Integrity Protocol, TKIP) и расширенный стандарт шифрования (Advanced Encryption Standard, AES). TKIP представляет собой предварительную замену WEP, в которой посредством обновлений программного обеспечения поддерживаются традиционные клиентские станции и точки доступа. Для сравнения, AES обеспечивает более высокий уровень безопасности, но скорее всего его применение будет возможно лишь на новой аппаратуре. В качестве дополнительного компонента к расширению 802.11i стандарта 802.11, о котором следует упомянуть, выступает стандарт 802.1x. Он определяет аутентификацию на основе портов и предусматривает метод проверки регистрационных данных пользователя в точках доступа.

Теперь, когда мы рассмотрели семейство беспроводных стандартов IEEE 802.11, самое время сосредоточиться на структуре и функционировании беспроводных сетей 802.11.

Работа беспроводных локальных сетей

Существует два основных типа устройств для беспроводных локальных сетей; они называются *клиентскими станциями* (client station) и *точками доступа* (Access Point, AP). Помимо того, что точка доступа выполняет мостовую функцию, позволяя кадрам перетекать между проводной и беспроводной инфраструктурами, считается, что благодаря поддержке радиочастотной передачи данных она представляет беспроводную станцию.

Режимы работы

Беспроводные локальные сети IEEE 802.11 функционируют в одном из двух режимов: специальном ("ad hoc") или инфраструктурном. Специальная сеть содержит две или более клиентских станций, которые напрямую взаимодействуют друг с другом. Для сравнения, инфраструктурный режим работы предусматривает связь всех клиентов с точкой доступа, не зависимо от направления кадров. Таким образом, находясь в инфраструктурном режиме, два клиента могут обмениваться информацией исключительно через точку доступа.

Клиент беспроводной локальной сети

На рис. 6.4 приведен пример платы адаптера для беспроводной локальной сети, которая в сочетании с соответствующим программным обеспечением превращает

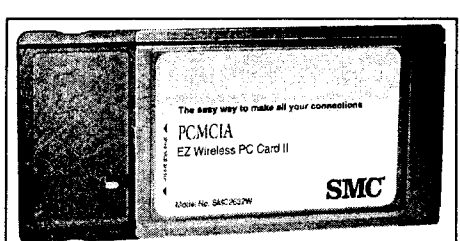


Рис. 6.4. Плата адаптера беспроводной сети SMC PC Card (фотография предоставлена SMC Networks)

ноутбук любого класса в клиента беспроводной локальной сети IEEE 802.11. Плата PC Card, изображенная на рис. 6.4, произведена компанией SMC Networks; в ее состав входит встроенная антенна, размещенная в левой части платы и заключенная в пластик. Именно левая часть платы PC Card, когда она вставлена в ноутбук, выступает из слота.

Комбинированный маршрутизатор/точка доступа

Многие производители изготавливают автономные точки доступа, но некоторые компании реализовали в точке доступа сочетание функциональности моста с базовыми функциями маршрутизатора и коммутатора локальной сети. Одним из таких продуктов является широкополосный маршрутизатор SMC Networks Barricade, изображенный на рис. 6.5. В состав этой беспроводной точки доступа/маршрутизатора входят три порта для коммутатора локальной сети Ethernet 10/100 Мбит/с, а также Ethernet-порт для соединения с кабельным или DSL-модемом. Обратите внимание на две антенны, установленные на этом широкополосном маршрутизаторе/точке доступа, показанном на рис. 6.5. Благодаря применению двух антенн, расстояние между которыми примерно равно длине волны, устройство имеет возможность выбора наилучшего сигнала. Использование сдвоенных антенн называется пространственным разнесением; благодаря этой технике повышается качество приема беспроводного трафика.

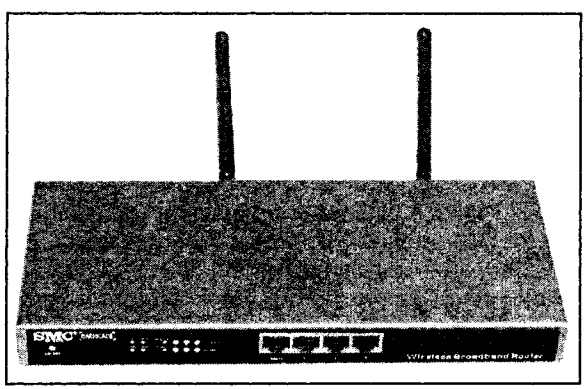


Рис. 6.5. Маршрутизатор SMC Networks Barricade (фотография предоставлена SMC Networks)

IBSS и BSS

Когда две или более станций обмениваются информацией напрямую в специальном режиме, они образуют независимую элементарную абонентскую группу (Independent Basic Service Set, IBSS). В специальном режиме станции могут взаимодействовать лишь в том случае, если расстояние между ними не превышает дальность передачи. На рис. 6.6 показан пример схемы из трех клиентских станций, находящихся в специальном режиме и формирующих независимую элементарную абонентскую группу. Если клиенту, расположенному в специальной сети, требуется установить связь с устройством, находящимся за пределами IBSS, он должен переключить режим работы на инфраструктурный и установить связь с точкой доступа.

В инфраструктурном режиме каждый клиент взаимодействует с точкой доступа. Она исполняет роль Ethernet-моста, осуществляя перенаправление кадров либо к другой беспроводной станции, либо в проводную инфраструктуру. Точка доступа вместе с использующими ее клиентами образуют базовую абонентскую группу (Basic Service Set, BSS). Так как во время обмена информацией между двумя станциями точка доступа, в сущности, действует как повторитель, диапазон BSS может превышать диапазон IBSS. На рис. 6.7 приведен пример базовой абонентской группы, получающейся из инфраструктурной беспроводной локальной сети.

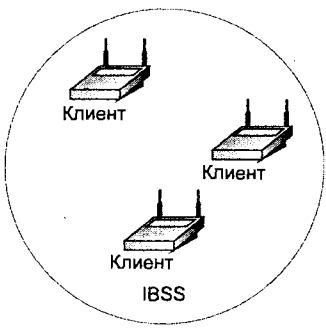


Рис. 6.6. Пример специальной сети, образующей независимую элементарную абонентскую группу (IBSS)

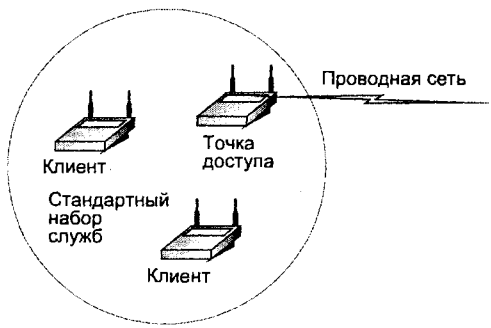


Рис. 6.7. Пример базовой абонентской группы, сформированной на основе беспроводной инфраструктурной сети

Система распределения

В среде беспроводной локальной сети области действия отдельных базовых абонентских групп связываются с помощью системы распределения (Distribution System, DS). DS может формироваться посредством беспроводной локальной сети, связывающей несколько точек доступа, промежуточной точки доступа, действующей как радиочастотный ретранслятор, или другой системы связи. На самом деле, стандарт IEEE 802.11 предоставляет право формирования системы распределения пользователю.

Ассоциация и аутентификация

Прежде чем обмениваться информацией с точкой доступа, станция должна установить с ней связь. Установка связи — это двухэтапный процесс, затрагивающий три состояния. В исходном состоянии станция не аутентифицируется и не ассоциируется с какой-либо точкой доступа. Во втором состоянии, на первом этапе, станция аутентифицирует себя на точке доступа, но не устанавливает ассоциацию с ней. В третьем состоянии, на финальном этапе, станция выполняет аутентификацию и ассоциацию с точкой доступа. Станции переключаются между этими тремя состояниями, обмениваясь с точкой доступа сообщениями в форме управляющих кадров. Чтобы прояснить процесс аутентификации и ассоциации, а также разобраться в других вопросах безопасности беспроводных локальных сетей, мы ознакомимся с меха-

низмом выполнения станцией самообнаружения и самоаутентификации на точке доступа.

Радиомаяки и SSID

Все точки доступа через фиксированные промежутки времени передают маяковые управляющие кадры. Маяковый кадр идентифицирует точку доступа путем включения в свой состав ее сетевого имени. Для обозначения последнего существует технический термин — идентификатор абонентской группы (Service Set Identifier, SSID). Обычно SSID определяется при конфигурации AP, но в некоторых точках доступа по умолчанию используется хорошо известное имя наподобие "wireless" (беспроводной), или MAC-адрес, встроенный в постоянное запоминающее устройство (Read-Only Memory, ROM).

Клиентская станция ожидает получения маяковых кадров, которые реализуют механизм идентификации точек доступа в рамках определенного диапазона. Клиент выбирает, к какому BSS присоединиться, в зависимости от выделенного для него сетевого имени. Таким образом, сетевое имя, или SSID, рассматривается некоторыми субъектами как сетевой пароль. К сожалению, по целому ряду причин, SSID является очень плохим паролем. Во-первых, SSID в рамках маякового кадра передается в незашифрованном виде, и его раскрытие не представляет большой сложности для неавторизованных третьих лиц. Во-вторых, на множестве Web-сайтов вы можете без труда найти руководства по точкам доступа различных производителей, в которых будет указано SSID, или сетевое имя, по умолчанию применяемое каждой точкой доступа. В-третьих, наиболее важным для многих неавторизованных третьих лиц, желающих присоединиться к точке доступа, является факт существования двух настроек клиента, которые обычно позволяют обойти настройки SSID в точке доступа. Этими двумя настройками конфигурации являются "any" и пробел. Целью установки "any" или пробела является возможность для клиентской станции получить список SSID, или сетевых имен, от точек доступа в рамках диапазона клиента. Следовательно, оператор клиента сможет выбрать ту точку доступа, с которой он захочет работать.

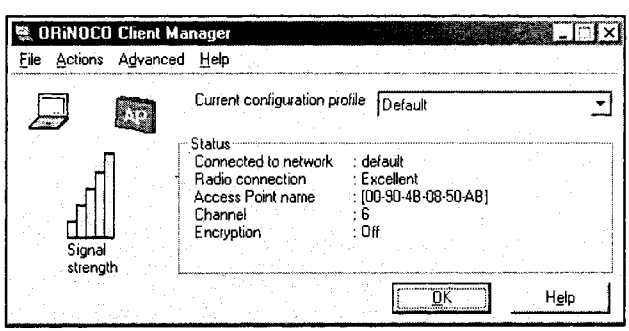


Рис. 6.8. Использование Orinoco Client Manager для обращения к точке доступа SMC Networks, сетевое имя которой соответствует ее MAC-адресу

На рис. 6.8 изображена сервисная программа Orinoco Client Manager от Agere Systems, обеспечивающая обращение платы PC Card беспроводной локальной сети Orinoco к

широкополосному маршрутизатору/точке доступа SMC Networks Barricade. Чтобы подсоединиться к точке доступа SMC Networks, автор установил в клиенте Orinoco сетевое имя "any". В результате появилась возможность радиосоединения с точкой доступа SMC Networks, применяющей SSID в форме MAC-адреса. Если внимательно посмотреть на рис. 6.8, можно заметить группу под названием **Status**, в которой имя точки доступа определено как 00-90-4B-08-50-AB. Это — MAC-адрес маршрутизатора SMC Networks Barricade и одновременно сетевое имя, по умолчанию используемое этим устройством.

Методы аутентификации

После установки одинаковых или эквивалентных сетевых имен для клиентской станции и точки доступа эти устройства обмениваются несколькими управляющими кадрами в целях взаимной аутентификации. В соответствии со стандартом IEEE 802.11, поддерживаются два метода аутентификации: открытая система и общий ключ. Методом аутентификации по умолчанию является открытая система. Само его название говорит о том, что эта система обеспечивает возможность удовлетворения любых запросов об аутентификации. Следовательно, ее можно рассматривать как несущественный аутентификационный процесс.

Второй метод аутентификации называется общим ключом. Он основан на применении секретного ключа WEP, настраиваемого на клиентской машине и на точке доступа. Совместно с вектором инициализации он используется для генерации псевдослучайной последовательности, которая, в свою очередь, обеспечивает шифрование данных.

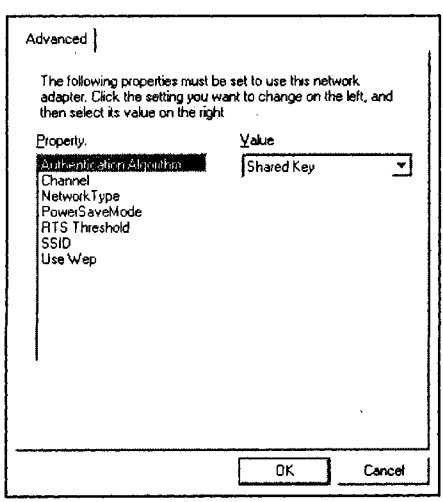


Рис. 6.9. Применение диалогового окна конфигурации клиента SMC Networks для задания аутентификации по общему ключу

На рис. 6.9 проиллюстрирована конфигурация клиента SMC Networks, предусматривающая использование аутентификации с общим ключом. При такой настройке станция, становящаяся инициатором, передает управляющий кадр запроса на аутен-

тификацию, в котором фиксирует просьбу о применении общего ключа. Получатель такого запроса на аутентификацию, в качестве которого в нашем примере выступает точка доступа, отвечает клиенту передачей кадра, управляющего аутентификацией. Этот кадр содержит 128 байт текста для опознания, полученного с применением генератора псевдослучайных чисел WEP из общего секретного ключа и случайным методом выбранного вектора IV. По получении текста, содержащегося в управляющем кадре, инициатор расшифровывает его и использует свой общий ключ и новый случайно выбранный вектор IV, чтобы закодировать его в новом кадре. Этот зашифрованный управляющий кадр затем передается ответчику. Тот расшифровывает полученный кадр и проверяет правильность значения контрольной суммы ICV, а также соответствие расшифрованного текста 128 байтам, направленным в исходном тексте для опознания. Если все предыдущие этапы успешно завершены, процесс аутентификации признается успешно завершившимся. В таком случае инициатор и ответчик меняются ролями, и вышеописанный процесс повторяется — для того, чтобы обеспечить действенность взаимной аутентификации.

Получив знания на тему обращения клиента к точке доступа, рассмотрим физическую и логическую конфигурацию точек доступа.

Настройка точки доступа

С физической точки зрения, типичная точка доступа обычно подсоединена с помощью кабеля к проводной инфраструктуре для обеспечения связи между беспроводными и проводными станциями. Точка доступа функционирует как MAC-мост, выполняя операции лавинной маршрутизации, переадресации и фильтрации кадров наподобие проводного моста Ethernet.

Точки доступа с возможностями маршрутизации обычно поддерживают протокол DHCP и трансляцию сетевых адресов (NAT). DHCP предоставляет точке доступа возможность динамического назначения или аренды IP-адресов клиентам, прошедшим аутентификацию и ассоциированным с ней. Так как клиенты беспроводной локальной сети являются станциями в частной внутренней сети, наделение каждого из них общеопознаваемым IP-адресом было бы в высшей степени расточительным действием. Вместо этого, большинство точек доступа поддерживают использование адресов по стандарту RFC 1918. В качестве памятки, документ RFC 1918 (под названием "Выделение адресов для частных интерсетей") определяет три блока адресного пространства IP для частных внутренних сетей. Эти блоки адресов таковы:

```
10.0.0.0-10.255.255.255 (префикс 10/8)
172.16.0.0-172.31.255.255 (префикс 172.16/12)
192.168.0.0-192.168.255.255 (префикс 192.168/16)
```

Обратите внимание, что первый блок предоставляет один номер сети класса A, второй — набор из 16 смежных номеров сети класса B, а третий — набор из 256 смежных номеров сети класса C.

Дублирование IP-адресов может произойти в том случае, если две или несколько организаций подключат свои частные сети к Интернету, продолжая при этом пользоваться адресами RFC 1918. Это породит абсолютную неразбериху в маршрутизации и приведет к невозможности прямого использования станций, настроенных с учетом адресов RFC 1918, в Интернете. Чтобы избежать такой ситуации, необхо-

димо задействовать промежуточное устройство, которое будет заниматься трансляцией (преобразованием) сетевых адресов. В мире беспроводных межсетевых коммуникаций в качестве такого промежуточного устройства обычно выступает комбинированный маршрутизатор/точка доступа, наподобие широкополосного маршрутизатора SMC Networks Barricade, изображенного выше на рис. 6.5.

Большинство комбинированных маршрутизаторов/точек доступа осуществляют трансляцию сетевых адресов путем преобразования адресов RFC 1918, выделенных клиентам с помощью DHCP, в единственный IP-адрес. Чтобы выполнить эту задачу и позволить множеству станций одновременно получать доступ в Интернет, процесс NAT генерирует таблицу отображения адресов RFC 1918 в номера верхних портов. Иногда это действие называется трансляцией адресов портов (Port Address Translation, PAT). В результате создается таблица преобразования, позволяющая множеству клиентских станций пользоваться единым общедоступным IP-адресом, т. к. адреса RFC 1918 отдельных клиентов отличаются друг от друга по номерам портов, использованных в процессе преобразования.

На рис. 6.10 изображено главное меню экрана **Configuration** беспроводного широкополосного маршрутизатора SMC Networks Barricade. Внимательно изучив содержимое этого и некоторых других, дополнительных, экранов, связанных с этим продуктом, мы сможем разобраться в настройках, необходимых для конфигурации точек доступа или комбинированных маршрутизаторов/точек доступа.

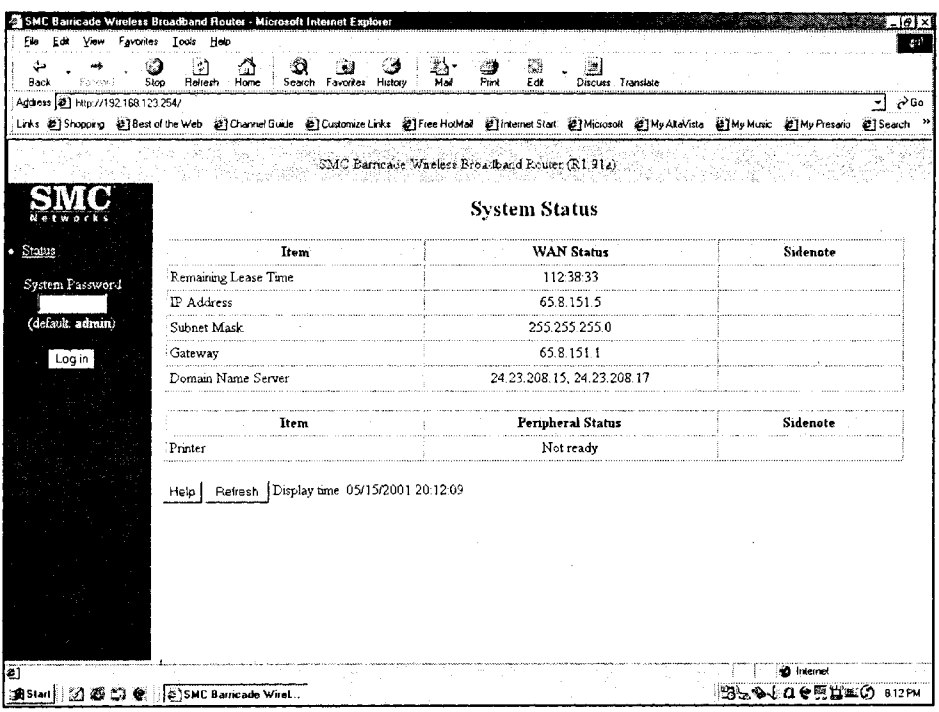


Рис. 6.10. Чтобы начать работу с широкополосным маршрутизатором SMC Networks Barricade, вы должны ввести системный пароль

Взглянув на левую часть изображения на рис. 6.10, вы обратите внимание на поле ввода системного пароля. В области экрана, находящейся чуть ниже этого поля, пользователь, выполняющий конфигурацию устройства, информируется о значении по умолчанию — "admin". Подобно другим производителям, SMC Networks поставляет свои продукты с настройками по умолчанию, которые следует заменить сразу после интеграции устройства в производственную среду. В противном случае, т. е. в случае сохранения системного пароля, принятого по умолчанию, вы получите вопиющую проблему системы безопасности. Происхождение этой проблемы связано с тем, что точка доступа периодически транслирует маяковые кадры, идентифицирующие устройство. Приложив некоторые усилия — скажем, выполнив поиск сетевого руководства или отправив ряд Ping-запросов, — можно выяснить адрес RFC 1918, применяемый частной сетью в точке доступа/маршрутизаторе. Если взглянуть на адресную строку браузера, показанного на рис. 6.10, станет понятно, что настройки, по умолчанию принимаемые в беспроводных широкополосных маршрутизаторах SMC Networks Barricade, определяют IP-адрес RFC 1918 192.168.123.254. Таким образом, если системный пароль, исходно принимаемый по умолчанию, не изменить, любой желающий, введя в адресную строку своего браузера этот адрес, сможет получить доступ к экрану конфигурации.

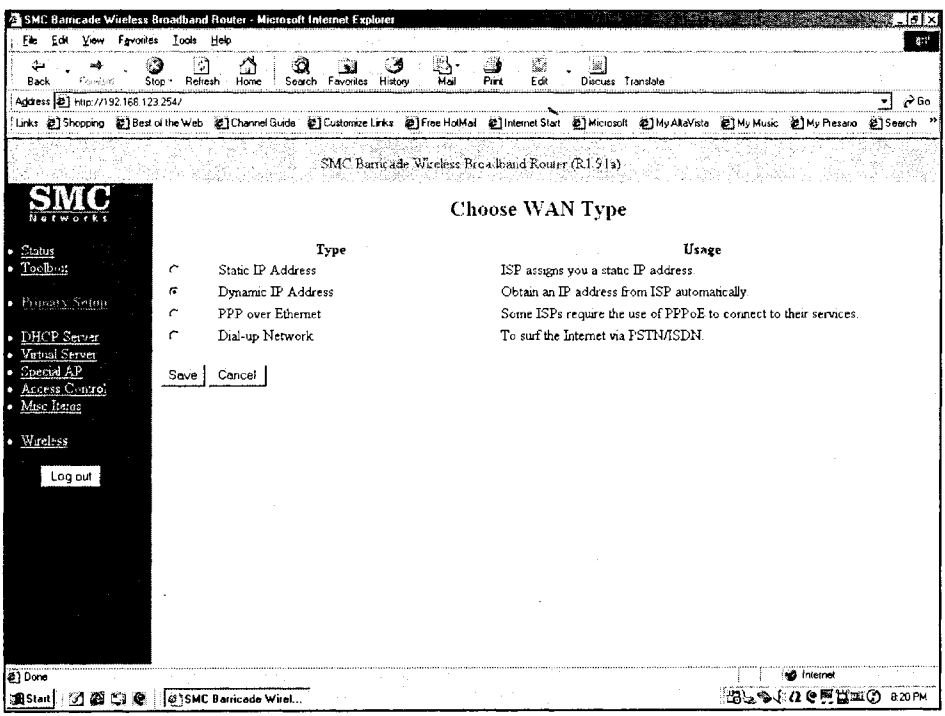


Рис. 6.11. Выбор типа соединения с глобальной сетью в настройках широкополосного маршрутизатора SMC Networks Barricade

После успешного входа на экран конфигурации вы столкнетесь с рядом конфигурационных вариантов. На рис. 6.11 приводится пример вариантов (опций), между ко-

торыми пользователь может выбирать. Они показаны в левой части рис. 6.11, причем в активном состоянии находится ссылка **Primary Setup** (в результате ее выбора появляется окно под названием **Choose WAN Type**). Окно **Choose WAN Type** показано в правой части данной иллюстрации. Чтобы настроить комбинированный маршрутизатор/точку доступа для подключения к глобальной сети, на этом экране конфигурации вы можете выбрать одно из четырех положений переключателя. Так как автор пользовался интернет-соединением по кабельному модему, для которого его поставщик услуг сети Интернет выделяет динамический IP-адрес, переключатель был установлен во второе положение (**Dynamic IP Address**).

В дополнение к настройке соединения с глобальной сетью, SMC Networks предусматривает еще несколько экранов конфигурации с некоторым количеством средств настройки безопасности. Пользуясь рассматриваемым комбинированным маршрутизатором/точкой доступа, вы получаете возможность включить WEP с 64- или 128-разрядным секретным ключом, а также (по желанию) скрыть FTP-порт. Кроме того, вы можете воспользоваться экраном конфигурации управления доступом для фильтрации пакетов, получаемых из сети Интернет, на основе нескольких параметров, в числе которых — их IP-адреса и номера портов; эта возможность напоминает таблицу доступа к маршрутизатору компании Cisco. Что касается сокрытия FTP-порта, беспроводной широкополосный маршрутизатор SMC Networks Barricade позволяет пользователю определить для FTP-доступа из Интернета номер порта, отличный от 21. Это не совсем механизм обеспечения безопасности, но все же он предохраняет FTP-сервер от случайного наблюдения.

Благодаря тому, что программы наподобие AirSmart и WEPCrack способны обнаруживать секретный ключ, пассивно записывая 4—5 миллионов кадров, некоторые производители теперь обеспечивают поддержку динамической замены ключей WEP. Одним из примеров этой возможности могут выступить беспроводные точки доступа Cisco Aironet. Вы можете либо согласиться с периодом замены ключей WEP, принимаемым по умолчанию, либо настроить точки доступа Cisco на динамическую замену секретных ключей по прошествии заданного периода времени.

Выявление неисправностей

В заключительной части нашего исследования функций беспроводной локальной сети мы сосредоточимся на ряде методик, которые могут оказаться полезными, если клиенты вашей беспроводной сети, получая сигнал от точки доступа, тем не менее, не смогут обмениваться друг с другом информацией. Если вы пользуетесь конфигурационной утилитой из числа тех, что поставляются с большинством клиентских плат адаптеров для беспроводных локальных сетей, обратите внимание на индикатор уровня сигнала. Он может быть представлен в виде одной или нескольких горизонтальных или вертикальных линеек; с другой стороны, возможно, он обозначает получаемый сигнал определителями "прекрасно", "хорошо", "плохо" или "отсутствует" или любым другим набором слов. Пример индикатора уровня сигнала в виде ряда вертикальных линеек уже приводился на рис. 6.8.

Важно отметить, что обозначение высокого уровня сигнала значит лишь, что клиентская станция "слышит" сигналы, приходящие с точки доступа. Само по себе это не означает, что клиент и точка доступа настроены согласованно. Если клиент во-

обще не отображает уровень принимаемого сигнала, или он предельно низок, возможным решением проблемы может быть изменение положения антенн на одном или на обоих устройствах.

Проверьте размещение точки доступа и клиента. Если получить последовательность сигналов, тем не менее, не удается, следует проверить окружение на предмет потенциальных источников электромагнитных помех. К примеру, микроволновые печи и новейшие модели беспроводных телефонов работают в 2,4-гигагерцевом частотном диапазоне. Другим потенциальным источником помех могут быть Bluetooth-совместимые устройства (например, карманные компьютеры и некоторые сотовые телефоны), поскольку они также действуют в частотном диапазоне, применяемом стандартом 802.11 и расширением 802.11b. Наконец, что не менее важно, необходимо убедиться в том, что программно-аппаратные средства на точке доступа, с одной стороны, и программно-аппаратные/программные средства на клиентской станции, с другой, соответствуют современным требованиям. Нелишне периодически заходить на Web-сайт производителя и интересоваться наличием обновлений для применяемого вами аппаратного обеспечения. Кроме исправлений старых ошибок, в обновлениях могут присутствовать новые функции.

Добившись последовательности сигналов между клиентом беспроводной локальной сети и точкой доступа, необходимо определить наличие/отсутствие возможности обмена информации между этими двумя устройствами. Чтобы протестировать связь между ними, можете отправить Ping-запрос с клиента на точку доступа. Если ответ на такой запрос будет получен, значит, возможность соединения между клиентской станцией и точкой доступа существует. Кроме того, получение Ping-ответа указывает на корректную конфигурацию обоих устройств, обеспечивающую возможность приема подобных ответов. Если же ответа на Ping-запрос не последует, весьма вероятно, что конфигурации оборудования на клиенте и точке доступа несовместимы. Таким образом, на каждом из устройств необходимо проверить настройку включения/отключения WEP, а также структуру секретного ключа.

Хороший способ избавиться от проблемы WEP в случае неполучения Ping-ответа — отключить WEP на клиентской станции и на точке доступа. Если после этого ответ точки доступа на Ping-запрос получить удастся, вы будете знать, что проблема заключалась в конфигурации WEP. Если же вас опять постигнет неудача, попробуйте воспользоваться методами, описанными в предыдущих двух абзацах.

Если вы получите ответ на Ping-запрос, отправленный на точку доступа, но, тем не менее, не сможете подсоединиться к удаленному компьютеру в сети Интернет или в проводной локальной сети организации, подключенной к точке доступа, значит, вероятнее всего, проблема заключается в конфигурации соединения с глобальной сетью на точке доступа. В такой ситуации вам следует тщательно изучить конфигурацию DHCP и NAT, и проверить правильность присвоения устройствам IP-адресов, а также корректность их преобразования в единый IP-адрес, применяемый для соединения с сетью Интернет и выхода на интерфейс проводной сети. Если вы аккуратно выполните все вышеописанные действия, скорее всего, вам удастся изолировать и разрешить проблемы, связанные с конфигурацией: именно они составляют подавляющее большинство всех проблем коммуникации в беспроводных локальных сетях.

Дополнительные ресурсы

Беспроводные продукты Agere Systems Orinoco: **www.orinocowireless.com/**.

Cisco Systems: **www.cisco.com/**.

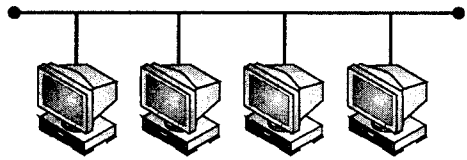
Linksys: **www.linksys.com/**.

Беспроводные продукты Netgear: **www.netgear.com/**.

SMC Networks: **www.smc.com**.

Институт инженеров по электротехнике и электронике: **www.ieee.org**.

Общество по проблемам совместимости в беспроводных сетях Ethernet (Wireless Ethernet Compatibility Alliance): **www.wi-fi.org/**.



ГЛАВА 7

Введение в технологию глобальных сетей

Глобальная сеть (Wide Area Network, WAN) используется для объединения географически удаленных узлов. Как правило, с ее применением связана необходимость аренды оборудования у сторонней организации, а именно — у поставщика телекоммуникационных услуг (провайдера), или, как его еще называют, у владельца сети связи ("carrier"). Расходы на глобальную сеть составляют самую значительную долю в стоимости владения корпоративной сетью. Следовательно, именно в этой области компромисс между ценой и производительностью наиболее резко выражен и критичен.

В этой главе рассматриваются три основных класса WAN-технологий: синхронные последовательные линии, технология коммутации пакетов и технология коммутации каналов. Важнейшие технологии, образующие эти категории, будут обсуждаться и анализироваться с позиций проектирования, внедрения и обслуживания. В этом разделе вопросы разработки рассматриваются только в связи с различными наиболее важными технологиями глобальных сетей. Кроме того, будут проанализированы мотивы, побуждающие к выбору той или иной технологии.

Технологии глобальных сетей традиционно разделяются на три фундаментальные категории. Сначала будут рассмотрены синхронные последовательные или двухточечные выделенные линии с точки зрения проектирования сети. Второй категорией, которую мы изучим, будет технология коммутации пакетов в глобальной сети. С некоторой натяжкой ретрансляцию кадров (Frame Relay), X.25 и асинхронный режим передачи (Asynchronous Transfer Mode — ATM) можно описать как технологии коммутации пакетов. Ретрансляция кадров претерпела значительные усовершенствования, и в настоящее время эта технология вытесняет X.25; по этой причине обсуждать последнюю в данной главе мы не будем: трудно себе представить, чтобы какую-нибудь новую сеть проектировали на основе X.25. Технически ATM можно описать как ретрансляцию ячеек, т. к. в этой технологии происходит коммутация ячеек фиксированной длины, а не фреймов переменной длины. Тем не менее она помещается в одну категорию с ретрансляцией кадров. Мы обратимся к мотивам применения ATM, а также обсудим основные проблемы проектирования, связанные с реализацией этой технологии. Третьей категорией является коммутируемая глобальная сеть, или глобальная сеть с коммутацией каналов. С этой технологией мы ознакомимся на примере ISDN (Integrated Services Digital Network — цифровая сеть с комплексными услугами). В данной главе будут изучены и специфические трудности, связанные с различными применениями ISDN.

Синхронные последовательные линии

Последовательную линию можно арендовать у поставщика услуг связи, и это позволит напрямую соединить два узла. Схематично такое решение показано ниже (рис. 7.1), где выделенная линия со скоростью передачи 256 Кбит/с связывает два офиса, находящиеся в Нью-Йорке и Чикаго.

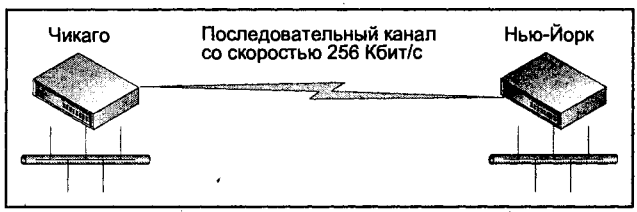


Рис. 7.1. Двухточечная выделенная линия

Таким образом, упрощается связь между локальными сетями указанных офисов. К примеру, клиентские машины в Нью-Йорке могут регистрироваться на серверах в Чикаго, обмениваясь соответствующим трафиком по выделенной линии. Естественно, то же самое могут делать пользователи в Чикаго.

Если говорить о физическом соединении, то выделенная линия соединяется с сетью поставщика услуг с помощью устройства обслуживания канала и данных (Channel Subscriber Unit/Data Subscriber Unit, CSU/DSU). Именно этим устройством в здании клиента заканчивается выделенная линия. В Соединенных Штатах клиент обычно покупает CSU/DSU. В других частях света это устройство, напротив, принадлежит и управляется владельцем сети связи. Таким образом, положение демаркационной линии, на которой ответственность переходит от клиента к хозяину сети связи, может варьироваться.

Каждый терминальный узел соединения синхронизируется от единого источника тактирования, расположенного в пределах сети поставщика услуг. Частота или скорость такого тактирования эквивалентна закупленной пропускной способности. К примеру, линия со скоростью передачи 64 Кбит/с тактируется на скорости 64 Кбит/с. CSU/DSU выполняет роль телекоммуникационного оборудования (Data Communications Equipment, DCE), и одной из его основных функций является распространение тактов, получаемых из общедоступной сети. Как правило, CSU/DSU подсоединяется к маршрутизатору по кабелю V.35 или X.21. В качестве интерфейса между локальной и глобальной сетью может выступать и мост, однако маршрутизаторы заняли место мостов по причинам, обсуждаемым в *гл. 14*. Маршрутизатор может быть подключен к CSU/DSU с помощью кабеля EIA/TIA-232, но в этом случае скорость ограничивается до 115,2 Кбайт/с. Маршрутизатор является устройством, обращающимся к службе глобальной сети, и для его обозначения применяется выражение "терминальное оборудование" (Data Terminal Equipment, DTE).

Скорости последовательной линии кратны базовому блоку — 64 Кбайт/с, а восходит это к голосовой телефонии. Спектр звуковых частот человеческого голоса лежит в диапазоне от 300 Гц до 3,4 кГц. Таким образом, ширина спектра составляет приблизительно 4 кГц. Это — аналоговый голос. При его передаче по цифровым каналам аналоговый сигнал необходимо дискретизировать, а затем аппроксимировать циф-

ровым потоком битов. В соответствии с теоремой Найквиста, при дискретизации аналогового сигнала цифровая частота дискретизации должна быть по крайней мере в два раза выше наибольшей частоты сигнала. Таким образом, дискретизация голосового сигнала должна осуществляться с частотой 8 кГц. Каждая выборка кодируется 8 разрядами, и в результате получается, что аналоговому голосовому сигналу соответствует цифровая скорость передачи данных 64 Кбит/с.

Итак, отдельный цифровой канал составляет 64 Кбит/с. В Соединенных Штатах скорость цифрового канала зачастую снижается до 56 Кбит/с. Это происходит при передаче сигналов по методу "избыточный бит", который предусматривает выделение одного из каждых восьми бит на цели самой передачи сигналов.

Пропускную способность последовательной линии можно наращивать по формуле $n \times 64$ Кбит/с до 2 Мбит/с; в результате получается 30 каналов. Магистральные скорости в сети, принадлежащей поставщику услуг, соответствуют плезиохронной цифровой иерархии (Plesiochronous Digital Hierarchy, PDH[1]). Четыре канала со скоростью передачи 2 Мбит/с мультиплексируются до 8 Мбит/с. Каналы со скоростью передачи 8 Мбит/с мультиплексируются (x4) до 34 Мбит/с. Соответственно, следующий показатель каналов характеризуется скоростью 140 Мбит/с. Эти значения не в точности соответствуют умножению предыдущих показателей на четыре, т. к. фактические скорости передачи в битах не совсем равны скоростям, приведенным здесь. Дело в том, что какой-то процент пропускной способности необходимо задействовать для кадрирования, передачи сигналов и управляющих служебных сигналов. В Соединенных Штатах применяется несколько другая иерархия PDH, т. к. в качестве главного элемента выступает скорость передачи 56 Кбит/с. В нижеследующей таблице (табл. 7.1) приводятся итоговые значения пропускной способности PDH как для Соединенных Штатов, так и для Европы; они олицетворяют два традиционно различных подхода к цифровому мультиплексированию.

Таблица 7.1. *Значения пропускной способности линий PDH*

Европа (бит/с)	**Соединенные Штаты (бит/с)**
64 K	56 K (DS-0)
2 M (E-1)	1,54 M (T-1)
8 M	
34 M (E-3)	45 M (T-3)
140 M	

Клиент волен приобрести канал, действующий на любой из этих скоростей. Впрочем, самые высокие скорости, как правило, оказываются востребованными клиентами с крайне высокими требованиями по пропускной способности и очень толстыми кошельками.

По показателю производительности плезиохронные оптические сети уступают место синхронной цифровой иерархии (Synchronous Digital Hierarchy, SDH) или синхронной оптической сети (Synchronous Optical Network, SONET), как она называется в

[1] PDH — европейский стандарт для волоконно-оптических сетей. — *Ред.*

Штатах. Эта высокоскоростная технология передачи на оптической основе предназначена для магистральных сетей поставщиков телекоммуникационных услуг. Ее основополагающий модуль — 155 Мбит/с; он называется STM-1 (Synchronous Transmission Module — синхронный транспортный модуль). STM-4 соответствует 622 Мбит/с. SDH/SONET олицетворяет существенное достижение по сравнению с PDH; оно выражается в повышенной эффективности мультиплексирования и демультиплексирования, а также в улучшенной управляемости.

Как бы то ни было, высшие уровни иерархии цифрового мультиплексирования не имеют прямого отношения к клиентам из сферы малого или среднего бизнеса.

Свободная выделенная линия представляется простейшим и наиболее укоренившимся методом связывания географически рассредоточенных узлов, но он же является самым дорогим. Основное преимущество синхронных выделенных линий — это их технологическая простота. Это значит, что для размещения и выявления неисправностей этой технологии требуется наименьшая квалификация, а это в конечном итоге может снизить издержки на обслуживание. Применение двухточечных линий последовательной передачи также связано с минимальными накладными расходами, в результате чего увеличивается фактическая пропускная способность и устраняются дополнительные источники задержек и дрожания (т. е. колебания задержек). Последовательные каналы при достаточной пропускной способности потенциально способны демонстрировать превосходные характеристики качества обслуживания (Quality of Service, QoS). Основными источниками задержек и дрожания в последовательном канале являются процедуры организации очередей и установления последовательности выдачи (сериализация) пакетов, выполняемые на маршрутизаторе. Задержка пакетизации может произойти в случае, если небольшой пакет ожидает пересылки по каналу крупного пакета. Задержки этого типа более вероятны в низкоскоростных каналах. Впрочем, финансовая смета пропускной способности всегда имеет рамки, и существуют более эффективные по цене методы сокращения задержек и дрожания в последовательных каналах. Сложные технологии организации очередей предусматривают фрагментирование крупных пакетов и присвоение высокого приоритета небольшим пакетам; в результате в последовательном канале обеспечивается более равномерный профиль задержек. Это особенно важно в отношении чувствительных к задержкам приложений реального времени, таким как пакетированный голос, видео и мультимедиа.

Самым критичным недостатком последовательных выделенных линий является их стоимость — она настолько значительна, что в настоящее время во многих отраслях промышленности каналы этого типа рассматриваются как неэффективный метод использования дорогостоящей пропускной способности. Эти соображения подтолкнули к переходу от технологии последовательных выделенных линий к технологиям коммутации пакетов, таким как ретрансляция кадров и асинхронный режим передача (ATM); при условии высоких требований к пропускной способности они демонстрируют более высокую эффективность.

Синхронные последовательные каналы, или выделенные линии, являются наиболее традиционными из всех технологий глобальных сетей, получивших сегодня распространение. Это действительно самая простая технология глобальных сетей, но, как бы то ни было, при планировании внедрения последовательных каналов следует принимать во внимание следующие соображения.

- Применение последовательных выделенных линий зачастую оборачивается наиболее значительными расходами на пропускную способность в глобальной сети.

Чтобы соблюсти баланс "затраты/эффективность" в отношении выделенных линий, уровень их использования должен превышать минимум в 50 процентов пропускной способности, т. к. абонент платит за приобретаемую скорость канала, и объем затрат не зависит от уровня его применения. Определяясь с тем, какая скорость выделенной линии будет для вас адекватной, необходимо принять во внимание существующие уровни трафика и оставить некоторое пространство в расчете на рост.

- Выделенные линии менее гибки, чем другие технологии глобальных сетей, в отношении корректировки доступной пропускной способности. Такие технологии, как ретрансляция кадров и ATM, предусматривают покупку гибкого профиля пропускной способности, который, как правило, можно без труда изменить. Для выделенных линий гибкость характерна не всегда. Следовательно, перед приобретением выделенной линии следует провести тщательное планирование загрузки.
- Преимущество синхронных последовательных каналов заключается в том, что непроизводительные издержки, связанные с ними, ниже, чем у технологий коммутации пакетов наподобие ретрансляции кадров или ATM.

Ниже приводятся возможные варианты выбора протокола канального (2-го) уровня для последовательных линий.

- HDLC (High-Level Data Link Control — высокоуровневый протокол управления каналом). Является производным от протокола SDLC (Synchronous Data Link Control — синхронное управление передачей данных) компании IBM, разработанного для поддержки единственного протокола, называемого SNA (Systems Network Architecture — системная сетевая архитектура). HDLC никогда не был стандартизирован для поддержки множества других протоколов, и по этой причине является специализированным протоколом. Большинство производителей сетевых продуктов разработали собственные реализации HDLC. В результате всего этого HDLC не может применяться в последовательной линии, соединяющей два маршрутизатора от разных производителей.

  Преимуществами HDLC являются простота функционирования и настройки. Кроме того, связанные с ним непроизводительные издержки (служебные сигналы и данные) минимальны. Указанные обстоятельства не стоит недооценивать: благодаря им HDLC вполне подходит в качестве протокола канального уровня для конфигурации с маршрутизаторами от одного производителя.

- PPP (Point-to-Point Protocol — протокол двухточечного соединения). Это сложный протокол канального уровня глобальной сети, который можно использовать в последовательных линиях и ISDN. Более подробный анализ его характеристик будет приведен ниже — в разделе, посвященном ISDN. Хотя он и сложнее HDLC, единственными значительными его дополнительными свойствами являются стандартность (а это может быть важно) и поддержка аутентификации CHAP (Challenge Handshake Authentication Protocol — протокол аутентификации с предварительным согласованием вызова).

  Аутентификация в условиях последовательного канала, вероятно, не так важна, как в открытой сети типа ISDN, но, тем не менее, она может стать надежным компонентом вашей политики безопасности.

- SLIP (Serial Line Internet Protocol — межсетевой протокол для последовательного канала). Даже и не думайте! Место SLIP занято PPP.

Резервирование последовательного соединения делает возможным его расширение, если работа одних последовательных линий поддерживается другими линиями, в частности, когда требуется, чтобы обслуживание не ухудшалось слишком сильно даже в случае отказа соединения. Потенциально более эффективные по цене решения включают следующие.

- Приобретение двух последовательных линий, которые вместе обеспечивают суммарное использование глобальной сети с данного узла. Эти соединения можно настроить на работу в режиме выравнивания нагрузки. Если одна линия выйдет из строя, в сети может проявиться ухудшение обслуживания вследствие перегрузки. Это — классический вариант соотношения цена/производительность.
- Применение иной технологии (например, ISDN) для восстановления сетевого соединения в случае неисправности последовательной линии. Кроме того, ISDN может принять на себя часть нагрузки последовательных линий при превышении определенного уровня информационного трафика. Это иногда называют "подкачкой полосы пропускания" (bandwidth top-up).
- Осуществление сжатия в последовательных каналах. Часто игра стоит свеч: алгоритмы сжатия увеличивают пропускную способность дорогостоящих выделенных линий. Степень увеличения пропускной способности зависит от конкретного типа сжатия и протокола, к которому сжатие применяется. Наряду с тем, что преимущества сжатия очевидны, у него есть два потенциальных недостатка.
  - Сжатие может потреблять значительные ресурсы процессора и памяти устройства, на котором оно выполняется. В алгоритмах сжатия используется принцип буферизации определенного объема данных и их анализа на предмет повторяющихся структур, что и позволяет производить сжатие данных. Некоторые методы сжатия наподобие Stacker применяют крайне сложный алгоритм. Его преимущество заключается в снижении нагрузки на память и объема буферизируемых данных. Недостатком алгоритма сжатия Stacker является потенциально высокий уровень потребления ресурсов процессора, причиной которому — опять же, его сложность. Алгоритм сжатия Predictor немного проще, а потому он в меньшей степени загружает процессор. С другой стороны, для выявления повторяющихся шаблонов он должен буферизировать более существенные объемы данных, а потому уровень потребления им ресурсов памяти выше, чем в случае со Stacker.
  - Обычно сжатие увеличивает временную задержку, которая может накапливаться, если сжатие осуществляется в нескольких последовательных соединениях между источником и приемником. Это может вызвать проблемы для приложений, сильно зависящих от времени, наподобие SNA или LAT.

    По этим причинам сжатие имеет смысл применять лишь в медленных каналах глобальных сетей, скорость передачи данных в которых колеблется от 56 до 128 Кбит/с.

При реализации сжатия следует принять во внимание несколько альтернатив. Сжатие можно осуществить посредством программного обеспечения, работающего на маршрутизаторе. С другой стороны, его можно выполнить с помощью аппаратного обеспечения, которое может быть либо встроенным в маршрутизатор, либо внешним по отношению к нему. В данном случае выбор следует делать исходя из параметров цены и производительности, которые, без сомнения, разнятся в зависимости от конкретного производителя.

Оценивая производительность сжатия, необходимо учитывать разные типы сжатия для заданных типов приложений и сетевого трафика. Большинство производителей аппаратного и программного обеспечения поддерживают следующие типы сжатия.

- Полное сжатие данных. Иногда этот тип называется сжатием канала, т. к. он компрессирует все данные, проходящие по каналу — и заголовки, и полезную нагрузку. Различные производители предусматривают сжатие такого типа либо на аппаратном, либо на программном уровне. Это хороший вариант для двухточечных последовательных линий. Степень повышения производительности варьирует в зависимости от конкретного продукта, выполняющего сжатие, и характера трафика.
- Сжатие заголовков. Этот тип сжатия часто реализуется программным обеспечением маршрутизатора и применяется к трафику, который главным образом состоит из заголовка — в качестве примеров такового можно привести сеансы Telnet, TAL или Xremote. В пакетах Telnet, скажем, присутствует 20-байтовый TCP-заголовок, IP-заголовок аналогичного размера и всего лишь 1 байт полезной нагрузки. Сжатие заголовков интенсивно использует ресурсы процессора, поскольку сжать только заголовок сложнее.
- Сжатие полезной нагрузки (payload). Этот тип сжатия также сопровождается значительным потреблением ресурсов процессора, и происходит это по той же причине. Сжатие полезной составляющей имеет смысл выполнять при ретрансляции разнотипных кадров по каналу с коммутацией пакетов (Frame Relay) или в асинхронном режиме передачи (ATM), поскольку при прохождении данных в этих средах заголовок канального уровня должен оставаться неизменным. Другими словами, идентификатор канального соединения (Data Link Connection Identifier, DLCI) или ATM-идентификаторы виртуального пути/канала (Virtual Path Identifier, VPI; Virtual Channel Identifier, VCI) не могут подвергаться каким-либо манипуляциям со стороны компрессии при прохождении через общедоступную сеть. Благодаря более эффективному использованию пропускной способности этот тип сжатия эффективен и с точки зрения затрат. К примеру, в один пакет ретрансляции кадров может входить несколько небольших IP-пакетов, и все они будут сжаты как полезная составляющая пакета. Впрочем, следует учесть, что сжатие не только способствует повышенной загрузке процессора, но и увеличивает время ожидания. В целом, если большая часть данных проходит по пути, состоящем более чем из трех транзитов между маршрутизаторами, данный метод сжатия применять не стоит. Это, конечно же, не непреложное правило, и его справедливость в каждом конкретном случае зависит от того, в какой степени трафик чувствителен к задержкам.

PPP и Multilink PPP

Протокол двухточечного соединения (PPP) действует на канальном (2-м) уровне; он является производным от HDLC и может работать через любой интерфейс терминального/телекоммуникационного оборудования (DTE/DCE). Он обеспечивает поддержку множества протоколов 3-го уровня и способен выполнять как синхронную, так и асинхронную передачу. Основные свойства PPP сделали его идеально подходящим как для сетей ISDN, так и для последовательных каналов.

В состав PPP входит компонент 2-го уровня — протокол управления связью (Link Control Protocol, LCP), который ведет "переговоры" с узлами о создании соединения

канального уровня, управлении и закрытии соединения. Кроме того, PPP поддерживает семейство протоколов управления сетевого уровня (Network Control Protocols, NCP), которые отвечают за поддержку большинства наиболее распространенных настольных протоколов 3-го уровня, включая IP, IPX, DECNET и AppleTalk.

Основными параметрами LCP, о которых необходимо "договариваться", являются проверки на предмет обнаружения ошибок, аутентификация, сжатие и Multilink PPP.

Аутентификация

Самым распространенным типом аутентификации в условиях канала PPP является протокол аутентификации с предварительным согласованием вызова (CHAP). Кроме того, в PPP присутствует поддержка других протоколов системы защиты — как более сложных типа TACACS, так и более простых наподобие протокола аутентификации пароля (Password Authentication Protocol, PAP). Преимущество, выгодно отличающее CHAP от PAP, заключается в том, что пароль шифруется именно с помощью CHAP, а следовательно, не может быть обнаружен сетевым анализатором. Если пароль незашифрован, он небезопасен, и это обстоятельство делает CHAP чуть ли не единственно возможным выбором среди всех протоколов аутентификации, поддерживаемых в PPP. Что еще приятнее, конфигурация и управление CHAP ничуть не сложнее, чем аналогичные операции с PAP.

Обнаружение ошибок

После организации канала PPP отправляет по нему "магическое число". Оно представляет собой уникальный поток битов. При получении точно такого же потока битов на том же конце канала (т. е. в той точке, из которой он был отправлен) PPP делает вывод о наличии в канале цикла. Зачастую этот тест преподносится как дополнительный пример изощренности PPP, но надо сказать, что это далеко не единственный протокол канального уровня для глобальной сети, обладающий способностью обнаружения циклов.

Сжатие

Для PPP можно настроить сжатие STAC или Predictor. Улучшение пропускной способности может варьировать в зависимости от того, какой протокол настольного ПК транспортируется. К примеру, коэффициент сжатия IP обычно немного выше, чем аналогичный показатель для IPX. При настройке сжатия, как и в случае с аутентификацией, важно убедиться в совместимости конфигурации на обоих концах канала. Быть может, это звучит банально, но на практике именно простые ошибки порождают большинство проблем.

Multilink PPP

Одним из последних достижений, относящихся к PPP, является стандарт Multilink PPP, или MPPP[1]. При использовании традиционного PPP в сетях ISDN возникали

[1] MPPP — стандарт IETF для соединения B-каналов в сети ISDN на основе PPP. — *Ред.*

проблемы в достижении эффективного использования двух B-каналов[1] одновременно. Маршрутизатор можно настроить на подключение второго B-канала либо при вызове ISDN, либо при превышении некоторого порога загрузки.

В нормальной ситуации трафик передается по первому каналу до тех пор, пока не понадобится второй канал для обеспечения пропускной способности. Это демонстрирует тот факт, что пока первый канал остается загруженным, второй канал иногда откликается на вызов ISDN, даже если истекло его время ожидания запросов.

При возрастании требований к пропускной способности задействуется второй канал. Пакеты могут отсылаться непосредственно обоими каналами. Однако нет никакой гарантии, что трафик двух каналов будет направлен по одному и тому же пути в рамках общедоступной сети ISDN; следовательно, нет гарантии, что по ходу перемещения к точке назначения данные в каналах подвергнутся одинаковым задержкам. Отсюда делаем вывод о высокой вероятности нарушения порядка поступления пакетов на маршрутизатор назначения. Это обстоятельство может стать источником проблем с ненадежными или крайне чувствительными ко времени передачи протоколами. Даже при использовании надежных протоколов очень большое количество повторных передач может свести на нет эффект применения двух каналов. К примеру, наблюдались такие случаи работы приложений на основе TCP, когда высокий процент повторных передач TCP приводил к тому, что пропускная способность двух каналов не сильно отличалась от одного.

Решение этой проблемы заключается в Multilink PPP. В этом расширении реализована функция упорядочивания, которая гарантирует, что на канальном уровне данные перекомпонуются в корректную последовательность; таким образом, необходимость в повторных передачах на более высоких уровнях отпадает. MPPP организуется на стадии настройки LCP, причем конфигурация, предусматривающая поддержку стандарта, должна быть выполнена на обоих концах. Способность MPPP к упорядочиванию позволяет рассматривать два B-канала как логически сгруппированный канал.

Выводы о PPP

Протокол двухточечного соединения подходит для последовательных каналов, на концах которых функционируют маршрутизаторы от разных производителей. К примеру, если стандартом в вашей собственной сети является маршрутизатор Cisco, а в сети вашего делового партнера установлены маршрутизаторы Nortel, и между этими двумя сетями организован последовательный канал, PPP представляется оптимальным решением. В отличие от HDLC, PPP является стандартом, что делает его идеальным выбором для неоднородных сред.

Функция обнаружения циклов, поддержка алгоритмов сжатия Stacker и Predictor — эти возможности характерны и для HDLC. Впрочем, PPP выделяется функциями аутентификации и многоканальности. Стандарт Multilink PPP практичен в условиях ISDN, и в этом вы убедитесь, ознакомившись с материалом, представленным далее в этой главе. Поддержка аутентификации CHAP — это еще одна причина, по которой для вызовов ISDN применяется именно PPP. ISDN во многом напоминает ши-

[1] B-канал (B channels или Bearer channels) — это два однонаправленных 64 Кбит/с канала сети ISDN. — *Ред.*

рокую открытую сеть, и любой домашний пользователь ISDN является потенциальным взломщиком вашей корпоративной сети. Аутентификацию PPP можно задействовать и в последовательных каналах, но там это не так критично.

Технология коммутации пакетов

Коммутация пакетов — это одна из трех основополагающих категорий технологии глобальных сетей. Разнородные узлы в сети предприятия связываются с помощью сети с коммутацией пакетов, принадлежащей поставщику услуг. Рассмотрим два узла, показанных на нижеследующей иллюстрации (рис. 7.2).

Рис. 7.2. Сеть с коммутацией пакетов

Трафик, проходящий от узла А к узлу В, выходит из локального маршрутизатора на узле А и входит в общедоступную сеть с коммутацией пакетов (которая, вероятнее всего, принадлежит поставщику телекоммуникационных услуг). Поставщик не предоставляет выделенного сквозного физического соединения между двумя узлами, как было бы в случае с прямым последовательным каналом. Вместо этого он обеспечивает направление сетью трафика, полученного от узла А, таким образом, что он в конечном итоге покидает сеть с коммутацией пакетов в узле В. Единицей коммутации трафика в общедоступной сети выступает пакет. Трафик, выходящий из маршрутизатора в узле А, всегда прекращает свое существование в узле В; следовательно, с точки зрения клиента, в отношении потока трафика это напоминает последовательный канал. Тем не менее между ними есть несколько фундаментальных различий. Этот тип соединения называется постоянным каналом, т. к. две конечных точки фиксированы. Но, т. к. на протяжении всего пути не существует никакого выделенного физического соединения, это соединение обозначается как постоянный виртуальный канал (Permanent Virtual Circuit, PVC).

Для владельца сети связи применение PVC вместо выделенных физических соединений является более эффективным по цене методом предоставления пропускной способности, и такое снижение стоимости распространяется на заказчика. Если вы как клиент не используете пропускную способность, которая предусматривается вашим PVC, владелец сети может незамедлительно предоставить ее другому покупателю. Процедура динамического распределения пропускной способности в соответствии с уровнем потребности в ней называется статистическим мультиплексированием (statistical multiplexing), а осуществляется она поставщиком телекоммуникационных услуг.

Хотя технология коммутации пакетов намного экономичнее прямых последовательных каналов, она не обеспечивает аналогичного уровня гарантии на сквозную пропускную способность, т. к. клиент, по существу, обращается к общей сети. Техноло-

гия коммутации пакетов не всегда обеспечивает тот же уровень качества обслуживания, что и последовательные каналы. Однако с учетом получаемой стоимости служб WAN-технологий, соотношение выгод и потерь признается многими клиентами стоящим.

X.25

X.25 — это старейший вид технологии коммутации пакетов, и он постепенно замещается более новым технологиям — в частности, ретрансляцией кадров. Эта технология коммутации пакетов разрабатывалась в эпоху, когда каналы глобальной сети все еще были относительно ненадежны. По этой причине в X.25 присутствует множество функций проверки ошибок, которые в большинстве современных сетей с их высоконадежными WAN-каналами лишь приводят к ненужным издержкам. Впрочем, X.25 все еще стоит уделять некоторое внимание, т. к. надежность этого протокола сослужила хорошую службу многим клиентам; отсюда — вялость перехода на новые технологии. Как бы то ни было, поскольку дни этой технологии, естественно, сочтены, рассматриваться она будет менее подробно, чем ретрансляция кадров далее в этой главе.

Пример кода далее по тексту относится к нижеприведенной иллюстрации, на которой показан простой и типичный образец IP на основе X.25 (рис. 7.3).

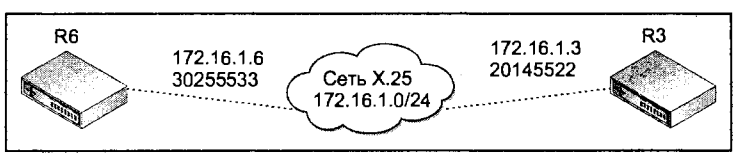


Рис. 7.3. Пример IP в сети на основе X.25

Эта конфигурация, как она выглядела бы на маршрутизаторе Cisco, справедлива для обоих маршрутизаторов. X.25 становится доступным в маршрутизаторе с помощью команды `encapsulation x25`. Это тот же тип последовательного интерфейса, который можно было бы применить в условиях прямого синхронного последовательного канала. Таким образом, что касается физического представления, здесь нет ничего нового. Доступ к сети X.25 осуществляется через локальный модуль обслуживания канала и данных (CSU/DSU). Помимо прочего, следует обратить внимание на то, что X.25 является нешироковещательной средой; таким образом, для того чтобы задействовать перенаправление широковещательных сообщений наподобие обновлений маршрутизации, необходимо ключевое слово `broadcast`.

```
r6#
interface Serial1
ip address 172.16.1.6 255.255.255.0
encapsulation x25
x25 address 20145522
x25 map ip 172.16.1.3 30255533 btroadcast
r3#
interface Serial0
```

```
ip address 172.16.1.3 255.255.255.0
encapsulation x25
x25 address 30255533
x25 map ip 172.16.1.6 20145522 broadcast
```

Виртуальные каналы X.25 идентифицируются с помощью адресов X.121. Эти адреса имеют глобальное значение, и в некотором отношении они схожи с телефонными номерами. Каждому устройству, которое обращается к сети X.25, выделяется адрес X.121.

В нашем примере IP действует в сети X.25. Это всего лишь означает, что виртуальные каналы X.25 осуществляют передачу IP-трафика сетевого уровня. Если пользователю локальной сети R6 потребуется обратиться к ресурсам локальной сети R3, маршрутизатор R6 должен быть запрограммирован на отправку соответствующего трафика на адрес 172.16.1.6, т. е. на IP-адрес интерфейса X.25 сети R3. Впрочем, здесь необходимо совершение еще одного, дополнительного действия. R6 необходимо "сообщить", какой адрес X.121 соответствует данному IP-адресу, т. к., в конечном счете, трафик требуется отправить по постоянному виртуальному каналу X.25. Именно в этом заключается назначение оператора

```
x25 map ip 172.16.1.3 30255533 broadcast
```

для R3. Маршрутизатор R6 располагает аналогичным оператором соответствия, необходимым для разрешения IP-адреса R3 в адрес X.25.

Ретрансляция кадров (Frame Relay)

Ретрансляция кадров — это WAN-технология, основанная на коммутации пакетов, распространенность которой все возрастает. Прослеживается тенденция замены ретрансляцией кадров старых, традиционных технологий наподобие X.25 и двухточечных последовательных каналов. В устройстве протокола ретрансляции кадров ставка сделана на повышенную надежность современных каналов глобальной сети. В отличие от X.25, протокол этот сам по себе не предусматривает никаких методов контроля ошибок. Он делегирует процедуры обнаружения и исправления ошибок более высоким уровням стека связи. С другой стороны, в технологии ретрансляции кадров присутствует контроль перегрузки, который выражается в сообщениях с уведомлениями о перегрузке.

Одним из факторов, стимулирующих переход к ретрансляции кадров, является ее способность приспосабливать закупленную пропускную способность к профилям потребления приложений, работающих в сети. Таким образом, ретрансляция кадров обеспечивает потенциал для более продуктивного и экономически эффективного использования часто расширяющейся пропускной способности глобальной сети. В целях сетевого резервирования может быть задействован механизм полного или частичного объединения постоянных виртуальных каналов (PVC).

Одной из причин, делающих популярным выбор ретрансляции кадров в качестве основной WAN-технологии, является ее способность обеспечить устойчивость с помощью механизма PVC. Имеет смысл подробнее рассмотреть различные топологические схемы ретрансляции кадров, поскольку они применимы к любой технологии, основанной на коммутации пакетов.

Концентратор и спица

Простейшей топологией ретрансляции кадров является классическая схема концентратора и спицы (или звезда), показанная на следующей иллюстрации (рис. 7.4).

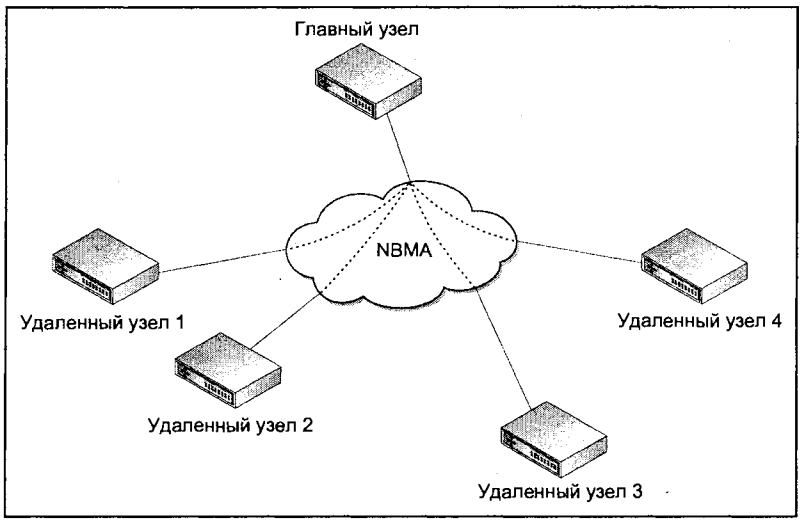


Рис. 7.4. Простейшая топология сети с ретрансляцией кадров

Каждый удаленный узел соединен с главным узлом с помощью отдельного постоянного виртуального канала. Любой обмен информацией между удаленными узлами должен осуществляться через узел-концентратор. Устойчивость такой конструкции, естественно, низка, т. к. отказ любого PVC приведет к потере соединения с глобальной сетью того удаленного узла, который им обслуживается.

Вторая проблема, связанная со звездообразной топологией, возникает, если между удаленными узлами существует значительный трафик. Это означает, что существенный трафик проходит по двум PVC, а не по одному, что, вероятно, не слишком эффективно с экономической точки зрения. Кроме того, трафик между удаленными узлами в такой топологии должен проходить по меньшей мере два транзита (hops) через маршрутизаторы, а целью любой схемы является сокращение количества транзитов. Таким образом, если два узла обмениваются достаточно большими объемами данных, имеет смысл напрямую провести между ними PVC.

Частичное объединение

Топология частичного объединения, пример которой показан на рис. 7.5, подразумевает наличие у большинства узлов (но не у всех) по меньшей мере двух PVC, по которым выполняется соединение с сетью ретрансляции кадров. Таким образом, отказ любого отдельного PVC не повлечет за собой потерю соединения с глобальной сетью хотя бы для одного узла.

Возможная проблема, связанная с частичным объединением, заключается в существовании точки отказа в виде маршрутизатора на главном узле. Эту проблему можно

разрешить путем организации двойного подключения удаленных узлов к разным маршрутизаторам узла-концентратора, как показано ниже (рис. 7.6). Иногда такую схему называют двойным частичным объединением. Маршрутизаторы-концентраторы можно расположить на разных узлах, что позволит добиться более серьезного уровня резервирования. В данном случае два маршрутизатора-концентратора нужно было бы связать посредством двух PVC (в целях резервирования) или, если

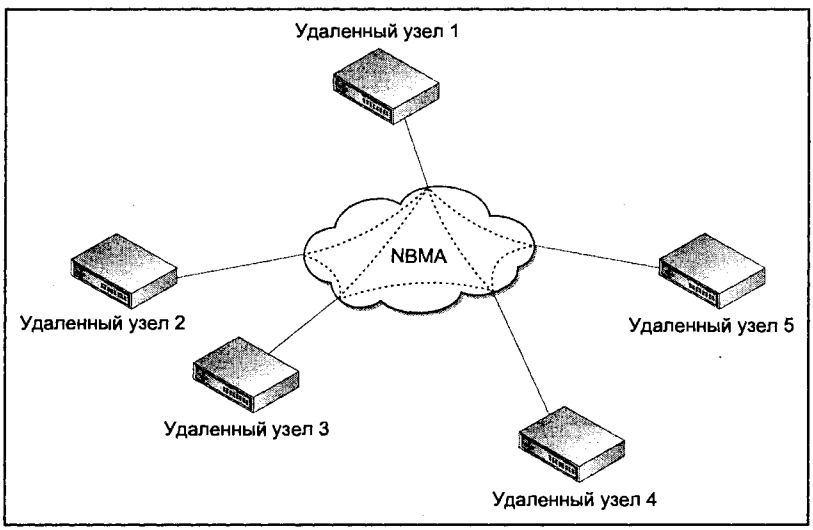


Рис. 7.5. Пример топологии частичного объединения

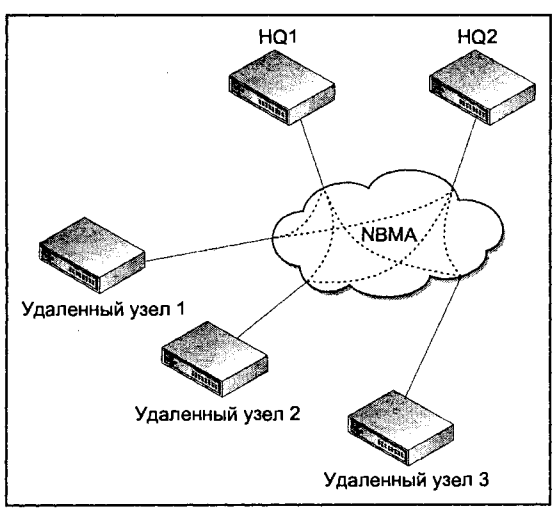


Рис. 7.6. Пример топологии двойного частичного объединения

два узла географически близки, с помощью устойчивой территориальной магистрали. Наличие двух центральных узлов для компании не всегда удобно, т. к. только один из них может быть хорошо приспособленным для размещения основных прикладных ресурсов. Но даже в этом случае на узле-концентраторе должно быть два маршрутизатора.

Полное объединение

Как показано ниже (рис. 7.7), топология полного объединения подразумевает прямое соединение всех узлов друг с другом. Естественно, уровень резервирования в такой схеме очень высок — впрочем, как и ее стоимость.

Обратите внимание, что на иллюстрации показано полное объединение четырех узлов. Чтобы такую топологию можно было организовать, необходимо в общей сложности шесть постоянных виртуальных каналов.

Если говорить о более общих правилах, можно утверждать, что при необходимости полного объединения n узлов общее количество PVC вычисляется по формуле $n(n - 1) / 2$. К примеру, чтобы обеспечить полное объединение 10 узлов, необходимо $10 \times 9/2 = 45$ PVC, и т. д. Что касается показателей устойчивости в сети из n узлов, от каждого узла отходит n PVC, и чтобы изолировать каждый конкретный узел, все они должны дать сбой. Это звучит впечатляюще, но, если неисправность вследствие какой-либо локальной проблемы случится в одном PVC, вполне вероятно, что вместе с ним откажутся работать несколько других. Дело в том, что достичь абсолютной устойчивости при наличии петли обратной связи на коммутатор ретрансляции кадров довольно сложно. И будет очень досадно обнаружить, что после столь серьезных затрат на обеспечение устойчивости все PVC будут заканчиваться на одном и том же блоке общего оборудования в местном центральном офисе! Лично я считаю, что частичное объединение с дополнительным резервированием с помощью другой технологии наподобие ISDN — это более оптимальное и экономически эффективное решение, чем полное объединение.

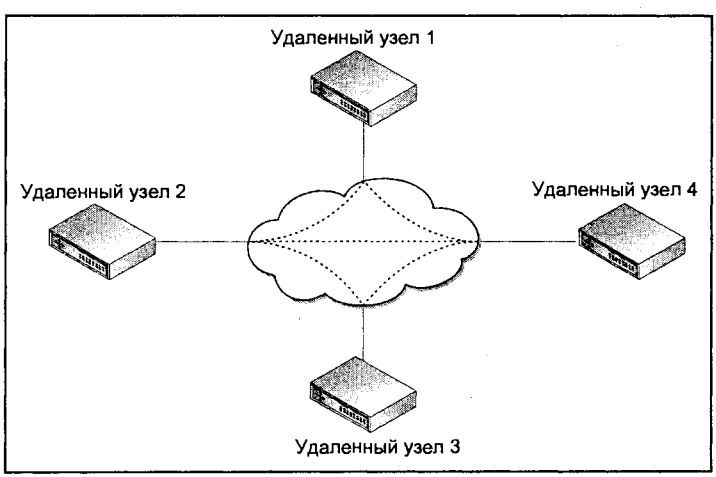


Рис. 7.7. Пример топологии полного объединения

Естественно, что основным фактором, ограничивающим применение полного объединения, являются затраты на его организацию. Впрочем, некоторые поставщики услуг предлагают конкурентные расценки на каналы PVC, которые используются исключительно для целей резервирования. Следовательно, это решение нельзя сбрасывать со счетов по одной лишь стоимостной причине, особенно в отсутствие надлежащего анализа затрат.

Как бы то ни было, есть и другая причина, по которой топология полного объединения встречается не так уж часто. Большинство современных инфраструктур связи не рассчитаны на обеспечение распространенной двухточечной передачи. Превалирует клиент-серверная модель, в которой серверные ресурсы сосредотачиваются на небольшом количестве узлов и не распространяются по сети равномерно.

Функционирование ретрансляции кадров

Протокол ретрансляции кадров функционирует между маршрутизатором или другим устройством доступа в сети ретрансляции кадров (Frame Relay Access Device, FRAD), с одной стороны, и локальным коммутатором ретрансляции кадров, который в большинстве случаев принадлежит поставщику услуг, с другой. Для обеспечения перекрестной связности используется постоянный виртуальный канал (PVC). PVC "постоянен", т. к. его конечные точки всегда одинаковы — точно так же, как и в выделенной линии. Слово "виртуальный" используется потому, что выделенное физическое соединение на всем пути через сеть поставщика услуг отсутствует. Напротив, поставщик услуг программирует коммутаторы таким образом, чтобы гарантировать, к примеру, что трафик, вошедший в сеть ретрансляции кадров из узла A, выйдет из этой сети, попав на узел B.

Таким образом, на самом элементарном уровне прослеживается схожесть с применением выделенной линии, соединяющей узел A с узлом B. Впрочем, есть ряд фундаментальных и очень серьезных различий. Так как ретрансляция кадров является технологией на основе коммутации пакетов, она связана с дополнительными непроизводительными издержками. Факт отсутствия выделенного физического канала на всем протяжении пути дает владельцу сети возможность выдвинуть предложение о гибкой пропускной способности, которое имеет шансы оказаться экономически эффективным с точки зрения клиента. Услуги ретрансляции кадров предусматривают приобретение согласованной скорости передачи информации (Committed Information Rate, CIR) для каждого постоянного виртуального канала (PVC). CIR — это та сквозная пропускная способность, наличие которой владелец сети гарантирует. Помимо нее клиент волен приобрести дополнительную пакетную скорость, которая и будет представлять собой максимальную скорость трафика, обеспечиваемую на всем протяжении PVC. Естественно, что максимально возможной пакетной скоростью будет являться физическая скорость клиентского канала доступа к поставщику услуг ретрансляции кадров. Впрочем, владелец сети не гарантирует передачу трафика со скоростью, превышающей CIR. CIR можно сравнить с билетом на самолет; в таком случае попытка передачи информации по сети со скоростью больше CIR подобна полету "по возможности". Сможете ли вы справиться с задачей, зависит от того, насколько загружена сеть. При превышении CIR все последующие пакеты маркируются меткой Discard Eligible (возможно отвержение) — для этого в заголовке ретрансляции кадров устанавливается разряд DE. Эта операция выполняется на локальном коммутаторе ретрансляции кадров. Если на узле в сети ретрансляции кад-

ров обнаруживается перегрузка, первыми выбрасываются пакеты с меткой DE. По выявлении перегрузки коммутатор ретрансляции кадров отправляет источнику сообщение BECN (Backward Explicit Congestion Notifier — обратное уведомление о явной перегрузке). Если уровень интеллекта отправляющего маршрутизатора или другого устройства доступа в сети с ретрансляцией кадров (FRAD) достаточен, это устройство может отрегулировать скорость отправки, снизив его до CIR.

Таким образом, клиент может рассчитать выбор CIR и максимальной пакетной скорости с тем, чтобы получить экономически эффективный профиль пропускной способности, адекватный всем прикладным требованиям. Приложения, использующие TCP, более устойчивы к выбрасыванию пакетов, а, следовательно, связанное с ними снижение производительности будет менее значительным, чем у ненадежных приложений на основе UDP. В отношении голосовых приложений слишком значительный процент выброшенных пакетов окажет негативное влияние на качество голоса. Есть и дополнительная проблема, которая может стать осязаемой при передаче голосового трафика со скоростью, превышающей CIR. Не говоря уже о выбрасывании трафика DE во время перегрузок, коммутатор ретрансляции кадров может выполнять ее буферизацию с использованием низкого приоритета. Таким образом, трафик, вероятно, достигнет пункта назначения, но со значительной задержкой; кроме того, он может демонстрировать дрожание и колебание задержки, что окажет серьезное влияние на качество голоса и воспроизведение в реальном времени. Следует избегать отправки трафика реального времени со скоростью, превышающей CIR, причем эту рекомендацию следует сделать общим правилом. Оно практично, т. к. службы ретрансляции кадров связаны с определенными гарантиями относительно пропускной способности, однако гарантий, связанных с недопущением задержек, они не предусматривают. Это обстоятельство может повлечь за собой необходимость применения отдельных PVC для трафика в реальном времени, с одной стороны, и обычного трафика с другой.

Сеть ретрансляции кадров может обеспечить устойчивую работу экономически эффективным способом. В резервных PVC CIR может быть ниже, чем в основных. Такой резервный PVC лучше всего располагать в кабельном туннеле, в котором нет локального коммутатора ретрансляции кадров, поскольку устойчивость должна быть не только теоретической.

Интерфейс локального управления при ретрансляции кадров

В целях поддержания активности протокола терминальное и телекоммуникационное оборудование (маршрутизатор в качестве DTE и коммутатор ретрансляции кадров в качестве DCE) обмениваются сообщениями интерфейсов локального управления (Local Management Interfaces, LMI) ретрансляции кадров. По умолчанию, DTE отсылает DCE LMI-сообщения с запросами о состоянии каждые 10 секунд, а DCE возвращает ответы о состоянии. Протокол LMI требует, чтобы интервал активности соединения на маршрутизаторе был меньше, чем на коммутаторе, с которым он осуществляет соединение. Сообщения с запросами и ответами о состоянии предназначены для подтверждения совместимости конфигураций и целостности канала между маршрутизатором и коммутатором, а также проверки состояния настроенных PVC. Оповещение о состоянии PVC является расширением протокола LMI — наряду с другими факультативными расширениями наподобие мультивещания, глобальной адресации и управления потоками.

Некоторые параметры LMI, такие как периодичность опросов и пороги ошибок, можно настраивать, однако в большинстве случаев необходимость в изменении значений по умолчанию отсутствует.

Таким образом, если резюмировать назначение сообщений LMI, которыми обмениваются маршрутизатор и коммутатор владельца сети ретрансляции кадров, можно сказать следующее:

- LMI исполняет роль механизма поддержания активности между маршрутизатором и концентратором;
- сообщения LMI, кроме того, содержат информацию о том, какие PVC прерываются на маршрутизаторе, а также данные о состоянии этих PVC — к примеру, об их активности/неактивности.

Отображение DLCI

При ретрансляции кадров PVC локально определяется с помощью идентификатора канального соединения (DLCI). Номер DLCI имеет значение исключительно в рамках обмена информацией между маршрутизатором и локальным коммутатором ретрансляции кадров. Таким образом, появляется возможность идентификации обоих концов PVC с помощью одного и того же DLCI. Номер DLCI применяется для того, чтобы локально различать множество виртуальных каналов, находящихся в пределах одного физического кабеля. Узлу, связанному с сетью ретрансляции кадров лишь одним PVC, требуется один DLCI. С другой стороны, в схеме частичного объединения узел, располагающий двумя PVC, должен различать их с помощью двух различных DLCI. Принцип DLCI как локально значимого адреса отличается от адресов X.121 и телефонных номеров ISDN, т. к. два последних являются примерами глобальной уникальной адресации.

Так что же происходит, когда IP функционирует через ретрансляцию кадров (а обычно так и есть)? Маршрутизатор на каждом из PVC ретрансляции кадров должен знать, каким DLCI воспользоваться, чтобы попасть на соответствующий IP-адрес следующего транзита. Оператор отображения DLCI привязывает адрес назначения следующего транзита для протокола настольного ПК к локальному DLCI. Важно четко понимать, что это значит, поскольку я наблюдал, как проблемы с отображением DLCI приводили к неразберихе. Помните, что DLCI в нерасширенной форме значим лишь локально — для DTE и DCE. Этот идентификатор обеспечивает различие между логическими каналами в пределах физического соединения с коммутатором ретрансляции кадров. Затем коммутатор ретрансляции кадров задействует каждый из этих каналов — в зависимости от своей собственной конфигурации в отношении каждого DLCI. Оператор отображения DLCI, в сущности, говорит маршрутизатору примерно следующее: "чтобы попасть на нужный адрес назначения, воспользуйся этим DLCI". Множество протоколов могут иметь адреса, отображаемые на один и тот же DLCI. В следующем примере маршрутизатор Cisco настроен на ретрансляцию кадров. IP-адрес линии ретрансляции кадров этого маршрутизатора — 192.168.250.2. Существуют два PVC, которые завершаются на этом маршрутизаторе, и им соответствуют два DLCI. Маршрутизатор с IP-адресом 192.168.250.1 связан с PVC, обозначенным через DLCI 201. DLCI 203 идентифицирует PVC, обеспечивающий соединение с IP-адресом назначения 192.168.250.3. Следовательно, локальный маршрутизатор знает, что для достижения 192.168.250.3 трафик необходимо

отсылать на локальный коммутатор, который в заголовке ретрансляции кадров обозначается как DLCI 203.

```
interface Serial0
 ip address 192.168.250.2 255.255.255.0
 encapsulation frame-relay IETF
 frame-relay map ip 192.168.250.1 201 broadcast
 frame-relay map ip 192.168.250.3 203 broadcast
```

Вероятно, вы заметили, что в конце каждого оператора отображения в этом примере присутствует ключевое слово `broadcast`. Ретрансляция кадров является нешироковещательной средой, а поэтому для того, чтобы широковещательные сообщения могли пересылаться в сети с ретрансляцией кадров, это ключевое слово необходимо. Не будь этого оператора, и обновления маршрутизации, сообщения IPX SAP и любой другой трафик на основе широковещания не смог бы передаваться в среде ретрансляции кадров.

Кроме статического соответствия, маршрутизатор может выявлять для протокола адрес назначения, относящийся к определенному DLCI, с помощью Inverse ARP.

Асинхронный режим передачи

Асинхронный режим передачи (ATM) часто описывают как технологию с коммутацией пакетов, поскольку в нем используются виртуальные каналы и многие принципы, аналогичные принятым в ретрансляции кадров. Однако технически это технология "поячеечной передачи", т. к. в целях минимизации задержек и дрожания устройства доступа ATM фрагментируют данные на ячейки с фиксированной длиной в 53 байт.

ATM — это компромиссная технология, призванная объединить стабильность пропускной способности и задержек, которая ассоциируется с традиционной технологией мультиплексирования каналов с разделением времени (Time Division Multiplexing, TDM), обладающих гибкостью технологий коммутации каналов. Более высокие уровни ATM обеспечивают поддержку сложных функций, таких как динамическое изменение маршрута в коммутируемых виртуальных каналах (Switched Virtual Circuits, SVC). Кроме того, ATM легко приспосабливается к условиям пульсирующего трафика. Небольшие ячейки фиксированной длины, которая составляет 53 байта, обеспечивают минимизацию колебания задержки и дрожания в глобальной сети. Несмотря на то, что в ATM реализуются многие принципы, схожие с ретрансляцией кадров, коммутация компактных ячеек фиксированной длины в сочетании с функциями качества обслуживания (Quality of Service, QoS), присутствующими в стеке протоколов ATM, делает эту технологию более подходящей для гетерогенных приложений и приложений реального времени.

Как правило, в корпоративных сетях с применением ATM в качестве технологии глобальных сетей выдвигаются высокие требования к пропускной способности. Минимальная скорость постоянного виртуального канала (PVC) ATM соответствует диапазону T-1/E-1, хотя более типичны скорости порядка 20 Мбит/с и выше. Изначально ATM разрабатывался с расчетом на масштабируемость пропускной способности вплоть до 155 Мбит/с, так что он идет рука об руку с технологией передачи SONET.

Ресурсы ATM и параметры QoS

Ретрансляция кадров предоставляет пользователю схожую гибкость пропускной способности. Вместе с ATM у поставщика услуг можно приобрести поддерживаемую на заданном уровне (среднюю) скорость передачи ячеек (Sustainable Cell Rate, SCR) и максимальную скорость передачи ячеек (Peak Cell Rate, PCR). Этот принцип во многом аналогичен CIR и EIR в ретрансляции кадров. Следовательно, как и при использовании ретрансляции кадров, покупатель располагает определенным контролем над скоростями доступа и может подкорректировать их в соответствии с прикладными требованиями.

Помимо параметров трафика, относящихся к скорости передачи ячеек, ATM содержит параметры качества обслуживания (QoS). Их можно запросить с помощью сетевого пользовательского интерфейса, а назначение их заключается в обеспечении лучшего уровня обслуживания для различных приложений, чувствительных к задержкам и потерям.

- *Коэффициент потери ячеек* (Cell Loss Ratio, CLR). Этот параметр определяет отношение выброшенных ячеек к общему количеству ячеек, переданных по соединению. Предположительно, он будет совершенно незначительным. CLR можно установить на максимум для приложения, чувствительного к потере пакетов, такого как информационное приложение на базе UDP.
- *Вариация задержки ячеек* (Cell Delay Variation, CDV). CDV выражает среднее колебание величины задержки в рамках соединения ATM за определенный период времени. От сети ATM можно затребовать максимальное качество CDV для приложений, не допускающих большие колебания задержки, таких как голос и видео.
- *Задержка передачи ячеек* (Cell Transfer Delay, CTD). CTD выражает общее сквозное время ожидания, или задержку, в рамках соединения ATM. Этот параметр можно задать для голосовых и информационных приложений, чувствительных ко времени.

Кроме того, ATM поддерживает ряд принципиально отличных классов услуг, относящихся к характеру распределения пропускной способности по сети ATM.

Стандарт ATM Forum определил четыре категории услуг; они перечислены ниже.

- *Постоянная скорость передачи битов* (Constant Bit Rate, CBR). Эта категория услуг гарантирует постоянство битовой скорости в виртуальном канале ATM. CBR является необходимым условием передачи высококачественных голосовых и видеоданных. Это наиболее дорогостоящий тип услуг в общедоступной сети ATM, т. к., чтобы соблюсти технические условия, поставщик должен выделить достаточную пропускную способность на всем протяжении PVC. Постоянная битовая скорость эквивалентна значению SCR, приобретаемому у поставщика услуг. Если трафик отправляется по PVC со скоростью, превышающей SCR, существует вероятность выбрасывания ячеек во время перегрузки сети ATM. Бит приоритета потери ячеек (Cell Loss Priority, CLP), определяемый в ATM-заголовке, может указывать на тот трафик, выбрасывание которого в такой ситуации допустимо.
- *Переменная скорость передачи битов* (Variable Bit Rate, VBR). Для данной категории услуг скорость битовой передачи может варьироваться в соответствии с состоянием сети. Предопределенный максимум скорости PCR в канале PVC можно

достичь лишь в том случае, если перегрузка сети полностью отсутствует, а гарантировать это, естественно, нельзя. Между устройством доступа ATM и коммутатором можно на определенный период времени организовать среднюю пропускную способность. Класс услуг VBR подходит для приложений с пульсирующими данными, которые не сильно чувствительны ко времени. VBR располагает стандартом, определенным для трафика, работающего не в реальном времени; этот стандарт называется VBR-NRT, и для передачи потока данных обычно используется именно он. Его эквивалент, связанный с данными в реальном времени, ожидает утверждения.

- *Доступная скорость передачи битов* (Available Bit Rate, ABR). ABR — это особый вид переменной битовой скорости. Между коммутатором ATM и маршрутизатором (или любым адаптером ATM, обращающимся к сети) организуется контур обратной связи. Адаптер запрашивает определенную скорость передачи битов, но соглашается со всем, что позволяет текущий уровень использования сети. Если предоставленная скорость передачи ниже, чем запрошенная, через определенный период времени, когда уровень использования сети спадет, коммутатор может ее увеличить. Аналогичным образом, если исходная запрошенная скорость коммутатором предоставляется, впоследствии, в случае повышения уровня использования сети, он может снизить ее. Несмотря на видимую сложность ABR, применение этой категории сопряжено с меньшими издержками, чем для классов услуг CBR и VBR, а связано это с тем, что в данном случае выполняется лишь ограниченное гарантированное выделение пропускной способности.
- *Неопределенная скорость передачи битов* (Unspecified Bit Rate, UBR). В случае использования UBR скорость передачи данных никак не гарантируется. Все ячейки, отправляемые устройством доступа, могут быть выброшены сетью, или же их передача в пункт назначения может оказаться неудачной. Фактическая пропускная способность всецело зависит от состояния сети. По этой причине UBR зачастую сравнивают с "полетом по возможности".

Уровень адаптации ATM (ATM Adaptation Level, AAL) подготавливает ячейки к передаче по сети ATM. На передающей стороне пакеты переменной длины сегментируются на ячейки фиксированной длины, а на принимающем конце происходит их повторная сборка. Эта функция уровня адаптации ATM так и называется: сегментация и повторная сборка (Segmentation And Reassembly, SAR). Для обеспечения оптимизированной передачи всего многообразия типов трафика с разными требованиями и характеристиками определено множество различных протоколов AAL.

Существует пять протоколов AAL с разными свойствами в части профиля скорости передачи битов, работы на основе соединения/без установления соединения, и временных характеристик. Наиболее часто применяемыми инкапсуляциями уровня адаптации являются AAL1 и AAL5.

- AAL1 работает на основе соединений и обеспечивает постоянную скорость передачи битов. Постоянство задержки достигается реализацией синхронизации соединения во времени на всем пути от источника до получателя. Постоянные битовая скорость и задержка делают AAL1 идеальным вариантом для приложений, чувствительных к задержкам, наподобие голоса и видео.
- AAL5 являются наиболее распространенными протоколами уровня адаптации ATM из тех, что применяются для передачи данных. AAL5 работает на основе соединений и обеспечивает переменную битовую скорость.

Тип протокола AAL для постоянного виртуального канала ATM определяется и настраивается на маршрутизаторе и коммутаторе ATM. На разных PVC можно задействовать разные протоколы AAL. Таким образом, один PVC можно использовать для передачи голоса и видео, а другой — выделить исключительно под данные.

Способность поддерживать различные протоколы AAL делает ATM протоколом, приспособленным для обслуживания приложений с отличающимися характеристиками и сетевыми требованиями.

Отдельно от внутренних параметров задержки, которые можно запросить, профиль передачи ATM можно регулировать и другими путями, чтобы сделать возможной поддержку всевозможных типов трафика с различными требованиями по транспортировке. Некоторые специалисты предпочитают использовать бит CLP, чтобы присвоить более высокий приоритет приложениям, чувствительным к задержке, наподобие голоса и видео. При условии превышения устойчивой скорости передачи ячеек (SCR) и одновременном обнаружении перегрузки сеть будет выбрасывать трафик с установленным битом CLP. Единственным преимуществом его установки при входе в сеть является то, что он предоставляет клиенту некоторый контроль над тем, какие ячейки получат CLP. Если, к примеру, принять решение о CLP-маркировке чувствительного к задержкам голосового трафика на базе UDP, чтобы он выбрасывался, но не откладывался, этот трафик будет всегда носить метку CLP — вне зависимости от условий трафика. В конечном счете это может означать, что другие клиенты получают трафик через сеть поставщика услуг за ваш счет.

ATM, как правило, используется для получения скоростей глобальной сети, превышающих уровень T-1/E-1, а увеличение скорости возможно вплоть до 155 Мбит/с. Таким образом, сегмент рынка этой технологии формируется высокими требованиями к пропускной способности и сетями со строгими спецификациями QoS.

Функционирование ATM

Несмотря на более широкие функциональные возможности, в ATM задействованы многие принципы, схожие с ретрансляцией кадров. Маршрутизатор в условиях ATM обменивается с коммутатором ATM сообщениями интегрированного интерфейса локального управления (Integrated Local Management Interface, ILMI). Эти сообщения являются механизмом поддержки активности между маршрутизатором и коммутатором. Кроме того, ILMI-сообщения позволяют маршрутизатору определять состояние всех своих PVC.

Идентификатор виртуального канала (VCI) и идентификатор виртуального пути (VPI) отождествляют каждый постоянный виртуальный канал (PVC) ATM. Виртуальный путь представляет собой лишь группу виртуальных каналов. Пара VPI/VCI, как и DLCI, значима исключительно локально — для маршрутизатора и коммутатора ATM. Группировка виртуальных каналов в виртуальные пути позволяет коммутаторам ATM задействовать большие группы виртуальных каналов посредством принятия решений на основании номера виртуального пути. Это — наиболее эффективный метод работы в условиях магистрали крупной сети ATM.

При использовании IP через ATM маршрутизатор в каждом PVC должен знать, какие идентификаторы VPI/VCI следует применить, чтобы добраться до нужного IP-адреса следующего транзита в дальнем конце PVC. Соответствие VPI/VCI необходимо для привязки адреса назначения следующего транзита настольного протоко-

ла к локальному идентификатору VPI/VCI. Возможна и статическая конфигурация этого соответствия на маршрутизаторах, но чаще всего она выполняется с помощью Inverse ARP. Для примера рассмотрим сеть, схема которой приведена ниже (рис. 7.8). Маршрутизатор X может определить, что для достижения адреса 172.16.1.3 необходимо воспользоваться идентификаторами VPI = 0 и VCI = 19. Пакеты, предназначенные для 172.16.1.3, сегментируются на ячейки размером в 53 байт каждая. Заголовок в каждой ячейке содержит VPI/VCI, что позволяет сети ATM направлять все ячейки в необходимый пункт назначения.

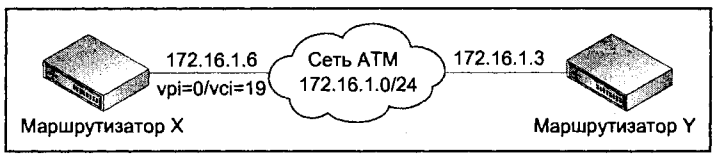


Рис. 7.8. Пример IP в сети ATM

Технология коммутации каналов

Коммутация каналов принципиально отличается от коммутации пакетов. При соединении на основе коммутации каналов передаваемая в пользование физическая линия охватывает непрерывную цепь на срок действия переключаемого соединения.

PSTN

Старейшим примером коммутации каналов является коммутируемая телефонная сеть общего пользования (Public Switched Telephone Network, PSTN). При совершении звонка цифры набираются по порядку, и именно это позволяет сети определить пункт назначения коммутации. Между вызывающей и вызываемой сторонами организуется выделенный канал, который сохраняется на протяжении всего времени вызова. Канал разрывается лишь по окончании звонка. Технология коммутации каналов является эффективным посредником при передаче голосовой информации именно потому, что она гарантирует выделенную сквозную пропускную способность на протяжении вызова. Этот принцип отличается от коммутации пакетов, при которой происходит обращение к общей сети, а доступная пропускная способность во время сеанса связи может изменяться.

Наиболее важным ограничением PSTN является пропускная способность. В табл. 7.2 представлена сводка теоретически максимальных скоростей, которые можно получить с помощью наиболее часто используемых модемных методик модуляции, стандартизированных Международным союзом телекоммуникаций (International Telecommunications Union, ITU).

Среди прочих ограничений, связанных с PSTN, следует упомянуть низкий уровень интеллекта и плохую управляемость, причина которой кроется в том, что абонентский канал между абонентом и центральным офисом телефонной компании — аналоговый по своей природе.

Таблица 7.2. Значения пропускной способности линий PSTN

Модуляция	Скорость (бит/с)
V.32	9 600
V32bis	14 400
V.34	28 800
V.34 Annex 1201H	33 600
V.90	56 000

ISDN

Название цифровой сети с комплексными услугами (ISDN) отчасти говорит само за себя. Это полностью сквозная цифровая сеть, принципиально отличающаяся от PSTN, в которой, несмотря на коммутацию и 100%-ную цифровую технологию передачи, абонентский канал является аналоговым. Даже в условиях наиболее современных реализаций PSTN устройства отправляют разряды в сеть с помощью аналоговых двухтональных многочастотных (Dual Tone Multiple Frequency, DTMF) сигналов. В ISDN разряды отсылаются локальному коммутатору ISDN в виде цифрового потока битов.

Термин "комплексные услуги" указывает на то, что при выделении достаточной пропускной способности сеть ISDN может предоставлять гетерогенное обслуживание, например, данных, голоса, видео и мультимедиа.

Подобно традиционной технологии PSTN, ISDN работает на основе соединений и коммутации каналов. Каждый из однонаправленных B-каналов характеризуется скоростью передачи в 64 Кбит/с и оптимизирован в расчете на традиционный голосовой трафик. Существуют две основные реализации ISDN. Интерфейс базового уровня скорости (Basic Rate ISDN, BRI) состоит из двух B-каналов и D-канала (D channel — дополнительный канал для задания конфигурации B-каналов) со скоростью в 16 Кбит/с для передачи сигналов. Интерфейс основного уровня скорости (Primary Rate Interface, PRI) ISDN состоит из 23 B-каналов и одного D-канала (в Соединенных Штатах), или 30 B-каналов и одного D-канала (в Европе). Скорость передачи по D-каналу в реализации основного уровня составляет 64 Кбайт/с, т. к. в этом случае задач, связанных с передачей сигналов, больше. Таким образом, сеть ISDN основного уровня предусматривает развитие скоростей до E-1/T-1.

В типичной реализации глобальной сети BRI применяется в рамках удаленных филиалов, а PRI — на центральном узле (узлах). По сути, ISDN как магистральная технология не является эффективной ни с технической, ни с экономической точек зрения. По приближенным подсчетам, если линия работает более 2—3 часов в день, затраты становятся запредельными, и с точки зрения соотношения затраты/эффективность ретрансляция кадров или выделенная линия выглядят более привлекательными. Оптимальным способом применения ISDN являются, в частности, периодические соединения со стороны удаленных узлов — к примеру, удаленных работников или небольших филиалов, для которых достаточно регулярных соединений с центральными серверами. Такие реализации ISDN часто называются предоставлением канала по требованию (dial-on-demand, DDR). Как бы то ни было, очень важно

правильно настроить маршрутизаторы на удаленных узлах — с тем, чтобы исключить вызовы ISDN по причинам, не связанным с необходимым применением этой технологии. Типичными примерами трафика, который может привести к неинформативным вызовам, являются динамические обновления маршрутизации и служебные сообщения приложений. По этой причине в условиях ISDN часто применяется статическая маршрутизация. Впрочем, благодаря непроизводительным административным издержкам статические маршруты плохо масштабируются в крупных сетях; отсюда и возникает необходимость в тщательном проектировании и конфигурации протокола динамической маршрутизации.

Помимо всего прочего, ISDN является весьма эффективным по цене решением задачи резервирования выделенной линии или ретрансляции кадров — именно потому, что тарификация ISDN производится на основе уровня ее использования. Другое преимущество ISDN лежит в его ориентированной на соединения природе, которая гарантирует, что в отдельном соединении по B-каналу пакеты никогда не смогут нарушить порядок прибывания к месту назначения и будут подвержены задержкам, носящим относительно постоянный характер. Чтобы увеличить пропускную способность, возможно, появится необходимость в объединении обоих B-каналов, которые в совокупности могут обеспечить скорость передачи 128 Кбит/с в один и тот же пункт назначения. Для того чтобы проделать эту операцию эффективно, необходим протокол наподобие Multilink PPP, который располагает специальным полем очередности, обеспечивающим строгий порядок прибытия пакетов в пункт назначения. Приложения, работающие в реальном времени, не терпят заметных колебаний задержки, возникающих из-за того, что пакеты проходят по общедоступной сети разными путями, в зависимости от применяемого B-канала. Кроме того, с непоследовательными пакетами не могут справляться ненадежные приложения на основе UDP. Даже в случае с надежными приложениями на базе TCP при наличии непоследовательных пакетов может потребоваться выполнение слишком большого количества повторных передач, а это, возможно, сведет на нет преимущества, связанные с использованием второго канала.

Надо полагать, приведенные варианты применения ISDN будут оставаться неизменными, что связано, прежде всего, со структурой тарификации, полностью зависящей от уровня использования.

Функционирование ISDN

Соединение ISDN с базовой скоростью обычно завершается на устройстве NT-1 (Network Terminator — сетевой терминатор) в помещении клиента. Подобно аналоговому телефону, NT-1 осуществляет переход от двух проводов к четырем. Кроме того, оно синхронизирует S-шину, а если к нему подсоединено несколько устройств, разбирает конфликты между ними. Обычно к NT-1 напрямую подсоединяется лишь одно устройство, хотя спецификация ISDN предусматривает подключение к S-шине до восьми устройств. Очевидно, только два таких устройства могут быть активны одновременно, т. к. 2 — это количество доступных B-каналов.

Маршрутизатор, напрямую подсоединенный к NT-1, как это в большинстве случаев и бывает, показан на рис. 7.9.

Интерфейс между терминалом ISDN и NT-1 называется S/T-интерфейсом. Это — один из основополагающих ориентиров, применяемых при составлении спецификаций для разных интерфейсов ISDN. Интерфейс между NT-1 и коммутатором связи

в местном центральном офисе ISDN называется U-интерфейсом. В некоторых регионах мира (особенно в Соединенных Штатах) ISDN присутствует просто в виде пассивного гнезда в стене, т. е. без применения NT-1. В таком случае у клиента должно быть собственное устройство NT-1. Именно поэтому многие маршрутизаторы объединяются с NT-1 и продаются в таком виде. Следовательно, ISDN-интерфейс на таком маршрутизаторе — скорее U-, чем S/T-интерфейс.

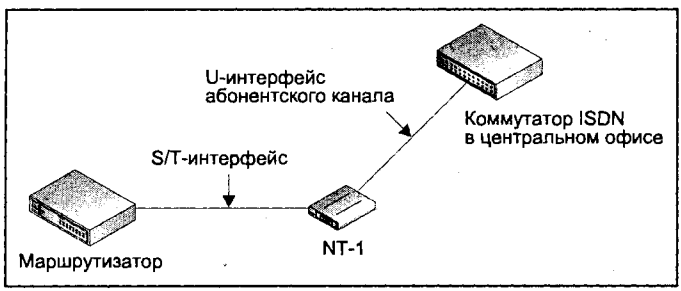


Рис. 7.9. Пример сети ISDN

ISDN-терминал (в нашем примере им является маршрутизатор) периодически обменивается сигнальными сообщениями Q.921[1] второго уровня с локальным коммутатором ISDN. С помощью этих сообщений коммутатор присваивает маршрутизатору значение терминального идентификатора конечной точки (Terminal Endpoint Identifier, TEI). Без этого значения маршрутизатор не может выполнять звонки ISDN.

Когда маршрутизатор пытается совершить вызов, он отправляет локальному коммутатору сигнальное сообщение Q.931[2] третьего уровня. Оно представляет собой простой запрос на организацию вызова, включающий номер терминала назначения. По своему характеру ISDN-адреса очень похожи на телефонные номера PSTN. Когда коммутатор получает запрос на организацию вызова Q.931, он направляет вызов в сторону пункта назначения, и делает это во многом аналогично современной цифровой телефонной сети.

При использовании IP через ISDN маршрутизаторы необходимо настроить таким образом, чтобы они знали, какой ISDN-номер следует вызвать, чтобы достичь IP-адреса назначения на другом конце сети. Рассмотрим следующую иллюстрацию, приведенную на рис. 7.10.

Маршрутизатор X определяет маршрут с помощью своей таблицы маршрутов IP, по данным которой для достижения адреса 10.1.1.0/24, адресом следующего транзита должен быть 10.7.7.3. Тот же маршрутизатор следует настроить с помощью оператора отображения номеров номеронабирателя, указывающего, что для обращения к 10.7.7.3 необходимо набрать 5551122 — ISDN-номер, связанный с маршрутизатором HQ.

---

[1] Q.921 — стандарт протокола LAP-D канального уровня (Link Access Protocol — протокол доступа к каналу связи). — *Ред.*

[2] Q.931 — протокол установления соединения сетевого уровня. — *Ред.*

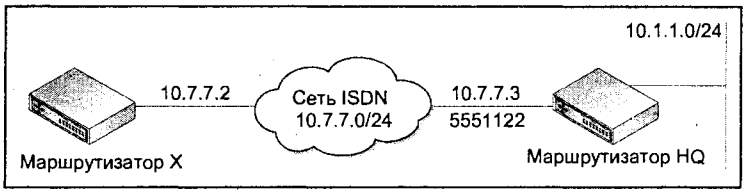


Рис. 7.10. Пример использования IP в сети ISDN

Если конфигурация сети недостаточно точна, неинформативный трафик может неумышленно запустить канал ISDN. К примеру, к его запуску могут привести широковещательные сообщения прикладного уровня или служебный трафик наподобие периодических обновлений маршрутизации; в результате это приведет к непомерно высоким расходам на вызовы. На маршрутизаторах можно настроить фильтры, которые исключат возможность инициирования вызова нежелательным трафиком. По той же причине в условиях ISDN динамическому протоколу маршрутизации часто предпочитают статическую IP-маршрутизацию.

Виртуальные частные сети

Виртуальная частная сеть (Virtual Private Network, VPN) — это зашифрованное соединение между двумя устройствами, способствующее безопасному обмену информацией между двумя доверенными сетями через ненадежный домен. Такое соединение, или VPN-туннель, пересекает ненадежную сеть наподобие Интернета, в результате чего появляется необходимость в шифровании конфиденциальной информации. Схема простой виртуальной частной сети между двумя аппаратными брандмауэрами показана ниже (рис. 7.11).

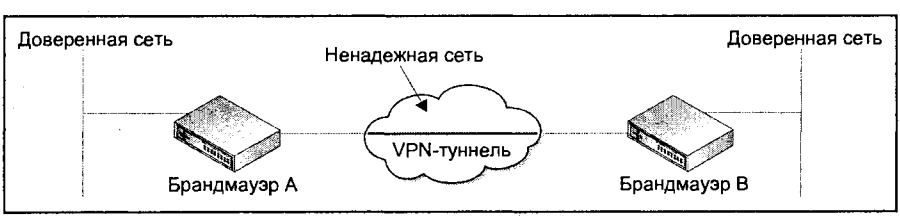


Рис. 7.11. Виртуальная частная сеть

VPN является логическим двухточечным соединением, при котором возможны следующие комбинации конечных устройств:

- от хоста к хосту;
- от шлюза к шлюзу;
- от хоста к шлюзу.

Хостами могут быть клиенты или серверы, а шлюзами — маршрутизаторы, брандмауэры, или интеллектуальные серверы.

Обычно VPN считается средством обеспечения защиты, а ее применение может помочь защитить соединение между двумя сетями. Впрочем, VPN гарантирует лишь

возможность организации канала связи с достаточным уровнем безопасности. Крайне важны конечные точки. К примеру, если между вашей собственной компанией и ее деловым партнером провести VPN, фактическая степень защиты будет зависеть от методов обеспечения безопасности на узле этого партнера.

При использовании VPN для соединения с другой сетью, уровень доверия в которой отличается от соответствующего уровня в вашей сети (как в случае с сетью бизнес-партнера), важно узнать следующие данные.

- Проводятся ли в удаленном офисе или в сети вашего делового партнера мероприятия по обеспечению защиты? К примеру, информированы ли они о новых угрозах, располагают ли соответствующими заплатами (patch) и решениями?
- Есть ли у вашего делового партнера действующая политика безопасности? Насколько тщательно она реализована? Какие элементы этой политики относятся к передаче информации *в* или *из* вашей собственной сети?

IPSec

Протокол IP версии 4 разрабатывался для реализации в сетях, которые считались безопасными. Поэтому обеспечение защиты не было неотъемлемым компонентом его проекта. Впрочем, существует множество протоколов системы защиты "заплатного" типа, которые можно объединить с IPv4. Одним из таких протоколов является IPSec (IP Security — протокол IP-защиты).

В среде IPv4 IPSec является факультативным компонентом, и каждый из партнеров по соединению должен осведомляться у другого на предмет поддержки им IPSec. В версии IPv6 поддержка IPSec обязательна. В таком случае есть возможность предположить, что всякая IP-передача с участием устройств IPv6 защищена. Структура адресации, характерная для IPv6, предусматривает использование 128 разрядов, однако существует проблема обратной совместимости с адресами IPv4, 32 разряда которых соответствуют младшим разрядам адреса IPv6, а в старших разрядах применяется постоянное предопределенное значение.

Протокол IP-защиты (IPSec) представляет собой набор открытых стандартов, который обеспечивает конфиденциальность данных через шифрование, целостность данных и аутентификацию между участвующими сторонами. IPSec предоставляет эти услуги на третьем уровне. Протокол обмена ключами в Интернете (Internet Key Exchange, IKE) применяется для управления взаимодействием узлов. Кроме того, IKE генерирует ключи шифрования и аутентификации, применяемые IPSec.

IPSec устанавливает защищенные туннели между двумя равноправными узлами сети, и в этом отношении он аналогичен реализации виртуальных частных сетей (VPN). Такими узлами обычно является пара аппаратных маршрутизаторов или брандмауэров. Эти конечные устройства должна быть настроены на обнаружение пакетов, которые считаются секретными и должны отсылаться через защищенные туннели. Определение параметров шифрования и аутентификации для туннеля также относится к конфигурации его защиты. Эту защиту можно задать ручной настройкой или через IKE-согласование двух узлов. Когда между узлами IPSec передаются так называемые "уязвимые" данные, IP-пакеты инкапсулируются в пакеты IPSec, которые содержат установленные параметры безопасности. Схематически отношения между узлами IPSec, применяющими аутентификацию и шифрование для защиты данных в туннеле IPSec, показаны на рис. 7.12.

Рис. 7.12. Отношения между узлами IPSec

В этом примере одноранговые узлы IPSec настроены на организацию защищенного туннеля в случае получения пакетов, обмен которыми производится между адресами 47.10.10.10 и 131.2.2.10 в любом направлении. Весь остальной трафик, проходящий между этими узлами, не подвергается шифрованию и не требует аутентификации.

Ниже вкратце изложены функции защиты, которые обеспечивает IPSec.

- Аутентификация данных. Аутентификация данных может включать две отдельных концепции.
  - Целостность данных. Проверка целостности данных должна производиться для того, чтобы гарантировать их неизменность. Этот элемент аутентификации данных является обязательным.
  - Аутентификация источника. Возможно осуществление дополнительной аутентификации источника данных. В ходе ее выполнения проверяется, действительно ли данные были отосланы заявленным отправителем.
- Конфиденциальность данных. Шифрование всего трафика, проходящего между узлами IPSec, обеспечивает сохранение конфиденциальности данных. Параметры шифрования наподобие ключей либо настраиваются вручную, либо устанавливаются с помощью протокола IKE.
- Антивоспроизведение. Эта функция позволяет получателю отклонить старые или дублированные пакеты, чтобы защитить его от атак повторного воспроизведения. Непрерывная повторная отправка одних и тех же пакетов зачастую свидетельствует об атаке типа "отказ в обслуживании".

Прежде чем приступать к внедрению IPSec, следует принять во внимание еще несколько вопросов и ограничений.

- На момент написания этих строк Проблемная группа проектирования Интернета (Internet Engineering Task Force, IETF) ратифицировала лишь те стандарты, которые касаются однонаправленного трафика IPSec. Никаких стандартов относительно многоадресного или широковещательного трафика до сих пор не разработано.
- Применение трансляции сетевых адресов (NAT) связано с проблемами интероперабельности. Как правило, следует использовать статическое преобразование для того, чтобы быть уверенными в непосредственном применении внешних глобальных адресов. Кроме того, трансляция должна выполняться перед инкапсуляцией IP-пакета в IPSec. Это гарантирует применение в IPSec глобальных адресов.

- С IPSec связаны заметные непроизводительные издержки и довольно высокий уровень загрузки центрального процессора. Наряду с процессами аутентификации и шифрования необходимо выполнять дополнительное действие — инкапсуляцию. В результате задержка может увеличиться, а требования к маршрутизаторам-терминаторам защищенных туннелей — повыситься в связи с дополнительной обработкой данных.
- Инкапсуляция IP-пакетов в IPSec может привести к превышению пакетом максимальной единицы передачи (Maximum Transmission Unit, MTU), установленной в данной передающей среде, а следовательно, — к фрагментации. Процесс повторной сборки связан с дополнительными непроизводительными издержками, что еще сильнее замедляет передачу информации. В отношении фрагментации есть еще один момент, который следует иметь в виду. Некоторые брандмауэры можно настроить на выполнение дополнительных проверок для выявления, и даже выбрасывания, фрагментированных пакетов, т. к. они часто используются при атаках типа "отказ в обслуживании". Если трудности возникают при передаче трафика IPSec брандмауэру назначения, наличие таких настроек следует проверить.
- IPSec пользуется номерами протокола 50 и 51, а IKE — номером 17 и UDP-портом 500. Эти протоколы и порты должны быть разрешены брандмауэрами и фильтрами пакетов на протяжении всего защищенного пути.

Заключение

Глобальная сеть выполняет функцию связывания географически рассредоточенных узлов. Различные варианты WAN-технологий обычно подразделяются на три четких категории: синхронные последовательные линии, технология коммутации пакетов и технология коммутации каналов.

Синхронные последовательные линии являются простейшим типом технологии глобальных сетей, т. к. узлы связываются прямыми двухточечными каналами, которые работают на скоростях, приобретенных у поставщика телекоммуникационных услуг. Владелец сети выделяет в ней путь с четко определенной пропускной способностью, тем самым соединяя узлы. Так как пропускная способность является фиксированной и не может быть передана другим клиентам, даже если она не используется, синхронные последовательные каналы, помимо прочего, являются самым дорогостоящим типом решения для глобальной сети.

В технологии коммутации пакетов для обеспечения межузловых связей применяются коммутируемые виртуальные соединения. Трафик коммутируется владельцем сети между источником и пунктом назначения, причем базовой единицей коммутации является пакет. Так как выделенные физические пути в данном случае отсутствуют, появляется возможность совместного использования пропускной способности разными клиентами. Метод, с помощью которого владелец сети динамически распределяет пропускную способность в зависимости от потребности в ней, называется статистическим мультиплексированием. Это решение более эффективно с экономической точки зрения, но в то же время полная гарантия сквозной пропускной способности невозможна, т. к. коммутация пакетов подразумевает обращение к среде, применяемой многими сторонами. Наиболее старым представителем технологии

коммутации пакетов является X.25, в настоящее время по большей части замененный ретрансляцией кадров. Технология ATM применима при наличии высоких требований в отношении пропускной способности.

Технология коммутации каналов подразумевает организацию выделенного физического канала между узлом-источником и узлом назначения, причем этот канал остается активным на протяжении всего сеанса связи. Классическим примером коммутации каналов является технология PSTN, при использовании которой выделенный физический канал, соединяющий вызывающего абонента с вызываемым, фиксируется в рамках сети на период вызова. Канал закрывается по окончании вызова. Развитие этого принципа для определенных информационных приложений демонстрирует ISDN.

Издержки, связанные с WAN-технологиями, обычно превышают все прочие издержки владения сетью. Таким образом, выбор технологии глобальной сети представляется важнейшим проектным решением — как с технологической, так и с экономической точки зрения. То, какую технологию вы сочтете оптимальной, зависит от требований по пропускной способности, профиля трафика (к примеру, трафик может быть постоянным, периодическим или пульсирующим) и финансовых ограничений. В конечном счете тип применяемой технологии и объем приобретенной пропускной способности могут быть сбалансированы для достижения компромисса между ценой и производительностью.

Дополнительные ресурсы

Руководство по ISDN Ральфа Беккера: **http://www.ralphb.net/ISDN/**.

Eicon Networks: **http://www.isdnzone.com/**.

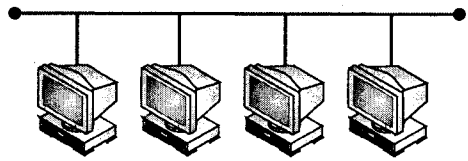
Marconi: **http://www.marconi.com/html/education/webbasedwantheory.htm**.

ArdRi Communications: **http://site.yahoo.com/cormac-s-long/wantec.html**.

RAD Data Communications: **http://www.rad.com/networks/netterms.htm**.

TechFest: **http://www.techfest.com/networking/wan.htm**.

Стэнфордский центр линейных ускорителей (Stanford Linear Accelerator Center): **http://www.slac.stanford.edu/comp/net/wan-mon/tutorial.html**.



ГЛАВА 8

Разводка сетевого кабеля

Независимо от того, работаете ли вы с локальной или с глобальной сетью, одним из компонентов ее инфраструктуры почти всегда будет обслуживание и выявление неисправностей сети. Дело в том, что за исключением беспроводной сети для физического соединения устройств в сеть необходимо использовать тот или иной вид кабеля. Конкретный тип кабеля зависит от применения сети, ее топологии, желаемой производительности и необходимой протяженности. В локальных и глобальных сетях используются три основных вида кабелей: коаксиальные, витая пара и оптические; их характеристики соответствуют тем или иным параметрам из числа вышеприведенных.

Коаксиальный кабель

Первоначально разработанный во время Второй мировой войны, коаксиальный кабель (coaxial cable; кроме того, в английском языке иногда употребляется сокращение coax) используется во многих узкополосных и широкополосных приложениях. Сфера применения коаксиального кабеля простирается от локальных сетей до кабельного телевидения и даже высокоскоростных телефонных каналов типа T-3 или DS-3. Некоторые распространенные типы коаксиального кабеля приведены в табл. 8.1.

Таблица 8.1. *Распространенные виды коаксиального кабеля и способы их применения*

Тип кабеля	Применение
RG-58A/U	Кабель с сопротивлением 50 Ом, в основном, применяемый для связывания "тонких" сетей (10Base2 Ethernet)
RG-8A/U	Кабель с сопротивлением 50 Ом, применяемый для связывания "толстых" сетей (10Base5 Ethernet)
RG-59/U	Кабель с сопротивлением 75 Ом, как правило, применяемый в системе кабельного телевидения
RG-62/U	Кабель с сопротивлением 93 Ом, применяемый в практически исчезнувшей сетевой архитектуре ARCNET

Если говорить о физическом устройстве коаксиального кабеля, то в него входит тонкий, одиночный медный провод, заключенный в оболочку из диэлектрического изолирующего материала и окруженный оплеткой, выполняющей функции экранирования и заземления. Для защиты от внешних условий проводник, изоляция и оплетка заключены в наружную защитную оболочку. Схема коаксиального кабеля приводится на рис. 8.1.

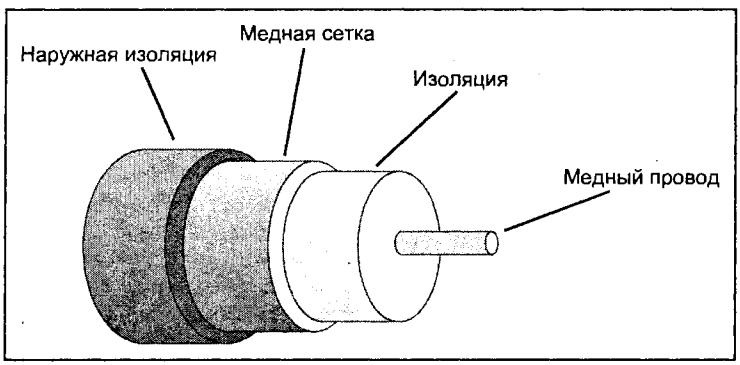


Рис. 8.1. Схема коаксиального кабеля

Благодаря своей структуре и экранированию коаксиальный кабель весьма устойчив к воздействию различного вида спектральных помех и является идеальным решением для больших протяженностей, на которых неэкранированная витая пара не может работать из-за чрезмерного ухудшения сигнала. К примеру, сеть Ethernet на основе коаксиального кабеля RG-58 (10Base2 или тонкого) характеризуется номинальной максимальной длиной в 185 м, а та же Ethernet на основе коаксиального кабеля RG-8A/U (10Base5 или толстого) может обеспечить максимальную протяженность в 500 м; для сравнения, максимальная длина Ethernet на основе витой пары (10BaseT) составляет 100 м. Мало того, что коаксиальный кабель помогает добиться значительной дальности передачи, он может работать в условиях довольно сильных спектральных помех или в среде со значительным электромагнитным излучением (Electromagnetic Interference, EMI) — например, в помещениях с электродвигателем или вблизи от балластного сопротивления флуоресцентных ламп.

К сожалению, также благодаря и конструктивным особенностям, скорость передачи в сети Ethernet стандарта 10Base2 ограничивается 10 Мбит/с, тогда как современная максимальная скорость Ethernet на базе витой пары достигает 1 Гбит/с (1000BaseT). Впрочем, следует иметь в виду, что коаксиальный кабель способен обеспечить более высокие скорости, но для этого его нужно применять вне стандарта Ethernet.

Узкополосная и широкополосная передача

За последние несколько лет применение термина "широкополосный" значительно расширилось; происходило это по мере того, как во все большем количестве домашних хозяйств появлялись высокоскоростные, постоянно активные средства связи с сетью Интернет типа кабельных модемов и цифровых абонентских линий

(Digital Subscriber Line, DSL). Если придерживаться традиционного значения этого термина, широкополосной называется любая передающая среда, по скорости передачи данных превосходящая обычную телефонную линию или обычную телефонную службу (Plain Old Telephone Service, POTS).

Передающие среды, не достигающие предельной скорости линии POTS, которая составляет 56 Кбит/с, обычно считаются узкополосными.

Впрочем, когда мы говорим об информационных сетях на основе коаксиальных кабелей, эти термины приобретают новое значение. Отчасти это происходит благодаря наличию двух способов передачи данных или сигналов по коаксиальному кабелю. Первый способ подразумевает изменение собственно уровня напряжения кабеля для передачи сигнала 0 или 1 (двоичного разряда). Эта задача выполняется путем установления уровня напряжения в −1,5 или +1,5 В постоянного тока, соответственно. Так как весь кабель используется как один канал, а передача сигналов осуществляется посредством изменения уровня напряжения, этот метод передачи называется *узкополосным*. Поскольку при узкополосной передаче данных доступен лишь один канал, единовременно передачу может осуществлять только одно устройство, хотя принимать данные могут все устройства в кабельной сети. В качестве отправной точки сети с тонким и толстым коаксиальным кабелем используют метод узкополосной передачи сигналов для пропускания пакетов данных по кабельной системе.

Второй метод передачи по коаксиальному кабелю намного сложнее узкополосного. Так как коаксиальный кабель может передавать сигналы в широком диапазоне частот, при *широкополосном* методе кабель не используется как единый канал с изменяющимся напряжением; напротив, кабель разбивается на множество каналов, и данные передаются на множестве различных частот. Такой способ организации каналов путем изменения частот передачи известен как *частотное разделение каналов* (Frequency Division Multiplexing, FDM). Разделение области частот не только позволяет различным устройствам осуществлять передачу в одно и то же время: если быть более точным, этот метод обеспечивает возможность одновременной передачи разнородных форм данных или сигналов (т. е. голоса, видео и данных). Широкополосная передача сигналов используется в системах кабельного телевидения (CATV, Cable TV) и кабельных модемов; в обеих средах она реализует передачу клиентам видеосигналов и данных.

Сети с тонким и толстым коаксиальным кабелем

Когда доктор Роберт Меткалфе, работая в Исследовательском центре Xerox в Пало-Альто (Xerox Palo Alto Research Center, PARC), в конце 1970-х гг. спроектировал сеть Ethernet, предполагалось, что она будет работать в шинной топологии (или в линейной цепи устройств) на основе двух различных типов коаксиального кабеля: RG-58 и RG-8A/U. Варианты Ethernet на базе коаксиального кабеля назвали *сетями с тонким коаксиальным кабелем* (thinnet) и *толстым коаксиальным кабелем* (thicknet), соответственно — из-за различий в толщине двух видов кабеля. У каждого из этих типов кабеля есть свои наборы особых характеристик, которые приведены в табл. 8.2; они определяют степень пригодности соответствующих типов для той или иной среды.

Сеть с тонким коаксиальным кабелем или 10Base2 Ethernet, как правило, используется для соединения сетевых устройств на скорости 10 Мбит/с с максимальной об-

щей дальностью в 185 м (от одного конца кабеля, или шины, до другого). Такая максимальная дальность определяется затуханием, или потерей сигнала на расстоянии, кабеля RG-58. По мере прохождения сигнала по кабелю он начинает ухудшаться и со временем становится настолько слабым, что устройство, расположенное дальше по каналу Ethernet, не может принимать этот сигнал с должной степенью надежности или перестает принимать его вообще. Так как тонкий и толстый коаксиальные кабели значительно различаются по толщине, величина затухания в тонком кабеле выше; к тому же, он более восприимчив к спектральным помехам. Тем не менее, несмотря на небольшую максимальную дальность тонкого коаксиального кабеля по сравнению с толстым, для соединения устройств, как правило, применяют именно тонкий кабель: благодаря значительно большему радиусу изгиба и удобству *Т-образных BNC-коннекторов* (Bayonet Nut Connector — байонетный соединитель) с ним намного проще работать.

Таблица 8.2. *Различные характеристики тонкого и толстого коаксиальных кабелей*

Характеристика	Тонкий коаксиальный кабель (RG-58)	Толстый коаксиальный кабель (RG-8A/U)
Диаметр проводника	0,94 мм	2,7 мм
Диаметр изоляции	2,52 мм	6,15 мм
Диаметр наружной оболочки	4,62 мм	10,3 мм
Радиус изгиба	5 см	25 см
Затухание (на частоте 10 МГц)	4,6 дБ/100 м	1,7 дБ/100 м

Как видно на рис. 8.2, типичная сеть с тонким коаксиальным кабелем или шиной состоит из сетевых хостов, или устройств, линейно объединенных кабелем RG-58. Каждое устройство подключено к кабельной сети Т-образным BNC-коннектором. Т-коннектор, по существу, содержит три точки соединения типа BNC: одна подключает к самому устройству, а две другие служат для прокладки входящего и исходящего кабеля RG-58 к следующему устройству на шине. На обоих концах кабельной шины должны быть установлены нагрузочные резисторы, которые поддерживают уровень сигнала и ограничивают помехи и искажение сигнала.

Сеть с толстым коаксиальным кабелем или 10Base5 Ethernet лучше приспособлена для сетевых магистралей, пролегающих между устройствами сети, и для условий с высокими спектральными помехами. Благодаря относительно низкой величине затухания, равной 1,7 дБ на 100 м, и значительно более толстой изоляции 10Base5 способна передавать данные со скоростью 10 Мбит/с на расстояние до 500 м — до того как уровень сигнала станет ниже приемлемого уровня. Хотя толстый коаксиальный кабель может использоваться для соединения сетевых хостов, в большинстве случаев рекомендуется этого не делать. В качестве аргументов приводится относительно небольшой радиус изгиба (затрудняющий операции с самим кабелем), а также необходимость в применении громоздких пронзающих ответвителей и ответвительных кабелей, которые менее практичны, чем Т BNC-коннекторы.

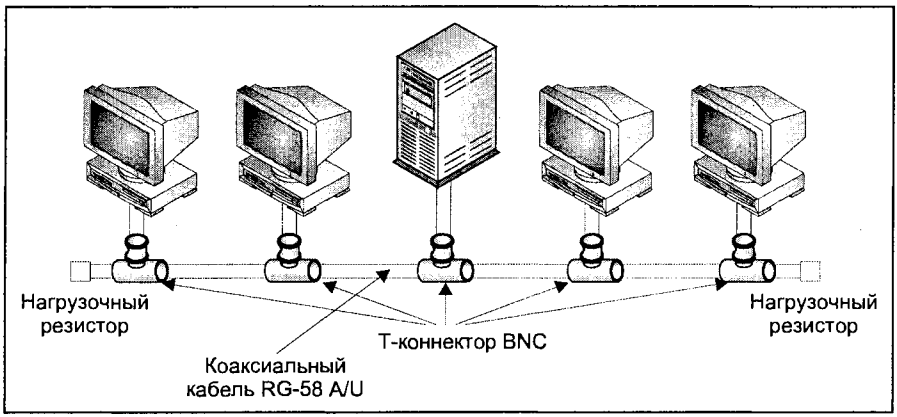


Рис. 8.2. Типичная сеть с тонким коаксиальным кабелем

Анализ коаксиальных кабелей

С появлением витой пары и оптоволокна, а также недорогих концентраторов и коммутаторов для Ethernet, распространенность сетей на базе коаксиальных кабелей уменьшилась. Хотя тонкий и толстый коаксиальные кабели используются редко, средства и материалы для развертывания и обслуживания сетей на их основе все еще широко доступны. Впрочем, прежде чем принимать решение об организации такой сети, необходимо рассмотреть несколько вопросов, связанных со стоимостью и типом применяемого кабеля, топологией сети, установкой и надежностью.

Стоимость и тип кабеля

Когда-то коаксиальный кабель стоил значительно меньше витой пары, теперь же различие между стоимостью этих двух типов кабелей минимально. Помимо этого есть еще несколько причин предпочтительного использования коаксиального кабеля по сравнению с витой парой. Если сеть будет работать в условиях сильного электромагнитного излучения или обладать значительной протяженностью, лучше остановить свой выбор на коаксиальном кабеле — если, конечно, пропускную способность в сети можно ограничить уровнем в 10 Мбит/с. При более высоких требованиях относительно пропускной способности лучше отдать предпочтение многомодовому оптоволоконному кабелю, т. к. его максимальная протяженность значительна, а к электромагнитному излучению он практически невосприимчив.

Если ограничения по пропускной способности коаксиального кабеля для вас приемлемы, выбор между RG-58 и RG-8A/U в значительной степени обусловливается двумя ключевыми факторами: дальностью и спектральными помехами. Если общая протяженность сети не превышает 185 м, имеет смысл выбрать кабель RG-58 — при условии, что он сможет обеспечить достаточное экранирование от любых источников электромагнитного излучения.

Впрочем, если общая протяженность превысит 185 м, но не достигнет или будет равной 500 м (или в случае необходимости более надежной защиты от электромагнитного излучения), рекомендуется остановиться на варианте RG-8A/U. Монтаж

толстого коаксиального кабеля может оказаться крайне утомительным занятием, но он предусматривает более аккуратный и радующий глаз способ установки — при условии использования ответвительных кабелей от магистрали, скрытых в стене или потолке.

Наконец, если прокладка будет осуществляться через пространство пленума[1], при монтаже необходимо воспользоваться кабелем типа пленум. Такой кабель стоит дороже, но зато в случае его возгорания токсических испарений будет намного меньше. Увеличение стоимости связано с различиями в применяемых материалах оболочки — или, в большинстве случаев, с использованием тефлона вместо поливинилхлорида.

Топология и коллизионные домены

Тонкий и толстый коаксиальные кабели проектировались в расчете на применение в рамках шинной топологии (в противоположность топологии типа "Звезда"); по этой причине все устройства, или хосты, соединяются линейным способом. В сети такого типа время от времени возникают трудности, связанные с установкой, особенно в том случае, если одно устройство расположено на значительном расстоянии от следующего.

Кроме того, эта топология не достаточно хорошо приспособлена к созданию множества коллизионных доменов; следовательно, в случае возникновения конфликтов, наличие слишком большого количества устройств или устройств с высоким уровнем использования сети может сильно снизить производительность сети. Если число коллизий велико, одним из способов создания еще одного коллизионного домена является соединение двух автономных коаксиальных сетей Ethernet с помощью устройства маршрутизации или моста.

Анализ установки

Чтобы обеспечить безотказный ввод в действие сети на основе коаксиальных кабелей, учитывайте следующие аспекты установки при ее планировании или реорганизации.

- Несмотря на то, что коаксиальный кабель защищен, все-таки имеет смысл воздержаться от прокладки сегментов кабеля неподалеку от электромоторов или балластных сопротивлений флуоресцентных ламп; в противном случае вероятность возникновения проблем, связанных с помехами, возрастает.
- Всегда помните и не выходите за пределы ограничений по дальности 10Base2 (185 м) и 10Base5 (500 м). Помимо фактической протяженности кабеля разумно прибавлять к его общей длине по 6 футов (1,83 м) на каждую рассечку (т. е. Т-коннектор или цилиндрический коннектор).
- Если для рассматриваемой сети необходима протяженность, превышающая разрешенную, в ней можно установить до четырех Ethernet-повторителей. Если одна из дальних рабочих станций будет испытывать трудности, попробуйте сократить количество повторителей между ней и сервером до двух.

---

[1] Пространство между перекрытием и фальшь-потолком. — *Ред.*

- Чтобы обеспечить достаточный уровень сигнала на всем протяжении сети, не следует превышать лимит в 30 Т-коннекторов в одном сегменте сети. Более того, расстояние между Т-коннекторами должно составлять по меньшей мере 4 фута (1,22 м). Не забывайте терминировать каждый конец сети нагрузочным резистором в 50 Ом (один из этих двух резисторов должен быть заземлен).
- Если для установки требуется монтаж 10Base5 с участием удобного в использовании кабеля 10Base2, рекомендуется применение системы ответвления тонкого коаксиального кабеля таких производителей как, например, AMP.

Надежность

При использовании в подходящих условиях сети на основе коаксиальных кабелей способны обеспечить многие годы бесперебойной, экономически эффективной работы. Впрочем, относительно простая конструкция шинной сети имеет свои недостатки, самым значительным из которых является существование единственной точки отказа. Это лучше всего сравнить с тем, как работают гирлянды, которые мы используем для украшения по праздникам: если неисправность возникнет в одной отдельно взятой части шины, в итоге из строя выйдет вся сеть.

Чтобы предупредить подобные происшествия, убедитесь в том, что все кабельные разъемы плотно обжаты (но не накручены) и что присутствует хороший контакт заземляющего металлического провода с оплеткой. Кроме того, не забывайте, что на обоих концах шины должны присутствовать плотно подсоединенные нагрузочные резисторы. Наконец, обеспечьте защиту всех компонентов кабельной инфраструктуры; сделайте так, чтобы на них никто не мог наступить или об них споткнуться.

Выявление повреждений коаксиального кабеля

В сетях с тонким и толстым коаксиальным кабелем обычно отсутствуют активные компоненты наподобие концентраторов и коммутаторов; впрочем, вполне возможно, что в них располагаются элементы, которые могут выйти из строя и стать источниками неполадок в сети. В их числе — нагрузочные резисторы, Т-образные BNC-коннекторы и BNC-коннекторы, сетевые адаптеры и даже сам кабель. К счастью, при работе с сетью на основе коаксиального кабеля выявление и починка вышедшего из строя компонента не представляет серьезной проблемы. Элементарными методами, применяемыми с этой целью, являются измерение сопротивления и напряжения.

Измерение сопротивления

Процедура измерения сопротивления заключается в том, чтобы обнаружить нарушенный сегмент кабеля или неисправный коннектор. Чтобы протестировать уровень сопротивления во всей сети, для начала необходимо выключить питание всех расположенных в ней устройств. Затем с помощью стандартного ампервольтметра или омметра измеряется уровень сопротивления на любом Т-коннекторе; для этого концы измерителя прикладываются к медному проводу и коаксиальной защите (т. е. к внешней части коннектора). В обычной сети 10Base2 или 10Base5 при наличии обоих нагрузочных резисторов измеритель должен показывать примерно 27 Ом (±5 Ом). Если в сети присутствует лишь один нагрузочный резистор, уровень сопротивления

должен вырасти примерно до 55 Ом (±10 Ом); в случае отсутствия обоих нагрузочных резисторов уровень сопротивления может расти до бесконечности. Указанные уровни сопротивления свидетельствуют об исправности кабеля и коннекторов.

Для того чтобы выявить неисправный сегмент кабеля и/или коннектор, нужно снять нагрузочный резистор с одного конца сети и проверить уровень сопротивления именно на этом конце, причем снятый резистор следует использовать далее для выделения из сети все более мелких сегментов. К примеру, после отсоединения от сети одной стороны Т-коннектора (самой дальней от неограниченного конца) и помещения на ее место нагрузочного резистора измеритель должен показывать уровень сопротивления в 55 Ом; если это так, вы будете знать, что все сегменты кабеля и коннекторы между ампервольтметром и местом текущего расположения нагрузочного резистора исправны. Значительно более высокий уровень сопротивления указывает на наличие проблем на сегменте кабеля между этими двумя пунктами; их можно изолировать еще больше, переместив нагрузочный резистор к Т-коннектору, расположенному ближе к ампервольтметру, — по одному сегменту за раз.

Очень часто сегмент кабеля отказывается работать из-за плохо подсоединенного BNC-коннектора, а не по причине выхода из строя самого кабеля. Если дело обстоит именно так, то проблема быстро решается путем урезания концов кабеля и установки новых обжимных BNC-коннекторов.

Примечание

Тестирование сетей 10Base5 необходимо проводить с пронзающих ответвителей, поскольку в таких сетях Т-коннекторы, как правило, отсутствуют.

Измерение напряжения

Этот метод проверки сети 10Base5 может помочь обнаружить потенциально неисправные модули доступа к среде (Medium Access Units, MAU). Кроме того, с его помощью можно определить наличие паразитного контура с замыканием через землю, причина возникновения которого может заключаться в наличии в сети нескольких точек заземления. При тестировании на любом пронзающем ответвителе с помощью вольтметра нормальный уровень напряжения в сети 10Base5 не должен превышать ±100 мВ. Если установленный уровень напряжения значительно превышает ±100 мВ, вполне возможно, что в сети присутствует короткое замыкание.

Чтобы обнаружить короткое замыкание, начните отсоединять по одному модулю от соответствующих пронзающих ответвителей; делайте это до тех пор, пока уровень напряжения не спадет до приемлемого. Если после отсоединения всех модулей вольтметр будет продолжать фиксировать значение, превышающее ±100 мВ, проверьте кабельный участок на наличие добавочного заземления: паразитный контур с замыканием через землю может привести и к повышению напряжения.

Сложные средства тестирования

Методы измерения сопротивления и напряжения могут помочь в обнаружении простых проблем, связанных с коаксиальным кабелем, но для того, чтобы с их помощью исправить ошибку в крупной сетевой среде, нужно потратить много времени. В целях ускорения процесса обнаружения сетевых неисправностей применяют

сложные устройства проверки кабелей, которые могут автоматически тестировать и идентифицировать любую присутствующую или потенциальную неисправность.

Эти устройства называются *динамическими рефлектометрами* (Time Domain Reflectometer, TDR). Средства диагностики, к которым относится динамический рефлектометр, работают примерно так же, как радар или сонар: они просто отсылают по сетевому кабелю сигнал, а затем измеряют время, необходимое определенному устройству для его отражения. После этого динамический рефлектометр оценивает интенсивность отраженного сигнала и пройденное им расстояние, чтобы выявить и диагностировать неисправность сети. Некоторые сложные кабельные тестеры способны оценить сеть с точки зрения уровня передачи данных и выявить проблемы производительности типа высокой частоты коллизий или искаженности кадров Ethernet.

Симптомы неисправностей

Симптом 8.1. Периодически пропадает соединение

Причин возникновения периодической потери соединения очень много, но самые распространенные из них связаны с неисправностью физических соединений. Среди таких причин — наличие неисправных или плохо прикрепленных BNC- или T-коннекторов, а также отказ нагрузочных резисторов или нахождение их в неприкрепленном состоянии. Во многих случаях выявить неисправный сегмент или плохо прикрепленный коннектор помогает мониторинг уровней сопротивления в сочетании с проверкой отдельных кабельных соединений.

Симптом 8.2. Отказал целый кабельный сегмент

Если из строя вышел целый сегмент, проблема, вероятно, заключается в самом кабеле. Такие проблемы обычно заявляют о себе в виде паразитных контуров с замыканием через землю или коротких замыканий в инфраструктуре кабеля; тем не менее нельзя исключать и возможность плохо укрепленных соединений и неисправных резисторов.

Симптом 8.3. Вы обнаружили необычайно высокое число коллизий

В сетях Ethernet коллизии являются обычным явлением — особенно в процессе увеличения размера сети и добавления в нее новых хостов и устройств. Коллизии в необычно больших количествах, как правило, возникают из-за обильных повторных передач, осуществляемых устройствами сети. В основном, повторные передачи происходят в результате искажения кадров или пакетов, а эти явления, в свою очередь, могут быть следствием отражений сигналов в кабеле из-за недостаточного нагрузочного сопротивления. Обязательно проверьте подключение обоих нагрузочных резисторов и обеспечение ими достаточного сопротивления в шине. Если при нормальном уровне сопротивления коллизии сохраняются, рекомендуется создать новый сегмент Ethernet, чтобы разделить передающие устройства на более мелкие коллизионные домены.

Симптом 8.4. Ошибки контрольной суммы кадра возникают часто или периодически

Хотя коллизии и фрагментированные пакеты в рамках Ethernet вполне обычны, чрезмерное или перемежающееся число их возникновений может указывать на

наличие помех. Учитывая, что измеренная величина нагрузочного сопротивления равняется приблизительно 27 Ом, источником помех, вероятнее всего, является электромотор, копировальный аппарат или балластное сопротивление флуоресцентной лампы. Проверьте, нет ли рядом с кабелем потенциальных источников электромагнитного излучения, и, если возможно, проложите кабель по-другому. Кроме того, убедитесь в том, что все сетевые устройства подсоединены к источнику переменного тока через какое-либо устройство, выполняющее фильтрацию помех в линии передачи: такие устройства зачастую оказываются способны значительно ограничить возможное наведение электрических шумов.

Симптом 8.5. После установки новой рабочей станции соединение отсутствует или характеризуется прерывистостью

Изменение состояния соединения существующих сетевых устройств после установки нового устройства или рабочей станции указывает на то, что один из компонентов новой сборки (кабель, коннекторы, сетевой адаптер и т. д.) является причиной возникновения ошибки в кабельной шине. Эти компоненты следует проверить, а при необходимости — заменить. С другой стороны, если существующая сеть работает вполне нормально, а новая рабочая станция не может установить соединение, вероятно, винить в этом следует ошибку конфигурации. Проверьте сетевой адаптер и конфигурацию новой рабочей станции. Распространенной ошибкой, допускаемой при конфигурации рабочей станции, является указание неверного для данной сети типа кадров: прежде чем менять сетевой адаптер, нужно убедиться в том, что подобная ошибка не была допущена и вами.

Витая пара

Коаксиальный кабель является прекрасным решением для недорогих сборок, небольших сетей и сетей, находящихся в среде со спектральными помехами. В то же время кабель типа витой пары намного более универсален и расширяем, а выполнять его монтаж и обслуживание значительно проще. Витая пара состоит из восьми по отдельности изолированных медных проводов, сгруппированных в четыре сплетенных комплекта пар, промаркированных различными цветами. Скручивание каждой пары в кабеле создает эффективную защиту, которая предотвращает появление перекрестных помех между парами и является эффективным средством защиты от помех низкого уровня. Кроме того, чтобы еще с большей степенью надежности предупредить появление помех между парами в кабеле, каждая из них характеризуется различным количеством витков на фут. В целях физической защиты от условий окружающей среды четыре комплекта пар помещаются в наружную оболочку, изготовленную либо из поливинилхлорида, либо из тефлона (в случае с пленумным кабелем).

Витая пара производится под разные уровни сертификации; они называются категориями и маркируются цифрами от 1 до 7. Чем выше категория, тем больше витков на фут присутствует в каждой паре. Повышенное количество витков обеспечивает более высокие скорости передачи данных, т. к. в пары проникает меньше помех; таким образом, чем скоростнее сеть, тем выше категория кабеля, который в ней требуется установить. В табл. 8.3 приводятся общедоступные категории витой пары с указанием типичных вариантов их использования и максимальной полезной протяженности.

Примечание

Аксессуары, необходимые для монтажа кабеля, типа разъемов и коммутационных панелей, маркируются в соответствии с аналогичными стандартами категорий; следовательно, при выборе этих деталей следует руководствоваться их категориями, которые должны соответствовать категории кабеля.

Таблица 8.3. *Основные категории витой пары*

Тип витой пары	Типичный вариант применения	Максимальная протяженность
Категория 2	Голос	Нет данных
Категория 3	Ethernet по спецификации 10BaseT и голос	100 м (на частоте 16 МГц)
Категория 5	Ethernet по спецификации 100BaseT	100 м (на частоте 100 МГц)
Категория 5e	Ethernet по спецификациям 100BaseT и 1000BaseT (минимальный уровень поддержки)	100 м (на частоте 100 МГц)
Категория 6	Ethernet по спецификации 1000BaseT	100 м (на частоте 250 МГц)
Категория 7	Ethernet по спецификации 1000BaseT	100 м (на частоте 600 МГц)

Неэкранированная витая пара

Витая пара существует в двух основных разновидностях, первая из которых — широко распространенная *неэкранированная* витая пара (Unshielded Twisted Pair, UTP), которая применяется в сетях 10BaseT, 100BaseT и даже 1000BaseT. "Неэкранированной" она называется потому, что ее пары не окружены металлической защитой и зависят от магнитного поля, создаваемого около витых пар (в большинстве типов среды этот вариант работает).

При использовании неэкранированной витой пары для организации сети Ethernet каждый из восьми проводов этих пар нужно обжать в восьмипозиционном (четырехпарном) модульном коннекторе RJ-45, показанном на рис. 8.3. Он напоминает более компактный двухпарный коннектор RJ-11, используемый в большинстве аналоговых телефонов, причем производится только в форме обжимного коннектора, поэтому для закрепления этого коннектора на кабеле необходимы специальные инструменты, которые, правда, широко доступны. Каждый провод должен быть вставлен в коннектор на обоих концах кабеля в порядке, определяемом стандартом 568B Ассоциации электронной промышленности/Ассоциации телекоммуникационной промышленности (Electronic Industry Association/Telecommunications Industry Association, EIA/TIA); этот порядок приводится в табл. 8.4. Выводы коннектора нумеруются слева направо при направлении его кабельного конца в противоположную сторону, а пластиковой лапки — вверх. Применение одинакового порядка на обоих концах кабеля приводит к тому, что формируется так называемый *проходной кабель*, который используется для подключения хоста или устройства к концентратору или коммутатору Ethernet. Если применить обратный порядок для передающей и прини-

мающий пар, получится *перекрестный кабель* или *кроссовер* (crossover), позволяющий двум хостам или устройствам обмениваться информацией напрямую, не используя концентратор или коммутатор Ethernet.

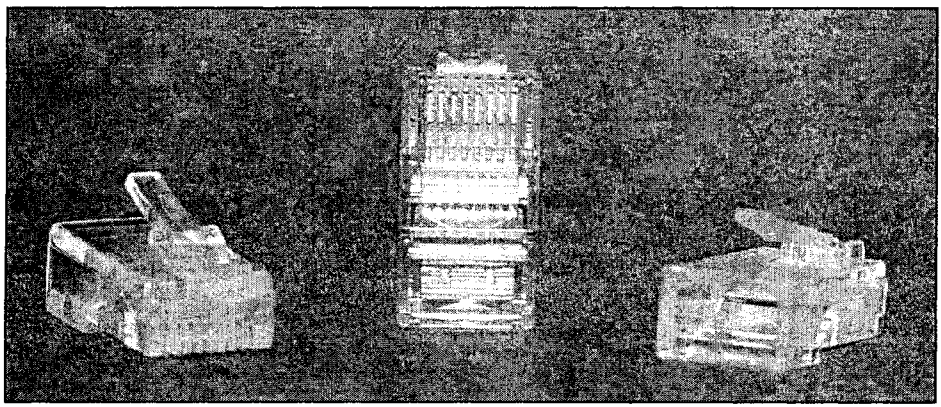


Рис. 8.3. Модульный коннектор RJ-45 для использования с витой парой

Таблица 8.4. *Назначения выводов разъема RJ-45 в соответствии со стандартом 568B EIA/TIA*

Номер вывода	Назначение (прямое соединение)	Цвет проводника прямого соединения	Цвет проводника кроссовера
1	Передача данных (+)	Бело-оранжевый	Бело-зеленый
2	Передача данных (–)	Оранжевый	Зеленый
3	Прием данных (+)	Бело-зеленый	Бело-оранжевый
4	В 10BaseT не используется	Синий	Синий
5	В 10BaseT не используется	Бело-синий	Бело-синий
6	Прием данных (–)	Зеленый	Оранжевый
7	В 10BaseT не используется	Бело-коричневый	Бело-коричневый
8	В 10BaseT не используется	Коричневый	Коричневый

Одним из многочисленных преимуществ витой пары является простота монтажа и обслуживания для каждого узла в отдельности; таким образом, добавление в сеть или удаление новой рабочей станции или неисправного сегмента кабеля не оказывает воздействия на другие узлы сети. Это заслуга звездообразной топологии (в противоположность шинной), применяемой в сетях на основе витой пары, где каждый узел имеет собственное соединение с объединяющим устройством: коммутатором или концентратором Ethernet.

Как правило, витая пара монтируется по фрагментной системе, т. е. между рабочей станцией, с одной стороны, и концентратором или коммутатором, с другой, не про-

кладывается прямой (цельный) кабель. Напротив, каждая рабочая станция располагает коротким соединительным кабелем (patch), который подключает ее сетевой адаптер к ближайшему разъему RJ-45. Этот разъем жестко соединен (либо врезан, либо смонтирован) через более длинный кабель с центральной соединительной панелью RJ-45, которая представляет собой большое количество разъемов RJ-45 на одной панели. Отходящий от этой наборной панели короткий коммутационный шнур (patch cord) связывает отдельный разъем с портом коммутатора или концентратора. Такая система позволяет выполнять в офисах предварительную проводку и запускать отдельные линии по мере появления необходимости. Кроме того, она значительно улучшает обслуживание кабеля и поиск повреждений в нем.

Хотя неэкранированная витая пара довольно устойчива к отказам, самодельные кабели нередко выходят из строя из-за плохого соединения между проводниками и разъемом RJ-45. Чтобы уменьшить вероятность таких случаев, а также сэкономить некоторое время на монтаже, есть смысл заказать готовые, автоматически обжатые соединительные кабели. Многие компании, занимающиеся электрикой, могут изготовить такие кабели любой длины (и цвета).

Примечание

Для витой пары обычно предлагаются провода двух типов: многожильные и одножильные. Витая пара с одножильным проводом обычно используется для прокладки кабеля между коммутационными панелями и гнездами (в стенах), а многожильные провода, как правило, применяются в кабелях, соединяющих гнезда с сетевыми адаптерами, т. к. степень их гибкости немного выше. Каждый из этих типов витой пары подойдет для любого применения при условии, что коннекторы и разъемы соответствуют типу используемого провода. При их несоответствии, которое определяется с помощью кабельного сканера, может возникнуть расщепление пар или короткое замыкание.

Экранированная витая пара

Несмотря на то, что неэкранированная витая пара устойчива к низким уровням внешних помех, есть среды с настолько сильными спектральными помехами, что для нормального функционирования сети в них необходима дополнительная защита. В подобных условиях довольно практична вторая разновидность витой пары, которая называется *экранированной*. Благодаря нескольким слоям металлической защиты внутри кабеля экранированная витая пара (Shielded Twisted Pair, STP) допускает функционирование в средах с интенсивными помехами без потерь в скорости и максимальной протяженности.

Так как конструкция, цветовое кодирование и коннекторы экранированной витой пары почти идентичны неэкранированной, экранированная витая пара подчиняется тем же промышленным стандартам и может применяться во всех средах Ethernet без каких-либо изменений. В неэкранированной витой паре защита обеспечивается электромагнитными полями, а в экранированной витой паре устойчивость к помехам усилена за счет экранирования каждой пары алюминиевой (или аналогичной) оболочкой, причем в некоторых случаях поверх всех индивидуально защищенных пар помещается оболочка из металлического провода с оплеткой, затем весь кабель защищается оболочкой из поливинилхлорида или тефлона.

Примечание

Из-за дополнительной защиты, реализуемой в экранированной витой паре, с этим типом кабеля работать несколько труднее, чем с неэкранированной витой парой, поскольку он не очень эластичен и не так хорошо гнется. Кроме того, необходимо убедиться в заземлении обоих концов экранированной витой пары, т. к. неправильное заземление может привести к появлению шумов.

Выявление повреждений витой пары

В отличие от коаксиального кабеля выявление повреждений витой пары не представляет большой трудности, отчасти благодаря типичной для нее звездообразной топологии. В сущности, если плохо работает вся сеть, вполне вероятно, что виноват в этом концентратор или коммутатор. Если же проблемы появляются на отдельно взятом хосте, скорее всего, их источник расположен где-то между самим хостом и его портом на коммутаторе или концентраторе — особенно в случае, если нет постоянного сигнала индикатора соединения на сетевом адаптере или в порту концентратора. К счастью, существуют некоторые довольно недорогие инструменты (например, кабельные сканеры), облегчающие выявление повреждений витой пары. Для более тщательного тестирования есть устройства типа динамического рефлектометра, предназначенные для сетей на основе витой пары; их стоимость в зависимости от выполняемых функций колеблется в диапазоне от $400 до $10 000.

Подобно коаксиальному кабелю многие проблемы с витой парой начинаются с коннекторов и/или разъемов, которыми ограничиваются линии неэкранированной витой пары. Сплошное тестирование кабеля лучше всего проводить, вооружившись недорогим кабельным сканером. Такие устройства продаются в виде комплектов, состоящих из двух частей. Одна часть — это сам сканер, или тестер проверки целостности, который подключается к одному концу кабеля. Другая часть — это обратный коннектор, который по внешнему виду напоминает мини-разъем RJ-45, а подключается к противоположному концу кабеля.

После соединения обоих концов выполняется краткий тест (сканирование) кабеля, и через несколько мгновений на дисплее сканера появляется информация о том, какой провод или пара закорочена, расщеплена или переставлена. К сожалению, большинство сканеров не умеет определять коннектор, в области которого локализуется проблема; поэтому необходимо снять (срезать) оба коннектора, а на их место поставить новые коннекторы RJ-45. Если сканер не сможет выявить неисправности, пошевелите кабель с каждого конца, чтобы вставить его в коннектор: дело в том, что один из проводов может быть не полностью установлен в выводе коннектора. Плохо укрепленные коннекторы всегда следует заменять, поскольку, даже если кабель пройдет испытания, в ближайшем будущем он, возможно, выйдет из строя.

Если после нескольких попыток обжать кабель в новые коннекторы ошибка будет повторяться, вполне возможно, что многожильные провода обжаты в одножильные коннекторы или наоборот. Чтобы избавиться от этой проблемы, убедитесь в том, что тип кабельного провода и тип коннектора совпадают.

Динамические рефлектометры и расширенные границы кабеля

Несмотря на то, что большинство неисправностей неэкранированной и экранированной витой пары связано с коннекторами, иногда проблемы обнаруживаются и в

самой витой паре — особенно если кабель подвергся необычно сильной физической нагрузке. Более того, некоторые неисправности кабеля не всегда материализуются, как, например, в случае перекрестных наводок вблизи концов кабеля (Near End Cross Talk, NEXT), которые представляют собой утечку сигнала от одной пары к другой. "Перекрестными" они называются потому, что могут произойти в разъеме RJ-45 на любом из концов кабеля, где пары расплетаются для обжима.

Распространенный метод выявления физических неисправностей кабеля такого типа предполагает использование в сетях на основе неэкранированной и экранированной витой пары динамического рефлектометра. Динамический рефлектометр передает сигнал по кабелю, а затем оценивает время возвращения отраженного сигнала и полученный уровень мощности. С помощью анализа этих факторов динамический рефлектометр может точно определить место возникновения физической неисправности внутри кабеля. Некоторые современные кабельные сканеры выполняют функции динамического рефлектометра по диагностике и выявлению физических неисправностей кабеля. Одним из подобных устройств является MicroScanner производства компании Fluke Networks; его цена составляет примерно $400.

Сложные анализаторы кабеля

При управлении или сопровождении крупной инфраструктуры на базе неэкранированной или экранированной витой пары сложные анализаторы кабеля могут помочь обеспечить максимально эффективную работу оборудования кабельной линии. Устройства типа серии Fluke DSP-4000 цифровых кабельных анализаторов, как правило, сочетают функции сложного анализатора кабеля и цифровых инструментов тестирования. Такое сочетание функций позволяет анализатору не только диагностировать и локализовать физические неисправности кабеля, но и обнаружить снижающие производительность факторы, такие как перекрестные наводки на концах кабеля, наведенные помехи или шум и даже общие проблемы передачи в Ethernet типа высокого уровня коллизий или многочисленных ошибок.

Перекрестные наводки NEXT, как правило, вызваны расплетенными парами в кабеле или на коммутационной панели. При обжиме кабеля или монтаже на коммутационной панели нельзя расплетать пары более чем на полдюйма (1,27 см). Раскручивание на большую длину приведет к помехам между передающим и принимающим сигналами в данной паре. Высокий уровень перекрестных наводок, кроме того, может быть вызван плохим качеством кабеля или коммутационных панелей.

Если анализатор указывает на чрезмерные коллизии в сети, скорее всего, что-то мешает передаче пакетов или кадров; иногда это можно отнести на счет высокого уровня электромагнитного излучения. Если дело обстоит именно так, убедитесь в том, что все кабельные линии находятся на достаточном расстоянии от любых источников электромагнитного излучения, и переместите те из них, которые наводят помехи. Если помехи в сети будут по-прежнему продолжаться, разумно заменить все подозрительные участки кабеля на экранированную витую пару.

Также источником чрезмерных коллизий может быть высокий уровень затухания. В Ethernet допускается потеря сигнала в 11,5 дБ, и проблемы возникают при превышении этого уровня; таким образом, если неисправность кабеля приводит к дополнительной потере сигнала, результатом будет появление понижающих производительность ошибок: контрольной последовательности кадра и коллизий.

Симптомы неисправностей

Симптом 8.6. Производительность сети понижена

Понижение производительности в масштабах всей сети может быть результатом большого количества коллизий, ошибок контрольной последовательности кадра и даже высокой степени использования сети. Важно отметить, что увеличение коллизий и повышение уровня использования сети может быть вызвано наличием в данном сегменте кабеля слишком большого количества хостов. Если дело обстоит именно так, возможно, вам стоит перейти с совместной на коммутируемую инфраструктуру Ethernet и при необходимости создать несколько коллизионных доменов, выполнив сегментирование концентратора или коммутатора или организовав виртуальные локальные сети (Virtual Local Area Network, VLAN).

Ошибки контрольной последовательности кадра могут происходить из-за помех внутри сети, связанных с перекрестными наводками или с электромагнитным излучением. Тестирование кабеля посредством сложного анализатора, скорее всего, поможет осуществить точную диагностику проблем, приводящих к появлению помех; в то же время даже поверхностный зрительный осмотр кабельного сегмента на предмет близлежащих источников электромагнитного излучения будет менее дорогостоящим способом решения проблемы. Среди известных источников электромагнитного излучения фигурируют копировальные аппараты, балластное сопротивление ламп, а также любые устройства с электромоторами. Помимо этого, все сетевые устройства, включая коммутаторы и концентраторы, должны быть подключены к сети переменного тока через сетевые фильтры — было замечено, что поступление электромагнитного шума может происходить через линии переменного тока.

Наконец, всегда необходимо обеспечивать однородность классов и типов кабеля в рамках всей сети: все кабели и нагрузочные устройства должны относиться к одной и той же категории сертификации и быть выбраны в соответствии с типом провода: одножильным или многожильным. Более того, всегда следует придерживаться номинальной максимальной протяженности, равной 100 м.

Симптом 8.7. Фиксируется большое количество коллизий или фрагментированных пакетов

Подобно симптому 8.6, большое количество коллизий может указывать на перегрузку сети. Если дело именно в этом, попытайтесь перейти к коммутируемой инфраструктуре или хотя бы переместить несколько рабочих станций в другой совместный сегмент Ethernet. Кроме того, имеет смысл прибегнуть к услугам сетевого анализатора или сходного устройства, которое позволит установить, не является ли причиной высокого уровня использования сети большой объем широковещательных сообщений или же широковещательный шторм, в результате которого коллизии происходят слишком часто. С другой стороны, если проблема заключается в большом количестве сверхкоротких кадров, виной тому могут быть помехи, влияющие на передачу.

Симптом 8.8. При установке новой рабочей станции соединение отсутствует или является неустойчивым

Неисправности с соединением новой рабочей станции можно отнести на счет повреждения кабельной линии, неисправности сетевого адаптера или неточной конфигурации этой станции. Периодически появляющиеся неисправности, как

фигурации этой станции. Периодически появляющиеся неисправности, как правило, являются следствием неплотного контакта в пределах кабельной линии или короткого замыкания в коннекторе из-за неправильно установленного провода. Убедитесь в том, что применяемые коннекторы соответствуют типу провода (многожильного или простого), и обожмите новые коннекторы, чтобы устранить периодические замыкания или слабую установку провода внутри самих коннекторов.

Кроме того, убедитесь, что используется кабель прямого соединения, а не перекрестного. Если рабочая станция или концентратор указывают, что соединение с кабелем в порядке, проверьте, нет ли ошибок в самой конфигурации новой рабочей станции.

Симптом 8.9. Рабочая станция полностью выходит из строя

Если связь рабочей станции с концентратором или коммутатором после успешной установки соединения пропадет, вероятнее всего, причиной этого будет являться физическая неисправность кабеля. Проведите визуальный осмотр кабельной линии на предмет повреждений или разрывов. Если никаких видимых признаков износа выявить не удастся, скорее всего, дело в неплотном креплении коннектора, и его следует заменить. Наконец, следует убедиться в отсутствии неисправностей порта коммутатора или концентратора. Сделать это можно, переставив неработающую кабельную линию в новый порт коммутатора или концентратора и проверив индикатор соединения.

Примечание

Известно, что электростатический разряд (Electrostatic Discharge, ESD) может привести к неисправности отдельных портов коммутатора и сетевого адаптера. Следовательно, прежде чем работать с кабелем, обязательно заземлите себя, прикоснувшись к открытому куску металла. Электростатический разряд может проходить и по соединенному кабелю, таким образом повреждая соединенный порт.

Оптический кабель

Хотя витая пара и коаксиальный кабель являются экономически эффективными средствами передачи и приема данных, но и тот и другой ограничены потенциальными помехами, а также малыми пределами дальности. Волоконно-оптический кабель — не самая дешевая разновидность кабеля — в дополнение ко всем вышеперечисленным возможностям обладает еще несколькими. Так как в волоконно-оптическом кабеле для передачи данных используются фотоны, такие кабели невосприимчивы к электромагнитному излучению и способны передавать сигналы на расстояния значительно большие, чем те, которые подвластны коаксиальному кабелю 10Base5. Во многом подобно витой паре, одна пара в которой предназначена для передачи, а другая — для приема, в волоконно-оптическом кабеле для передачи и приема фотонов должны использоваться два отдельных кабеля (хотя оба кабеля могут находиться в одной оболочке).

Волоконно-оптический (Fiber-Optic, FO) кабель состоит из длинной, тонкой стеклянной нити из кремния (для небольших расстояний используется полимер), которая называется *стержнем*. Он окружен отражающим стеклянным покрытием (похо-

жим на зеркало), которое называется *оболочкой*. Когда световые фотоны пытаются выйти за пределы стержня, оболочка отражает их, возвращая обратно. Оболочку окружает защитный пластик, а в некоторых случаях — дополнительный усиливающий материал типа кевлара. Аналогично витой паре и коаксиальному кабелю для внешней защиты применяется оболочка из поливинилхлорида или тефлона.

Типы волоконно-оптического кабеля

Когда лазер или светодиод передает свет по волоконно-оптическому кабелю, фотоны перемещаются по стеклу, отскакивая от зеркальной оболочки, окружающей стекловолоконную сердцевину. Так как оболочка и стержень не поглощают свет (или делают это в минимальных количествах), передаваемые сигналы могут проходить расстояния в несколько тысяч километров. Максимальная скорость и дальность передаваемого по оптоволоконному кабелю света зависят от того, насколько часто он отражается в стержне. Поэтому диаметр стержня оптоволоконного кабеля может быть различным — минимальный диаметр предназначен для более длинных и менее частых отражений, таким образом позволяя передавать свет на максимальные расстояния. Есть два основных типа волоконно-оптического кабеля: одномодовый и многомодовый; у каждого из них есть определенный набор свойств и способов применения.

Многомодовое волокно

При использовании волоконно-оптического кабеля в условиях локальной сети или предприятия чаще всего предпочтение отдают многомодовому волокну. Такая ситуация складывается благодаря меньшей стоимости кабеля ближней связи и оптоволоконного оборудования. Многомодовое волокно состоит из относительно крупного стержня, диаметр которого обычно составляет от 50 до 80 мк; следовательно, отражение фотонов происходит чаще, чем если бы стержень был меньше или уже. В многомодовом оптическом оборудовании для синтезирования фотонов используется не лазер, а светодиоды, которые генерируют инфракрасное излучение. Это различие в передающем оборудовании приводит к значительному снижению стоимости.

Существуют две формы многомодового волокна, которые различаются по ступенчатому или градиентному переходу между стержнем и оболочкой. Многомодовый кабель со ступенчатым показателем преломления (step-index multimode cable) характеризуется повышенным преломлением по сравнению с многомодовым кабелем с градиентным показателем преломления (gradual-index multimode cable); происходит это из-за дискретного изменения показателя преломления на границе между стержнем и оболочкой. Чем ниже уровень преломления, тем быстрее могут двигаться фотоны. Поэтому многомодовый кабель со ступенчатым показателем преломления не позволяет развивать скорость более 50 Мбит/с, в то время как многомодовый кабель с градиентным показателем преломления обеспечивает скорость до 1 Гбит/с. Последний чаще применяется в локальных сетях и в кампусных сетях ближней связи.

Тем не менее в многомодовом кабеле с градиентным показателем преломления преломление порождает различные пути прохода фотонов по кабелю — это явление называется многомодовым искажением. Фотоны, которые двигаются в сторону внешней части кабеля, перемещаются быстрее тех, которые находятся в сердцевине;

таким образом, одни фотоны достигают пункта назначения быстрее, чем другие. На небольших расстояниях (<2 км) это не создает проблемы, т. к. обычно все фотоны прибывают в пункт назначения одновременно. Но на значительных расстояниях это явление может привести к искажению сигнала.

Одномодовое волокно

Многомодовое волокно применяется для обеспечения экономичности на небольших расстояниях, а одномодовые волоконные каналы предназначены для дальней связи, высокоскоростных применений наподобие транспортной магистрали. Наиболее значительным отличием между ними является размер стержня: в одномодовом волокне он равен всего лишь 7—10 мк. Так как ограничения по дальности в одномодовом волокне менее жесткие, что обеспечивается значительно меньшим отражением, для передачи высокоинтенсивных фотонов применяется полупроводниковый лазер — в противоположность более слабому светодиоду, который используется в многомодовом волокне.

Наличие стеклянного стержня меньшего диаметра и мощных полупроводниковых лазеров обуславливает более высокую стоимость применения одномодового волокна по сравнению с многомодовым. Впрочем, большая стоимость компенсируется значительным преимуществом в скорости и дальности. К примеру, Международный союз электросвязи (ITU) опубликовал стандарт G.652, который обеспечивает поддержку одномодовой кабельной передачи на расстояния до 1000 км на скорости 2,5 Гбит/с и 3 км на скорости 40 Гбит/с. В одномодовом кабеле отражение лучей света не представляет особой проблемы, но протяженность кабеля ограничивается другим явлением под названием хроматической дисперсии.

Примечание

С одномодовым волоконно-оптическим кабелем работать значительно сложнее, чем с многомодовым из-за меньшего диаметра сердцевины. Ни тот, ни другой тип не предусматривает оптимального радиуса изгиба — это в целом несколько осложняет применение оптоволоконного кабеля.

Волоконные соединения

В волоконно-оптическом кабеле обоих типов применяется общий комплект оптических коннекторов, которые замыкают кабель на сетевые устройства. Как правило, для регенерации или преобразования световых импульсов в электрические сигналы принимающие устройства используют фотодиоды. Наиболее распространенные оптические коннекторы: ST и SC, используемые в приложениях 1000BaseFL. Другим распространенным коннектором, который применяется при создании информационных сетей, является MIC; наиболее часто он используется в сетях стандарта *FDDI* (Fiber Distributed Data Interface — распределенный интерфейс передачи данных по волоконно-оптическим каналам).

ST-коннекторы

Торцевой коннектор (Straight-Tip, ST) чаще всего встречается в сетях Ethernet, где между волокном и инфраструктурой неэкранированной витой пары применяются преобразователи среды передачи. Он напоминает BNC-коннектор для коаксиально-

го кабеля тем, что для блокировки его необходимо закрутить. ST-коннекторы требуют шлифовки волокна перед сборкой; следовательно, имеет смысл заказывать готовые кабели.

SC-коннекторы

Коннекторы с прямым соединением (Straight Connection, SC) не закручиваются, а просто вставляются в разъемы. Коннекторы такого типа также часто встречаются в сетях Ethernet, особенно на высокопроизводительных коммутаторах Ethernet. Подобно ST, SC-коннекторы требуют шлифовки и тщательной подгонки волокна, так что, заказав готовые кабели, вы можете сэкономить время и избавить себя от неисправностей, связанных с их неправильной самостоятельной установкой.

MIC-коннекторы

Интерфейсные коннекторы со средой (Medium Interface Connectors, MIC), как правило, применяются в сетях стандарта FDDI. Как и SC-коннекторы, они вставляются в разъемы, но в то же время устроены так, что обеспечивают механическое (подпружиненное) соединение разъема кабеля и порта концентратора.

MT-RJ и VF-45

Две компании спроектировали коннекторы, подходящие для применения не только в сетевой среде, но также для настольных волоконных соединений. Изначально разработанный компанией AMP коннектор MT-RJ содержит как передающие, так и приемные волокна, и, во многом подобно RJ-45, вставляется в разъемы. Коннектор VF-45 от компании 3M очень схож с RJ-45, включает передающие и приемные волокна, но, в отличие от MT-RJ, в нем есть защелка, которая не пропускает в точку соединения пыль и грязь.

Применение оптоволокна

Волоконно-оптический кабель лишен многих ограничений витой пары и коаксиального кабеля, но и с ним связано несколько трудностей, которые при всей их относительной незначительности нужно иметь в виду. Первой и наиболее существенной проблемой является гибкость кабеля. Так как волоконно-оптический кабель состоит из стекла и стеклоподобных веществ, у него довольно ограниченный радиус изгиба. При работе с оптоволокном следует соблюдать осторожность и избегать любых резких изгибов. Полезно не превышать радиус изгиба, равный 20 диаметрам кабеля. Кроме того, при склеивании или добавлении в оптоволоконный кабель коннекторов необходимо следить за тем, чтобы не повредить кожу осколками.

Хотя оптоволокно превышает даже ограничения по протяженности для коаксиального кабеля RG-8A/U, оно также ограничено. Существующие стандарты Ethernet предусматривают ограничение протяженности в 550 м для многомодового волокна и от 2 до 40 км (в зависимости от скорости) для одномодового волокна.

Наконец, прежде чем приступать к конструированию оптоволоконной инфраструктуры, необходимо принять во внимание ее стоимость. Оптоволокно обеспечивает значительное преимущество в производительности и протяженности, но затраты на прокладку этого кабеля значительно превосходят стоимость монтажа витой пары.

Учитывая такое увеличение стоимости, оптоволоконный кабель следует использовать только когда это действительно необходимо (т. е. для больших расстояний, магистрали между коммутаторами или высокоскоростных соединений).

Выявление повреждений оптоволокна

Подобно витой паре, большинство неисправностей волоконно-оптического кабеля влияют лишь на отдельный узел или сегмент кабеля. К счастью, при использовании оптоволокна проверять на наличие неисправностей нужно лишь одну пару передающих и принимающих кабелей. Но испытательное оборудование для оптоволоконных кабелей довольно дорогостоящее и, как правило, содержит оптический рефлектометр временной области (Optical Time Domain Reflectometer, OTDR).

Помимо дорогих оптических измерителей есть несколько методов, которые позволяют выявить неисправности быстро и значительно дешевле. Во-первых, если определенный сегмент кабеля еще не находился в активном состоянии, вполне вероятно, что нужно поменять передающие и принимающие коннекторы. Их нужно установить между двумя концами кабеля в прямо противоположном порядке; таким образом, передача на одном конце станет приемом на другом.

Если это возможно, проверьте, нет ли в кабельной линии резких изгибов — если надлежащий радиус изгиба не соблюдается, кабель может получить повреждения. При обнаружении повреждения кабеля замените этот участок.

Многие оптоволоконные устройства используют модульные оптические приемопередатчики, которые можно удалить или заменить. Если испытание оптоволоконной линии прошло успешно, но проблема не исчезла, попробуйте заменить приемопередатчик: возможно, он пришел в негодность или загрязнился.

Во многом подобно коаксиальному кабелю каждое место соединения в волоконной линии вводит повышенный уровень затухания. Поэтому слишком большое количество стыков или неудачные стыки могут привести к избыточной потере сигнала — вплоть до искаженной передачи или полного сбоя. Чтобы избежать чрезмерного затухания, ограничьте количество мест соединения в рамках данной волоконной линии. Если вы подозреваете, что проблема заключается именно в затухании, оптический рефлектометр временной области или измеритель света могут помочь подтвердить или опровергнуть ваши предположения.

Наконец, если подозрение падает на кабель, собранный вручную, рекомендуется заменить его целиком, или хотя бы поставить новые коннекторы — возможно, исходная стыковка ошибочна.

Примечание

Ни в коем случае не пытайтесь визуально проверить возможности передачи в подключенном оптоволоконном кабеле, т. к. воздействие лазерного излучения может привести к необратимому повреждению зрения. Помните, что в оптоволоконных системах, как правило, задействуются инфракрасные волны, выходящие за рамки видимой области спектра. При необходимости проверить оптический кабель пользуйтесь фонариком.

Симптомы неисправностей

Симптом 8.10. Отсутствует соединение в пределах сегмента оптоволоконного кабеля

В невозможности установить соединение, как правило, следует винить разрыв или неудачный стык, проверьте, чтобы передающие и принимающие коннекторы стояли на своих местах. Эта довольно часто встречающаяся неисправность в оптоволоконных структурах легко устранима. Если перестановка коннекторов не устраняет неисправность, проверьте, нет ли в кабеле резких изгибов или разрывов. При наличии любого физического повреждения лучше устранить поврежденный участок, заново склеив кабель, или установить новую кабельную линию. Кроме того, необходимо проверить правильность монтажа всех оптоволоконных коннекторов и, при необходимости, внести поправки.

Симптом 8.11. Соединение отсутствует или является нестабильным

Нестабильное соединение, как правило, обусловлено чрезмерным затуханием или слабым сигналом. Две основные причины этих состояний — это слишком большое количество стыков в кабельной линии или плохо смонтированный или загрязненный стык/коннектор. Кроме того, затухание может быть вызвано наличием резкого изгиба кабеля, пусть даже при этом не произойдет полного разрыва стержня.

Проверьте, нет ли внутри коннекторов плохо сведенных соединений или пыли и не поврежден ли кабель. При отсутствии физических дефектов и наличии задержки светодиода или отказа светодиода рекомендуется переставить все информационные приемопередатчики или сетевые адаптеры на линии. Если у вас есть оптический рефлектометр или измеритель света, проверьте интенсивность сигнала и/или затухание в кабеле.

Симптом 8.12. После установки новой рабочей станции соединение отсутствует

Как и при появлении предыдущей неисправности, в данном случае причиной может быть неисправность кабельной линии, стыка или коннектора. С помощью оптического рефлектометра или измерителя света проверьте кабельную линию и замените дефектный компонент. Если же в оборудовании неисправностей не обнаружено, проверьте исправность передающего оборудования на обоих концах и выполните все необходимые замены. Наконец, нужно удостовериться в том, что передающий и принимающий кабели не перепутаны.

Дополнительные ресурсы

3Com: **http://www.3com.com/technology/**.

Неисправности кабелей 3Com: **http://support.3com.com/infodeli/tools/netmgt/tncsunix/product/091500/c11ploss.htm#14431**.

Annixter: **http://www.anixter.com/techlib/**.

Bell Labs: **http://www.bell-labs.com/technology/lightwave/**.

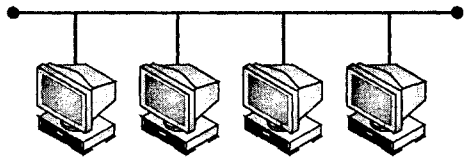
Cisco Systems:
http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/manguide/appa.htm.

Corning Fiber: **http://www.corningfiber.com**.

Развитие телефонного кабеля: **http://telecom.copper.org/evolution.html**.

Fluke Networks: **http://www.flukenetworks.com**.

Институт инженеров по электротехнике и радиоэлектронике (IEEE, Institute of Electrical and Electronics Engineers): **http://grouper.ieee.org/groups/802/3/**.



ГЛАВА 9

Материнские платы для серверов

Материнская (или системная) плата — это основа любого сервера, рабочей станции и обычной настольной системы (рис. 9.1). Устройства на материнской плате обеспечивают систему всеми ресурсами — линиями запроса прерывания (Interrupt ReQuest Line, IRQ), каналами прямого доступа к памяти (Direct Memory Access, DMA) и адресами ввода/вывода (I/O location) — и поддерживают ее ключевые устройства: процессор (Central Processing Unit, CPU), память, часы реального времени, базовую систему ввода/вывода (Basic Input/Output System, BIOS) и разъемы расширения. Материнская плата сервера поддерживает и другие ресурсы, имеющие важное значение для сети: дополнительные центральные процессоры, видеоконтроллер, встроенный

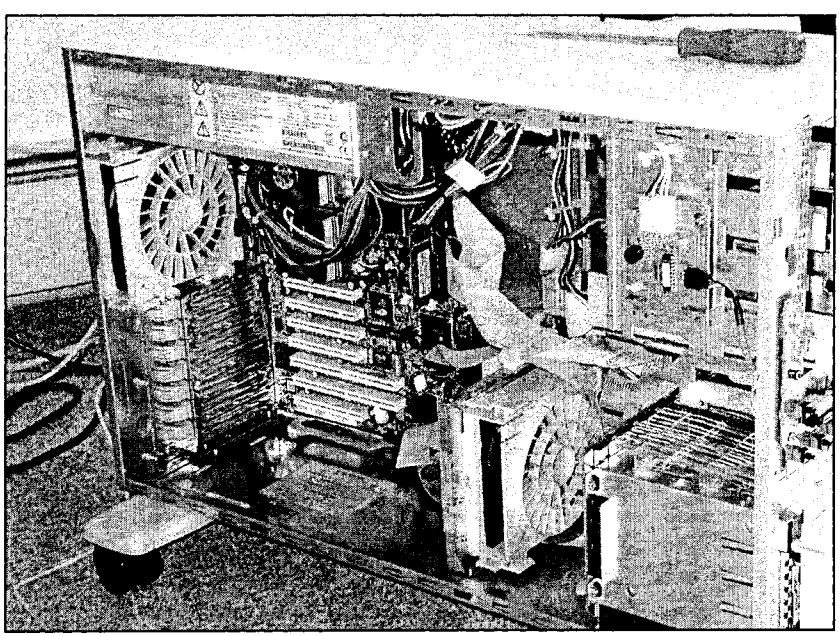


Рис. 9.1. Сервер Gateway 7400 — вид изнутри

SCSI (Small Computer Systems Interface — интерфейс малых вычислительных систем) хост-адаптер, встроенный IDE-контроллер (Integrated Drive Electronics — встроенный интерфейс накопителей) и другие средства, относящиеся к сетям (о них вы узнаете позже). В этой главе рассматриваются характеристики и структура типичной серверной материнской платы, особое внимание уделено процессору, памяти и другим устройствам на материнской плате, а также даны основные сведения об устранении неисправностей, которые помогут вам ликвидировать сбои в работе сервера с максимальной эффективностью.

Серверные материнские платы

Прежде чем вы сможете квалифицированно устанавливать и модернизировать серверную материнскую плату, а также устранять ее неисправности, необходимо научиться с легкостью ориентироваться в важных устройствах материнской платы. Несмотря на небольшие различия в устройстве материнских плат, в расположении их устройств разобраться необычайно просто. В данной книге мы подробно ознакомимся с материнской платой Intel L440GX+ (рис. 9.2) и кратко обсудим серверный корпус Intel SKA4.

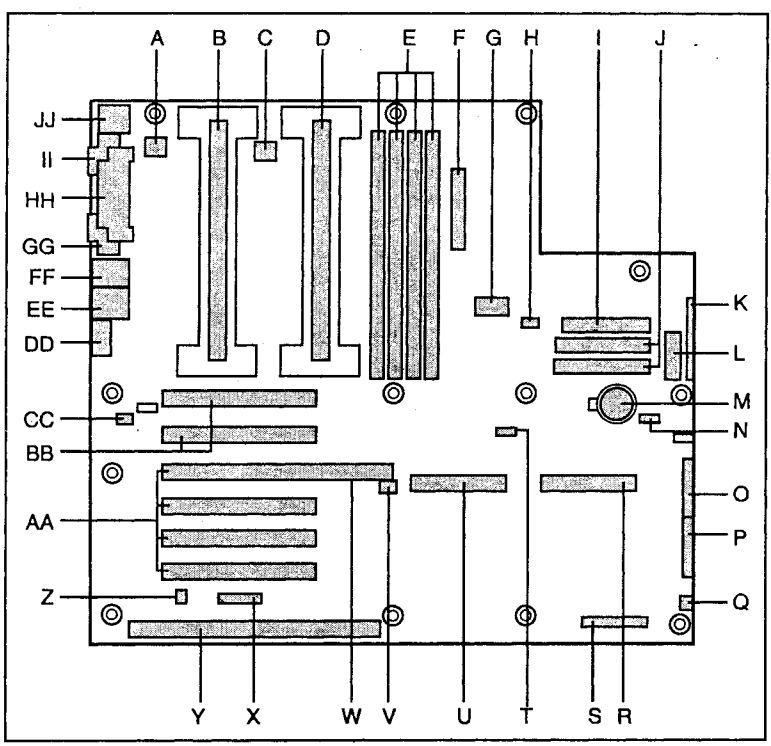


Рис. 9.2. Серверная материнская плата Intel L440GX (публикуется с разрешения Intel Corporation)

Процессор

На материнской плате необходимо установить по меньшей мере один процессор (см. элементы B и D на рис. 9.2). Серверная материнская плата, как правило, поддерживает несколько (два, четыре или восемь) процессоров с картриджем (под разъем вида Slot1 с 242 контактами) типа Pentium II, Pentium III, а чаще — разновидностей Pentium II/III Xeon. Процессорный интерфейс на L440GX+ поддерживает многопроцессорную систему (MultiProcessor, MP) и работает на частоте 100 МГц (новые материнские платы поддерживают процессоры Pentium III/IV Socket 370/478 на скорости шины от 133 МГц). Локальный *усовершенствованный программируемый контроллер прерываний* (Advanced Programmable Interrupt Controller, APIC) выполняет функцию управления прерываниями в средах с одним и несколькими процессорами. Картридж содержит ядро процессора с интегрированной кэш-памятью первого уровня (Level 1 Cache, L1) емкостью 16 Кбайт и кэш-память второго уровня (L2) емкостью 512 Кбайт. Кэш-память второго уровня L2 процессора Pentium II/III включает *пакетное статическое запоминающее устройство с произвольным доступом* (Burst Static RAM или BSRAM, где Random Access Memory, RAM — память с произвольным доступом), а скорость обработки *кода с исправлением ошибок* (Error-Correcting Code, ECC) составляет половину тактовой частоты ядра. Числовой сопроцессор процессора (схема для выполнения операций с плавающей точкой, Floating-Point Unit, FPU) значительно повышает скорость операций с плавающей точкой. Процессоры с картриджем фиксируются на материнской плате с помощью специального механизма. Охлаждающий вентилятор для каждого процессора подключен к локальному разъему питания вентилятора/тахометра (см. элементы A и C на рис. 9.2 соответственно).

Память

Чтобы хранить файлы и данные, запрашиваемые из сети, серверам нужна память — много памяти. Чтобы добиться максимальной эффективности системы, следует выбрать память, производительность которой будет наилучшей для вашей материнской платы. Серверной платой L440GX+ поддерживаются только синхронные динамические запоминающие устройства (Synchronous Dynamic RAM, или Synchronous DRAM, или SDRAM) PC100 с частотой 100 МГц с корректирующим кодом или без него. У вас может быть другая материнская плата, поэтому необходимо тщательно ознакомиться с ее техническими требованиями. К примеру, на вашем сервере может использоваться память типа PC133 SDRAM или PC600/PC800 Rambus DRAM (RDRAM). На материнской плате L440GX+ память распределена по четырем блокам модулей SDRAM DIMM (Dual In-line Memory Module — модуль памяти с двухрядным расположением выводов) (элемент E на рис. 9.2), каждый из которых обеспечивает 72 разряда нерасслоенной памяти (без чередования адресов) (т. е. 64 бита основной памяти плюс корректирующий код). Вы можете установить от 64 Мбайт до 2 Гбайт DIMM-модулей памяти с регистрами или от 32 Мбайт до 1 Гбайт DIMM-модулей небуферизованной памяти. Память следует добавлять в порядке от разъема 1 до разъема 4. Контроллер памяти автоматически обнаруживает, устанавливает размер и инициализирует память — в зависимости от типа, размера и скорости установленных модулей DIMM/RIMM (Rambus Interface Memory Module — модуль памяти с интерфейсом от фирмы Rambus). Затем, пользуясь регистрами конфигурации, контроллер сообщает о размере и распределении памяти серверу.

Примечание

Никогда не смешивайте небуферизованную память и память с регистрами. Для достижения лучшей целостности данных в серверной среде рекомендуется установить память с корректирующим кодом, хотя установка памяти без корректирующего кода также допустима. Если установить одновременно модуль памяти с корректирующим кодом и без него, то все функции корректировки ошибок будут отключены

Главный мост/контроллер памяти

Серверные материнские платы проектируются на основе главного набора микросхем (чипсета), который реализует большинство функций, поддерживаемых материнской платой. В нашем случае, плата Intel L440GX+ сконструирована на основе Intel 82440GX AGPSet (440GX). Этот чипсет поддерживает частоту системной шины процессора 100 МГц, содержит контроллер памяти DRAM, интерфейс шины PCI (Peripheral Connect Interconnect — межсоединение периферийных компонентов), интерфейс AGP (Accelerated Graphic Port — ускоренный графический порт) и функции управления режимом электропитания. Интерфейс системная шина/память в 440GX оптимизирован для частоты 100 МГц с использованием основной памяти SDRAM на частоте 100 МГц. В 440GX поддерживается интерфейс PCI, совместимый с PCI 2.1. Контроллер памяти 440GX поддерживает до 2 Гбайт памяти с корректирующим кодом (или без него) при использовании модулей памяти SDRAM PC100 SIMM (Single In-line Memory Module — модуль памяти с однорядным расположением выводов). Корректирующий код может обнаруживать и исправлять одноразрядные ошибки, а также, в целях обеспечения лучшей целостности данных, выявлять ошибки в нескольких разрядах.

Поддержка периферийных устройств

Сервер осуществляет взаимодействие с реальным миром через порты и разъемы, поэтому вам следует ознакомиться с различными устройствами и портами на материнской плате. Чип ввода/вывода (Super I/O chip) управляет многими системными портами ввода/вывода. Контроллеры (типа National 87309) обеспечивают поддержку двух последовательных портов, одного параллельного порта, накопителя на дискетах, PS/2-совместимой клавиатуры и мыши. Как показано на рис. 9.3, для каждого порта на серверной плате есть коннектор.

- *Последовательные порты.* Каждый последовательный порт (см. элементы GG и II на рис. 9.2 или элемент D на рис. 9.3) можно установить на один из четырех портов COM или активировать отдельно. Каждый порт во включенном состоянии можно запрограммировать на генерирование чувствительных к уровню или фронту прерываний. В отключенном состоянии последовательного порта его прерывания могут применяться другими встроенными платами.
- *Параллельный порт.* Чип ввода/вывода предусматривает один IEEE 1284-совместимый 25-контактный порт поддерживающий режимы двунаправленных портов EPP (Enhanced Parallel Port — улучшенный параллельный порт) и ECP (Extended Capabilities Port — порт с расширенными возможностями). Параллельный порт (см. элемент HH на рис. 9.2 или элемент C на рис. 9.3) можно настроить на другой адрес порта и прерывание. Режим ECP поддерживается с помощью двух воз-

можных каналов DMA. В отключенном состоянии параллельного порта его прерывания могут применяться другими встроенными платами.

- *USB-порты.* USB (Universal Serial Bus — универсальная последовательная шина) обеспечивает универсальный способ подсоединения различных внешних устройств (т. е. сканеров и принтеров) без необходимости отключать питание системы и выполнять установку устройства. Простые четырехпроводные кабели можно подключать и отсоединять, не мешая нормальному функционированию сервера. На большинстве материнских плат (включая L440GX+) есть двухпортовый концентратор USB (см. элемент EE на рис. 9.2 или элемент H на рис. 9.3).
- *Проникновение в корпус.* Как правило, все действия по обеспечению защиты связаны с паролями и авторизацией в пределах сетевой операционной системы; при этом физической безопасности сервера зачастую не придают большого значения. Коннектор датчика открытия корпуса (см. элемент Z на рис. 9.2) подсоединяется к физическому ключу на корпусе. При вскрытии корпуса система обеспечения защиты сервера оповещает об этом сетевого администратора *(более подробный анализ средств защиты сервера приводится далее в этой главе).*

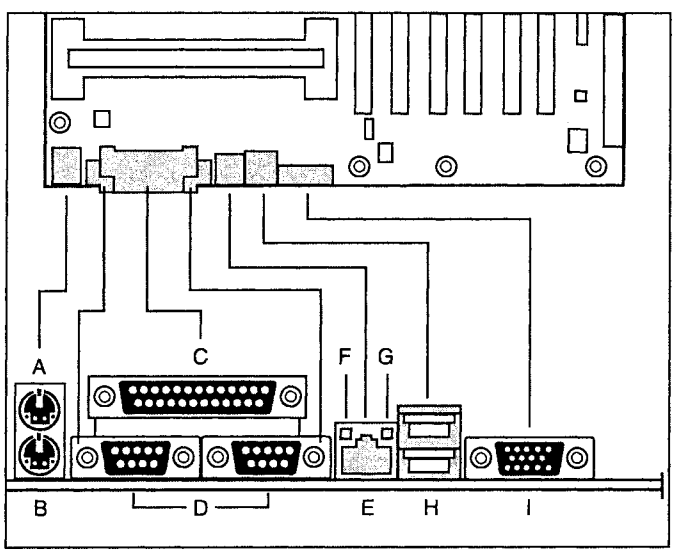


Рис. 9.3. Порты ввода/вывода на материнской плате серверного типа (публикуется с разрешения Intel Corporation)

- *Аккумуляторная поддержка.* Информация, определяющая конфигурацию системы, обычно хранится в небольшой области маломощной памяти под названием CMOS RAM (Complementary Metal-Oxide Semiconductor RAM — оперативная память КМОП на комплементарном металл-окись-полупроводнике). Так как при выключении питания системы эта информация должна быть сохранена, для поддержания CMOS RAM используется небольшой аккумулятор (см. элемент M на рис. 9.2). Его необходимо периодически заменять (информация о замене аккумулятора — в документации к материнской плате).

- *Разъемы расширения.* Вполне возможно, что вам потребуется присоединить к компьютеру одно или несколько устройств, расширяющих его функциональные возможности. Видеоадаптеры, адаптеры SCSI, адаптеры RAID и сетевые платы — вот лишь некоторые устройства, которые, как правило, используются на сервере. Для успешной работы устройства расширения его необходимо установить в подходящий разъем расширения (гнездо) — таким образом оно сможет взаимодействовать с центральной системой. Обычно на материнской плате имеется разъем ISA (Industry-Standard Architecture — архитектура индустриального стандарта) (см. элемент Y на рис. 9.2) и четыре или более гнезд PCI. В современных серверных материнских платах типа L440GX+ есть четыре 32-битовых разъема (слота) PCI с частотой 33 МГц и два 32-битовых разъема PCI большей производительности с частотой 66 МГц (см. элементы AA и BB на рис. 9.2 соответственно). Обычно при установке платы PCI с частотой 33 МГц в один из разъемов PCI с частотой 66 МГц скорость шины для этих разъемов уменьшается до 33 МГц.

Примечание

Компоненты некоторых полноразмерных плат расширения, установленных в разъеме 6, могут мешать фиксаторам коннекторов DIMM. Будьте внимательны при установке полноразмерных плат.

- *Видеопорт.* Графические средства, конечно, не являются жизненно важными для сетевого сервера, но на некоторых материнских платах есть интегрированный видеоконтроллер (см. элемент DD на рис. 9.2 или элемент I на рис. 9.3). В составе платы L440GX+ имеется VGA-совместимый 64-битовый SVGA-контроллер Cirrus Logic CL-GD5480. Стандартная конфигурация предполагает использование 2 Мбайт встроенной синхронной графической памяти (Synchronous Graphics RAM, SGRAM) с временем доступа, равным 10 нс. Видеоконтроллер поддерживает разрешение до 1600×1200 пикселов и до 16,7 млн цветов. Кроме того, для немерцающих дисплеев он обеспечивает частоту обновления кадров до 100 Гц. Расширить видеопамять серверной платы нельзя, хотя ее можно отключить и заменить видеокартой.
- *Контроллер SCSI.* Многие профессиональные серверные платы содержат встроенный хост-адаптер SCSI для устройств SCSI и обеспечивают поддержку RAID. На материнской плате L440GX+ имеется двухканальный SCSI-контроллер Adaptec AIC-7896, который независимо поддерживает два контроллера: UltraWide2 (LVDS) и UltraWide ("сверхширокий") SCSI в разъемах PCI (см. элементы U и R на рис. 9.2 соответственно). Разъем PCI 4 может быть модернизирован в RAID, что обеспечит поддержку контроллера Adaptec ARO-1130U2 RAIDport (см. элемент W на рис. 9.2). Шина SCSI терминируется на материнской плате с помощью активных оконечных нагрузок, которые нельзя отключить, и поэтому на одном конце шины всегда должен быть интегрированный контроллер SCSI. Устройство SCSI на конце кабеля также должно быть терминировано. Устройства LVDS (Low Voltage Differential Signaling — дифференциальные сигналы низкого напряжения), как правило, не нуждаются в терминировании, но устройства на базе традиционного несимметричного интерфейса SCSI обычно терминируются с помощью перемычки или резисторного блока. Если в составе серверной платы есть кабель SCSI, вполне возможно, что она была модернизирована и позволяет применять активную нагрузку. Подсоединяя любые устройства SCSI к этому кабелю,

убедитесь в том, что они не терминированы — данную опцию можно изменить на самом устройстве с помощью перемычки или блока оконечной нагрузки (чтобы определить текущую опцию, обратитесь к документации устройства SCSI). Оконечная нагрузка шины SCSI реализуется с помощью активной нагрузки на материнской плате и на конце кабеля SCSI.

- *IDE и контроллер гибких дисков.* IDE — это недорогой 40-контактный интерфейс, спроектированный для 16-битовых интеллектуальных дисководов, дисководов лазерных дисков и дисководов Iomega Jaz, накопителей на магнитной ленте ATAPI (AT Attachment Packet Interface — пакетный интерфейс для подключения периферийных устройств к AT-совместимым компьютерам (AT, Advanced Technology — улучшенная технология, стандарт ПК)) IDE и других типов дисководов со встроенной электроникой дискового контроллера. Микросхема PIIX4e материнской платы L440GX+ (также известная под названием PCI/ISA/IDE Accelerator (ускоритель)) — это многофункциональное устройство на серверной плате, которое действует как контроллер Fast IDE на основе PCI. PIIX4e управляет операциями программируемого управления вводом/выводом (Programmed Input/Output, PIO) и DMA-захвата шины на скорости передачи данных до 33 Мбайт/с (Ultra-DMA/33), хотя другие материнские платы могут поддерживать более высокую скорость передачи данных: 66 Мбайт/с (Ultra-DMA/66) или 100 Мбайт/с (Ultra-DMA/100). Контроллер IDE располагает двумя каналами (см. элемент J на рис. 9.2) и поддерживает по два устройства на один канал, т. е. максимальное число IDE-устройств составляет четыре. Светодиод активности жесткого диска на корпусе сервера можно подключить к соответствующему разъему материнской платы (см. элемент V на рис. 9.2). В состав материнской платы также входит простой 34-контактный разъем для дисковода гибких дисков (см. элемент I на рис. 9.2).

Примечание

Максимальная длина кабеля IDE составляет 18 дюймов (45,72 см). Увеличение длины кабеля может привести к снижению скорости передачи данных или их потере из-за интерференции электрических сигналов.

- *Сетевой адаптер.* Вполне возможно, что материнская плата вашего сервера имеет интегрированный сетевой адаптер, что исключает необходимость в одноканальном сетевом адаптере (см. элемент FF на рис. 9.2 или элемент E на рис. 9.3). Серверная плата L440GX+ поддерживает сетевой интерфейс 10BaseT/100BaseTX на основе микросхемы 82559 FastEthernet PCI Bus Controller от компании Intel. Как устройство управления передачей данных по шине PCI сетевой контроллер может передавать пакеты данных со скоростью до 132 Мбайт/с (32 бит на частоте 33 МГц). Он содержит два буфера обратного магазинного типа (FIFO, First-In First-Out — "первым пришел — первым обслужен") для передачи и приема; которые обеспечивают равномерную передачу данных к шине PCI. Контроллер обеспечивает поддержку сетей со скоростью передачи данных 10 Мбит/с и 100 Мбит/с с возможностью работы в дуплексном и полудуплексном режимах и с двусторонней передачей на скорости 100 Мбит/с. Кроме того, контроллер выполняет автораспознавание/переключение на скорости передачи данных в сети 10 или 100 Мбит/с. Светодиоды состояния сети на серверной плате являются индикаторами приема-передачи данных по локальной сети (зеленый светодиод:

элемент F на рис. 9.3) и режима передачи данных в 10/100 Мбит/с по локальной сети (оранжевый светодиод: элемент G на рис. 9.3).

- *Клавиатура и мышь.* Контроллер клавиатуры/мыши является PS/2-совместимым, а на задней панели входов/выходов есть коннекторы этих устройств (см. элемент JJ на рис. 9.2 или элементы B и A на рис. 9.3 соответственно). В качестве дополнительной функции обеспечения безопасности сервер после специальной настройки может блокировать ввод с клавиатуры и мыши по истечении некоторого предварительно определенного периода бездеятельности сервера. Таким образом, когда время, предустановленное на таймере бездеятельности, истекает, ввод с клавиатуры и мыши невозможен до тех пор, пока не будет введен серверный пароль.
- *Управление режимом электропитания.* Практически все современные серверные материнские платы (включая L440GX+) поддерживают сложные методы управления режимом электропитания типа ACPI (Advanced Configuration and Power Interface — усовершенствованный интерфейс управления конфигурированием и энергопотреблением), определенного в спецификации ACPI 1.0, PC97 и более поздних версиях. Операционная система с поддержкой ACPI может привести систему в состояние, когда скорость вращения жестких дисков снижается, системные вентиляторы останавливаются и любая обработка данных прекращается. Впрочем, электроснабжение при этом сохраняется, рассеивание мощности процессорами продолжается, а значит, вентиляторы источника электропитания и процессора также продолжат свою работу. Система "проснется" тогда, когда произойдет некое внешнее событие типа ввода с клавиатуры, движения мышью или же с помощью коннектора Wake On LAN (активизации по сети) (см. элемент T на рис. 9.2) будет обнаружена активность локальной сети. L440GX+ поддерживает состояния ожидания s0, s1, s4 и s5 (фактически доступные состояния зависят от конкретной версии Windows, UNIX или Linux).
  - s0. Это нормальное активное состояние системы.
  - s1. Это состояние ожидания процессора; при котором обработка данных замедляется (ее скорость уменьшается) или полностью останавливается.
  - s4. Это спящий режим или режим сохранения данных на жестком диске (Save to Disk). Содержимое памяти и состояние машины сохраняются на жестком диске, и система выключает питание большинства устройств. Нажатие на кнопку <Power> (или другое событие запуска) восстанавливает состояние системы с диска и возобновляет ее нормальную работу.
  - s5. Это состояние программного отключения ("soft off"). В этом состоянии работают лишь секция часов реального времени в микросхеме контроллера PIIX4 и микросхема контроллера управления материнской платой (Baseboard Management Controller, BMC).
- *Электропитание и охлаждение.* Электропитание обеспечивается через 20-контактный разъем питания ATX (Advanced Technology eXtension — расширенная технология AT), а также факультативный вспомогательный разъем питания ATX (см. элементы F и G на рис. 9.2). Через основной разъем питания проходят различные напряжения и электросигналы, необходимые для функционирования материнской платы и устройств расширения. В табл. 9.1 представлена схема расположения контактов разъема питания ATX. Кроме того, имеется достаточно много

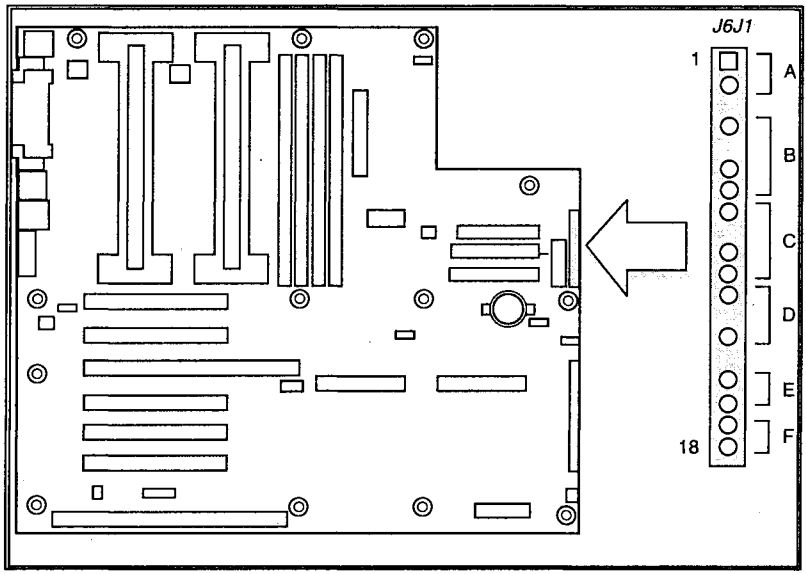


Рис. 9.4. Крупный план коннектора передней панели (публикуется с разрешения Intel Corporation)

Таблица 9.1. *Схема расположения контактов 20-контактного разъема питания ATX*

№ контакта	Описание	№ контакта	Описание
Контакт 1	+3.3 В постоянного тока	Контакт 11	+3,3 В постоянного тока
Контакт 2	+3.3 В постоянного тока	Контакт 12	–12 В постоянного тока
Контакт 3	Заземление	Контакт 13	Заземление
Контакт 4	+5 В постоянного тока	Контакт 14	Электропитание включено (PS-ON): "гибкий" сигнал регулирования мощности
Контакт 5	Заземление	Контакт 15	Заземление
Контакт 6	+5 В постоянного тока	Контакт 16	Заземление
Контакт 7	Заземление	Контакт 17	Заземление
Контакт 8	Нормальное энергоснабжение	Контакт 18	–5 В постоянного тока
Контакт 9	+5 В постоянного тока (резервная мощность)	Контакт 19	+5 В постоянного тока
Контакт 10	+12 В постоянного тока	Контакт 20	+5 В постоянного тока

коннекторов для вентиляторов корпуса (см. элементы H, Q и CC на рис. 9.2). В большинстве случаев применение всех доступных разъемов для вентиляторов корпуса не является обязательным, однако дополнительное охлаждение отнюдь не помешает серверу, находящемуся в условиях сильной загрузки.

- *Коннектор передней панели.* К материнской плате нужно подсоединить важные устройства управления и индикаторы корпуса через коннектор передней панели (см. элемент K на рис. 9.2). Плата L440GX+ предусматривает соединения для выключателя электропитания, светодиода активности жесткого диска, динамика, светодиода электропитания, переключателей сброса и ожидания. Подробная схема этих соединений приводится на рис. 9.4. Зачастую при замене и модернизации материнской платы на эти соединения обращают недостаточно внимания.

Управление сервером и функции обеспечения безопасности

Администраторы сетей и технические специалисты должны иметь доступ к серверу для его тестирования и изменения конфигурации. Следовательно, вам должны быть известны различные средства управления, поддерживаемые сервером, и понятны доступные функции обеспечения безопасности. Ниже будут рассмотрены функции этого типа, представленные в серверной материнской плате Intel L440GX+.

Управление сервером

Управление сервером осуществляется через микроконтроллер на материнской плате. Intel называет этот микроконтроллер BMC. По существу, BMC — это автономный компонент материнской платы, выполняющий мониторинг системных событий и регистрирующий их в энергонезависимой памяти под названиями *журнал системных событий* (System Event Log, SEL) и *запись о состоянии датчика* (Sensor Data Record, SDR). Среди типичных событий — состояния перегрева и перенапряжения, отказ вентилятора и проникновение в корпус. BMC обеспечивает доступ к информации журнала системных событий, так что работающее на сервере программное обеспечение может запрашивать и получать данные о текущем состоянии сервера. Нормально запитанный BMC выполняет следующие функции:

- контроль температуры и напряжений серверной платы;
- контроль наличия процессоров;
- обнаружение и обозначение неисправностей вентилятора;
- управление интерфейсами SEL и SDR;
- контроль синхронизации временных меток SDR/SEL;
- контроль таймера управления системой;
- контроль циклического таймера SMI (System Management Interrupt — прерывание для перехода в режим системного управления);
- управление обработчиком немаскируемых прерываний (Non-Maskable Interrupt, NMI) передней панели;

- контроль событий;
- управление безопасным режимом, включая бланкирование видео, обеспечение защиты от записи на гибкий диск и запуск блокировки/разблокирования передней панели;
- управление инициализацией сенсорного уровня;
- контроль поддержки активизации по сети.

Контроллер BMC и связанные с ним схемы получают электропитание от резервного источника питания ATX напряжением в 5 В, который остается в активном состоянии даже при выключении сервера (сервер при этом должен быть подключен к источнику переменного тока). После сбоя системы содержимое журнала системных событий можно извлечь и использовать для анализа специалистами. Для извлечения журнала системных событий можно задействовать программные средства управления сервером (типа программ Intel Server Control на компакт-диске, поставляемом вместе с серверной платой L440GX+). Как правило, обновление таких программных средств производится непосредственно с Web-сайта производителя. Для материнской платы L440GX+ эти программы можно скачать с сайта

support.intel.com/support/motherboards /server/l440gx.

В зависимости от конструкции вашей материнской платы у вас также может быть доступ к информации журнала системных событий и данных о состоянии датчиков. L440GX+ предоставляет возможность обращения к этим данным через шину интеллектуального управления Intel (Intelligent Management Bus, IMB) (см. элемент N на рис. 9.2). В материнскую плату (см. элемент S на рис. 9.2) можно вставить плату аварийного управления сервером типа Intel LANDesk Server Monitor Module card (SMM), получить данные журнала системных событий и сделать эти данные удаленно доступными через локальную сеть или телефонное соединение. Плата SMM поставляется в комплекте с LANDesk Server Manager Pro.

Аварийное управление и система оповещения event paging

Каждая минута, когда локальная сеть не работает, может повлиять на эффективность и продажи даже небольшой компании; именно поэтому средства управления сервером и журналы системных событий предназначены для обеспечения быстрого и окончательного восстановления системы в случае возникновения неисправностей. Материнская плата L440GX+ включает программное обеспечение порта EMP (Emergency Management Port — порт аварийного управления), который позволяет дистанционно управлять сервером через модемное или прямое (с использованием последовательных портов) соединение. Таким образом, специалист может получить доступ к серверу и произвести его проверку, находясь совершенно в другом месте (например, в удаленном офисе службы поддержки). Программное обеспечение EMP позволяет не только получать удаленный доступ к серверу, но и включать/выключать сервер или перезагружать его, а также просматривать содержимое журнала системных событий и данных о состоянии датчиков с целью обнаружения событий, которые могли стать причиной неисправности. Дистанционное получение этой информации позволяет специалисту выбрать подлежащие замене детали заранее, а затем произвести замену деталей непосредственно в сервере.

Система оповещения event paging позволяет серверу в случае возникновения неисправностей устанавливать исходящую связь и отправлять пейджинговое сообщение. Сервер можно настроить на автоматический вызов пейджинговой службы и отправку вам сообщения, как только произойдет событие, влекущее за собой возможный сбой в работе (например, изменение температуры и напряжения сверх допустимого диапазона, проникновение в корпус сервера, неисправность вентилятора и т. д.). В результате специалисты и администраторы получают практически незамедлительное оповещение о неисправности сервера. Так как система оповещения является частью автономного контроллера BMC, сообщение будет отправлено, даже если процессоры сервера будут отключены, а системное программное обеспечение недоступно. Отправка сообщения требует наличия внешнего модема, подключенного к порту EMP (обычно это последовательный порт COM2).

Безопасность

Обеспечение безопасности для сетевых администраторов является насущной проблемой. Необходимо исключить доступ в сеть неавторизованных пользователей и защитить аппаратное обеспечение сервера от случайного (и умышленного) повреждения. Как правило, сервер поддерживает и аппаратные, и программные средства обеспечения безопасности.

Механическая блокировка

Если сервер поддерживает механическую блокировку, можно воспользоваться датчиком обнаружения проникновения в корпус. При вскрытии корпуса сервера этот датчик передает аварийный сигнал на серверную плату, где его обрабатывают микропрограммные средства BMC и программное обеспечение управления сервером. В зависимости от того, как запрограммирован сервер, он может реагировать на проникновение отключением питания или блокировкой клавиатуры.

Программная блокировка

Настройка параметров CMOS и утилита SSU (System Setup Utility — утилита настройки системы) предусматривают функции защиты с помощью пароля, которые способны предотвратить несанкционированный или случайный доступ к системе. После включения средств защиты обращение к системе возможно лишь при условии введения правильного пароля (паролей). К примеру, программная система защиты:

- задействует таймер блокировки клавиатуры; в результате по истечении определенного периода времени для повторной активации клавиатуры и мыши сервер потребует ввести пароль;
- установит и активирует административный пароль;
- установит и активирует пароль пользователя;
- переведет систему в безопасный режим, при котором ввод данных с клавиатуры и мыши, а также применение переключателя сброса и выключателя электропитания на передней панели будут недоступны;
- активизирует сочетание горячих клавиш для запуска безопасного режима;

- блокирует запись на гибкий диск в условиях безопасного режима;
- запретит доступ к загрузочному сектору дисковода основного жесткого диска.

Безопасный режим

В безопасном режиме вы сможете загрузить сервер, и операционная система будет работать, но для использования клавиатуры или мыши необходимо ввести пароль пользователя. Отключить питание системы или перезапустить сервер, пользуясь переключателями на передней панели, невозможно. Безопасный режим не оказывает никакого воздействия на функции, поддерживаемые модулем контроля сервера (Server Monitor Module, SMM), или на регулировку питания часов реального времени. Вывод сервера из безопасного режима не меняет состояние энергоснабжения системы. К примеру, если нажать и отпустить выключатель электропитания, когда сервер находится в безопасном режиме, система не отключится после того, как будет выведена из этого режима. Если же во время выведения системы из безопасного режима выключатель электропитания на передней панели будет находиться в нажатом состоянии, отключение питания произойдет.

Примечание

Из производственного сервера следует удалять дисководы гибких дисков и лазерных дисков; таким образом, злоумышленник не сможет загрузить систему, отключив питание и вставив, скажем, загрузочную дискету UNIX. Новое программное обеспечение, как правило, можно загрузить из Интернета так, что эти дисководы, скорее всего, будут не нужны. Если же дисководы вам необходимы, установите настройки CMOS так, чтобы дисководы не являлись загрузочными устройствами.

Установка серверной материнской платы

Будете ли вы заменять неисправную материнскую плату или модернизировать существующий сервер, — в любом случае когда-нибудь вам придется устанавливать материнскую плату. Установка материнской платы — это чрезвычайно ответственная процедура, поэтому для того, чтобы должным образом переустановить все уже имеющиеся устройства, требуется особое внимание. В этой части главы рассматривается процесс установки материнской платы, процессора и памяти. Для примера возьмем материнскую плату ATX типа модели Intel L440GX+, изображенной на рис. 9.5. В документации к материнской плате всегда содержатся необходимые инструкции и указания.

Стандартные меры предосторожности

Прежде чем начинать установку материнской платы, необходимо ознакомиться с некоторыми предупреждениями и предостережениями, изложенными в этом разделе, и всегда иметь их в виду.

- Выключите питание сервера и выдерните вилку из розетки. Помните: просто выключить сервер средствами Windows недостаточно. Резервное питание подается на систему всегда, когда она подключена к источнику переменного тока. Вы обязательно должны выдернуть из розетки шнур питания и только после этого можете открывать корпус или приступать к работе. Кроме того, не забудьте выключить монитор.

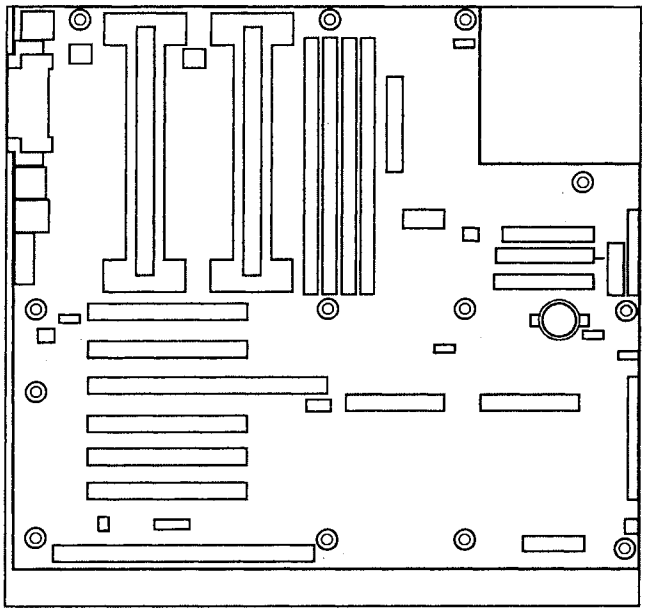


Рис. 9.5. Схема монтажных гнезд на типичной серверной материнской плате ATX (публикуется с разрешения Intel Corporation)

- Отсоедините кабели периферийных устройств. Помимо прочего, питание подается через большинство периферийных кабелей, подсоединенных к серверу. Как только вы отключили систему и выдернули из розетки шнур питания, обязательно отсоедините сетевой кабель, телефонный (модемный) кабель, кабели других локальных периферийных устройств (например, принтера, подключенного через параллельный порт) и выключите эти устройства.
- Снимите электростатический заряд. Материнская плата, как и большинство других устройств на сервере, крайне уязвима по отношению к случайному электростатическому разряду (ElectroStatic Discharge, ESD). Прежде чем открывать корпус сервера, вы должны снять с себя электростатический заряд с помощью специального надежно заземленного антистатического браслета. Кроме того, на рабочую поверхность следует поместить хорошо заземленный антистатический коврик. Берите все электронные платы только за края. После извлечения платы из ее защитной упаковки (или из системного блока сервера) положите ее стороной со смонтированными компонентами вверх на заземленную поверхность без статического напряжения.

Снятие платы

Сначала давайте посмотрим, как снимается материнская плата. Эта процедура особенно важна, когда в процессе модернизации сервера нужно извлечь материнскую плату. Прежде всего выключите сервер и выдерните из розетки шнур питания. Чтобы извлечь материнскую плату из корпуса, выполните представленную далее последовательность действий.

1. Откройте сервер, и снимите все периферийные устройства и компоненты, мешающие доступу к серверной плате. В большинстве случаев придется извлечь все платы расширения и кабели, подсоединенные к материнской плате, но вполне возможно, что потребуется снять один или несколько дисководов. Все зависит от конструкции конкретного корпуса (в руководстве к корпусу должна содержаться исчерпывающая информация по этому вопросу).
2. Промаркируйте и отсоедините все внутренние и внешние кабели, подключенные к платам расширения. Маркировка избавит вас от необходимости угадывать, что и куда присоединить при обратной сборке. Полезным будет и цифровой фотоснимок сервера изнутри.
3. Снимите все платы расширения. Не забывайте, что платы необходимо положить на антистатический коврик или в антистатический пакет, что сохранит их от случайного повреждения электростатическим разрядом.
4. Промаркируйте и отсоедините все внутренние и внешние кабели, подключенные к серверной плате (включая кабель питания ATX).
5. Если вы собираетесь переносить память и процессор (процессоры) на новую материнскую плату, именно сейчас их нужно снять. Поместите эти высокочувствительные устройства в подходящий антистатический контейнер и не вынимайте их до переустановки.
6. Открутите удерживающие материнскую плату шурупы и отложите их.
7. Снимите материнскую плату и поместите ее (стороной со смонтированными компонентами вверх) на антистатический коврик или в антистатический пакет — этим вы убережете ее от случайного повреждения электростатическим разрядом.
8. Если вы собираетесь хранить старую серверную плату в течение длительного времени, снимите резервный аккумулятор, положите его в плотный пластиковый пакет и прикрепите к антистатическому пакету с материнской платой.
9. Возможно, вам придется дополнительно снять и сохранить антиэлектромагнитный уплотнитель, который закрывает коннекторы ввода/вывода на плате (возможно, что на новой материнской плате будет предусмотрено новое защитное средство).

Примечание

Возможно, перед выполнением рассматриваемых действий вы посчитаете необходимым осуществить полное резервирование данных сервера на магнитной ленте — это рекомендуется делать перед любым серьезным обновлением компьютера. Изменения в оборудовании контроллера дисковода и других основных компонентов материнской платы иногда приводят к непредсказуемой работе системы, результатом которой может стать случайная потеря данных.

Установка платы

Теперь самое время устанавливать новую материнскую плату. При установке новой платы следует соблюдать предельную осторожность, чтобы не поцарапать ее поверхность. При работе на высоких скоростях передачи сигналов даже незначительные царапины могут снизить надежность сигналов. Серьезные царапины могут привести

к поломке новой материнской платы. В большинстве случаев сначала нужно установить материнскую плату, а затем — память и процессор; только после этого можно приступать к настройке системы. Монтаж материнской платы осуществляется следующим образом:

1. Возможно, на задней стороне корпуса потребуется установить антиэлектромагнитный уплотнитель — он поможет подогнать расположение портов ввода/вывода на вашей новой материнской плате.
2. Зафиксируйте новую материнскую плату в корпусе и проверьте, чтобы все крепежные отверстия были расположены на одной линии. Не продолжайте установку, пока не будут выверены все крепежные отверстия.
3. Вставьте шурупы в крепежные отверстия и в соответствующие гнезда на материнской плате. Надежно установите плату, а затем аккуратно закрутите все шурупы (не закручивайте шурупы слишком туго).
4. Подсоедините 20-контактный кабель питания ATX к соответствующему разъему питания на материнской плате.
5. Подсоедините к серверной плате все внутренние и внешние кабели и установите новый аккумулятор, чтобы сохранить конфигурационные данные материнской платы. При подключении кабелей обязательно проверьте соответствие контакта 1 кабеля и разъема (красная или синяя полоса на одной стороне кабеля всегда обозначает контакт 1).
6. Переустановите все платы расширения и закрепите их винтами на корпусе.
7. Подключите к платам расширения все внутренние и внешние кабели.

Примечание

Тщательно проверьте правильность крепежа всех шурупов на материнской плате. Плохо зафиксированные шурупы могут упасть на схему под напряжением или в вентилятор, что приведет к серьезным неисправностям системы.

Установка/замена периферийных устройств

Сетевые серверы, как правило, работают на базе быстрых процессоров и больших объемов памяти. После монтажа новой материнской платы вам нужно будет установить устройства памяти и хотя бы один процессор; только после этого можно будет включать питание сервера и выполнять его настройку. Обязательно следите за тем, чтобы при манипуляциях с внутренними компонентами сервера его питание было отключено, а шнур питания отсоединен.

Память

Память зачастую устанавливается в форме модулей DIMM, а типичная серверная материнская плата поддерживает до 4 модулей оперативной памяти SDRAM общей емкостью 1 Гбайт или более в разъемах DIMM (т. е. четыре DIMM-модуля по 256 Мбайт), как показано на рис. 9.6. На некоторых серверах используются модули памяти RDRAM в разъемах RIMM. Эта часть настоящей главы посвящена более распространенной архитектуре DIMM, так что пользователям RIMM следует обра-

титься за инструкциями к документации материнской платы. Так как вам может понадобиться обновить память в существующей конфигурации, для начала мы рассмотрим процесс снятия модулей DIMM.

Примечание

Память в высшей степени подвержена негативному воздействию электростатических разрядов. При работе с DIMM необходимо предпринимать все меры предосторожности.

1. Откройте корпус сервера и определите местонахождение разъемов DIMM.
2. Осторожно отогните пластиковые рычаги фиксирующего устройства и извлеките нужный модуль DIMM из разъема.
3. Держите модуль DIMM только за края (не дотрагивайтесь до его компонентов и золотистых краевых коннекторов) и аккуратно выньте его из разъема. Положите модуль DIMM в антистатическую упаковку.
4. При необходимости извлечения других модулей DIMM повторите перечисленные операции.

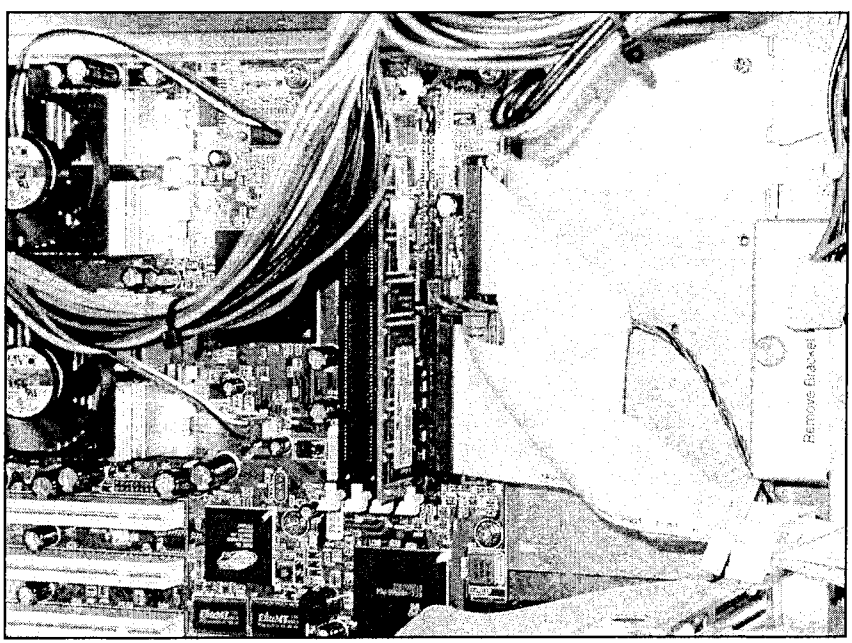


Рис. 9.6. Серверы могут поддерживать 1–2 Гбайт оперативной памяти в форме модулей DIMM или RIMM

Обратитесь к документации материнской платы и выберите один или несколько модулей DIMM, которые смогли бы обеспечить достаточный объем памяти для сервера. DIMM следует выбирать исходя из их емкости (например, 128 Мбайт), типа памяти (например, SDRAM), скорости (например, длительность цикла может быть

равна 8 нс) и корректировки ошибок (т. е. четность, нечетность, наличие или отсутствие корректирующего кода).

Примечание

Коннекторы в модулях DIMM и разъемах могут быть покрыты золотом или оловом, но смешение различных металлов (например, DIMM с золотыми контактами и разъем DIMM с оловянными контактами) впоследствии может привести к сбоям в работе памяти, результатом чего может стать потеря данных. Устанавливайте модули DIMM с позолоченными краевыми соединителями в позолоченные разъемы.

Теперь рассмотрим процесс установки DIMM:

1. Откройте корпус сервера и определите местонахождение разъемов DIMM.
2. Держите модуль DIMM только за края, извлеките его из антистатической упаковки.
3. Направьте модуль DIMM таким образом, чтобы два паза на его нижней грани располагалась по одной линии со шплинтами в разъеме.
4. Вставьте нижнюю сторону модуля DIMM в разъем и с усилием прижмите, пока он не будет правильно и полностью установлен в разъеме.
5. Аккуратно нажмите на пластиковые рычаги фиксирующего устройства на обоих концах разъема, зафиксировав их в закрытом положении.
6. При необходимости установки дополнительных модулей DIMM повторите перечисленные операции.

Примечание

При установке и извлечении модуля DIMM следует соблюдать предельную осторожность — чрезмерное давление может повредить разъем (и испортить материнскую плату). Усилий при манипуляциях с пластиковыми рычагами фиксирующего устройства нужно прилагать ровно столько, чтобы извлечь или зафиксировать модуль DIMM. Модули DIMM устроены таким образом, что их установка возможна только одним способом.

Процессор

Как правило, на материнской плате размещаются два или четыре процессора (хотя их может быть и больше). К примеру, наш сервер Gateway 7400 обеспечивает поддержку двух процессоров (рис. 9.7), в то время как версия Gateway 8400 способна разместить до четырех. К каждому устанавливаемому процессору нужно подключить подходящий радиатор/вентилятор, а в незанятых разъемах под процессоры должны стоять заглушки. Обратитесь к документации серверной материнской платы, чтобы уточнить тип и скорость совместимых с ней процессоров (например, один или два процессора Pentium III с частотой 800 МГц). При установке второго процессора обязательно убедитесь в том, что он совместим с уже существующим (включая, если это необходимо, производственную версию процессора).

Примечание

Процессоры крайне подвержены негативному действию электростатических разрядов. При работе с процессором следует предпринимать все меры предосторожности.

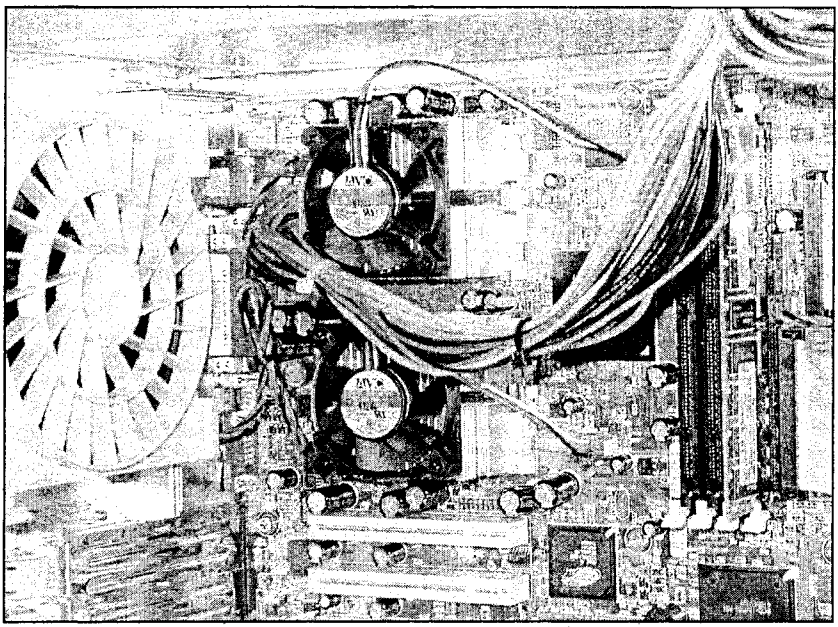


Рис. 9.7. Gateway 7400 обеспечивает поддержку двух процессоров Socket 370

Для начала рассмотрим, как правильно извлечь процессор.

1. Откройте корпус сервера и определите местонахождение разъема процессора.

Примечание

Если сервер недавно находился в рабочем состоянии, любой установленный на нем процессор и радиатор материнской платы будут горячими. Чтобы избежать возможных ожогов, перед выполнением манипуляций с процессорами следует подождать минимум 15 мин. после выключения системы.

2. Если на выбранном процессоре есть радиатор/вентилятор, отсоедините провод питания от его коннектора на серверной материнской плате:
   - При работе со слотовым процессором левой рукой отогните рычаг механизма фиксации так, чтобы процессор можно было вынуть из разъема. Правой рукой возьмите процессор со стороны, ближайшей к рычагу механизма фиксации, который вы отогнули, и выверните одну сторону процессора из разъема. Когда эта сторона будет извлечена, можно приступать ко второй. Возможно, сделать это будет трудно. Отгибайте рычаг механизма фиксации ровно настолько, чтобы освободить процессор из механизма фиксации.
   - Что касается сокетных процессоров, необходимо определить местоположение и освободить ZIF-рычаг (Zero Insertion Force — нулевое усилие установки), а затем установить его в крайнее вертикальное положение. Возможно, для того чтобы извлечь процессор из разъема, вам придется слегка раскачать его. Не пытайтесь извлечь процессор только с одной стороны — в результате контакты могут согнуться, что приведет к повреждению процессора.

3. Извлеките процессор и поместите его в антистатический пакет или коробку.
4. Выберите один или несколько процессоров, совместимых с вашей материнской платой, и убедитесь, что их радиаторы/вентиляторы установлены правильно.
5. Определите местоположение соответствующих разъемов под сокетные и слотовые процессоры, а также небольших коннекторов для вентиляторов рядом с каждым разъемом. Практически все современные серверные материнские платы способны автоматически определить процессор, задать скорость шины, множитель и напряжение процессора. Это означает, что для подготовки материнской платы к установке новых процессоров вам лишь нужно иногда установить перемычки.

Примечание

Как правило, для корректной работы системы необходимо устанавливать заглушки во все незанятые разъемы под процессоры Заглушка содержит схему терминирования AGTL+ и терминирования синхронизации. Если во всех незанятых разъемах под процессоры не будут установлены заглушки, то сервер может не загрузиться.

Теперь рассмотрим основные этапы установки процессора.

1. Откройте корпус сервера и определите местонахождение разъемов под процессоры.
   - Если на сервере уже установлен один процессор, а вы хотите разместить второй, необходимо удалить заглушку из этого разъема. Осторожно отогните рычаг механизма фиксации так, чтобы можно было вытащить заглушку из разъема. Возьмите заглушку за ближайшую к рычагу механизма фиксации сторону и вращательным движением извлеките ее из разъема. После этого выньте всю заглушку.
   - Если вам нужно заменить уже существующий процессор, оставьте заглушку в незанятом разъеме. Извлеките процессор, который хотите заменить.
   - Если на сервере установлено два процессора, причем и тот и другой планируется заменить, извлеките их.
2. Достаньте новый процессор из антистатической упаковки и сориентируйте его по отношению к разъему, причем особое внимание следует уделить выравниванию контакта 1.
3. При работе со слотовыми процессорами их нужно установить в механизм фиксации. Равномерно нажмите на обе стороны процессора, пока он не встанет в разъем со щелчком.
4. Если же речь идет о сокетном процессоре, полностью зафиксируйте его в разъеме, затем закройте и зафиксируйте ZIF-рычаг.

Примечание

Фиксирующие механизмы GRM (Grounded Retention Mechanism — закрепленный на плате механизм фиксации) несовместимы с компоновкой процессора типа SECC — новые GRM поддерживают только процессоры типа SECC2 (т. е. Pentium II/III Xeon) Если вы планируете использовать процессоры типа SECC (т. е. обычные Pentium II/III), нужно использовать механизм фиксации URM (Universal Retention Mechanism — универсальный механизм фиксации).

5. Подключите кабель питания вентилятора к трехконтактному соединителю на серверной плате.
6. Закройте корпус сервера, зафиксируйте крышку корпуса и убедитесь в том, что все индикаторы проникновения в корпус не активны.
7. Подсоедините все оставшиеся внешние кабели и подключите шнур питания.
8. Включите монитор и затем питание сервера. Запустите процедуру настройки сервера, чтобы выполнить настройку новой материнской платы, памяти и процессора (процессоров).

Конфигурирование материнской платы

После установки материнской платы, процессоров и памяти на сервере необходимо выполнить конфигурирование материнской платы в условиях нового аппаратного обеспечения. Как правило, конфигурирование сервера подразумевает установку перемычек материнской платы, запуск процедуры Setup для настройки параметров CMOS и исполнение всех прочих утилит, необходимых для настройки сервера в сетевом окружении.

Установка перемычек

В современных материнских платах количество применяемых перемычек ("джамперов", Jumper) сравнительно невелико — большая часть конфигурирования сервера выполняется с помощью настройки параметров CMOS и других программных средств. Впрочем, те немногие перемычки, которые есть на вашей материнской плате, связаны с основными вопросами обеспечения безопасности (т. е. очистка пароля, проникновение в корпус и т. д.). Расположение и назначение каждой перемычки подробно описаны в документации к серверной материнской плате. Если рассматривать плату Intel L440GX+ (рис. 9.8), важно получить представление о девяти наиболее важных перемычках.

- Разрешение записи в BIOS (BIOS WR EN, BIOS Write Enable). Эта перемычка защищает блок начальной загрузки BIOS. Если эта перемычка установлена, блок защищен и не может быть перезаписан (это положение также называется "защита от записи"). При отсутствии этой перемычки BIOS можно стереть и перепрограммировать. Учтите, что перемычка защищает только BIOS материнской платы, а не микропрограммные средства BMC.
- Обновление микропрограммных средств BMC (BMC FRC UP, BMC Firmware Upgrade). Эта перемычка контролирует цикл загрузки сервера. В состоянии по умолчанию сервер загружается в обычном режиме. В программном состоянии сервер пытается считать данные с гибкого диска, чтобы обновить программно-аппаратные средства BMC. Установка этой перемычки должна производиться совместно с перемычкой BMC WR EN. Учтите, что такая установка перемычек делает возможным перепрограммирование только микропрограммного обеспечения BMC, но не BIOS материнской платы.
- Разрешение записи в BMC (BMC WR EN, BMC Write Enable). Эта перемычка защищает блок начальной загрузки микропрограммных средств BMC. Когда она установлена, этот блок защищен и не может быть перезаписан (это положение

также называется "защита от записи"). Когда перемычка не установлена, микропрограммные средства BMC можно стирать и перепрограммировать. Учтите, что эта перемычка защищает только микропрограммные средства BMC, но не BIOS материнской платы.

- Очистка CMOS (CMOS CLR, Clear the CMOS). Эта перемычка защищает содержимое оперативной памяти CMOS. В защищенном режиме, принимаемом по умолчанию, содержимое оперативной памяти CMOS защищено (хотя его можно обновить с помощью процедуры настройки параметров CMOS). В незащищенном режиме система использует заводские установки оперативной памяти CMOS. Эта функция особенно полезна при восстановлении сервера после замены резервного аккумулятора или в случае неправильного изменения настроек.

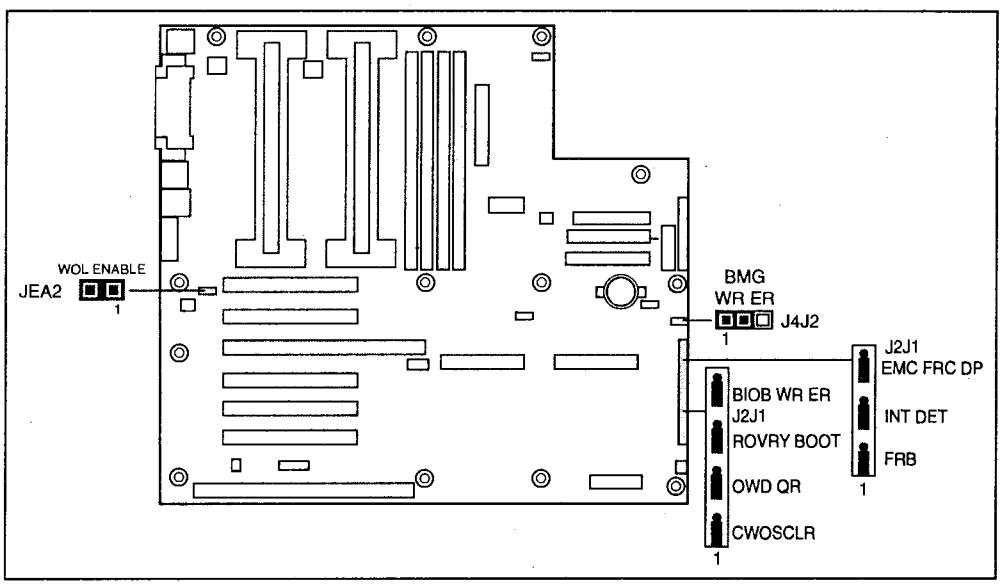


Рис. 9.8. Расположение перемычек на серверной материнской плате (публикуется с разрешения Intel Corporation)

- Отказобезопасная загрузка (Fault Resilient Booting, FRB — загрузка с амортизацией отказов). Эта перемычка отвечает за функцию FRB материнской платы. При включенном режиме FRB, если процессор 0 (процессор по умолчанию) не отвечает, система загружается с процессора 1. При отключенном режиме FRB в случае, если процессор 0 не отвечает, система загружаться не будет.
- Обнаружение проникновения (INT DET, Intrusion Detection). Если эта перемычка установлена, датчик, расположенный на корпусе, отправляет сигнал на сервер при снятии крышки корпуса (в результате сетевой администратор получает предупреждение об опасности). Если эта функция отключена, показания датчика игнорируются, и при снятии крышки корпуса предупреждение не отправляется.
- Очистка пароля (PSWD CLR, Clear the Password). В защитном режиме, устанавливаемом по умолчанию, система сохраняет текущий системный пароль (если он

определен). В режиме стирания система очистит этот пароль. Эта функция особенно полезна, если вы забыли системный пароль или установили его неправильно.

- Загрузка с восстановлением (RCVRY BOOT, Recovery Boot). Эта перемычка отвечает за цикл загрузки системы. В нормальном режиме, принимаемом по умолчанию, система пытается загрузиться с помощью BIOS, хранящейся во флэш-памяти. Если перемычка стоит в режиме восстановления, BIOS пытается выполнить загрузку с восстановлением, загружая код BIOS с гибкого диска на флэш-устройство. Как правило, эта функция используется в случаях, когда код BIOS материнской платы поврежден или нуждается в обновлении. Учтите, что эта перемычка отвечает только за BIOS материнской платы и к микропрограммным средствам BMC отношения не имеет.
- Разрешение активизации по сети (WOL EN, Wake On LAN Enable). Эта перемычка включает/отключает поддержку функции Wake On LAN материнской платы. Если материнская плата получает достаточное резервное электропитание (т. е. +5 В@0,8А через шину резервного питания) для поддержки функции Wake On LAN, вы имеете возможность включить эту функцию (она включена по умолчанию). В противном случае ее необходимо отключить.

Примечание

Практически во всех случаях перед изменением положения перемычки сервер следует выключать и отключить шнур питания После использования соответствующих функций (например, после очистки системного пароля) большинство перемычек необходимо возвращать в исходные (принимаемые по умолчанию) положения

Самотестирование при включении питания

Каждый раз, когда вы загружаете (или перезагружаете) сервер, из BIOS материнской платы запускается программа самотестирования по включению питания (Power-On Self Test, POST). Как правило, POST выполняет проверку серверной платы, установленных процессоров, памяти, клавиатуры и большинства установленных периферийных устройств. Во время проверки памяти POST отображает данные об объеме памяти, к которой она способна обратиться и которую способна протестировать (время, необходимое для тестирования памяти, зависит от ее объема в системе). Если в материнской плате, процессорах, памяти или других установленных устройствах обнаруживается неисправность, POST создает сообщение об ошибке. Нормальный процесс POST проходит приблизительно следующим образом.

1. Включите монитор и сервер. Через мгновение произойдет запуск POST и начнется подсчет памяти.
2. По окончании подсчета памяти на экран выводятся сообщения типа:

```
Press F2 key if you want to run SETUP (Нажмите <F2>, чтобы запустить
SETUP)
Keyboard...Detected          (Клавиатура...обнаружена)
Mouse...Detected             (Мышь...обнаружена)
```

3. Если, как в нашем примере, вы нажмете клавишу <F2>, произойдет запуск процедуры установки системных параметров CMOS Setup. В других материнских

платах и версиях BIOS могут использоваться другие клавиши, но они в любом случае будут обозначаться в сообщении.

4. Если вы не нажмете клавишу запуска установки параметров CMOS, исполнение POST завершится, и программа передаст управление операционной системе. Если у вас нет устройства (дисковода) для загрузки операционной системы, вышеуказанное сообщение будет оставаться на экране в течение нескольких секунд, пока продолжается процесс загрузки, а затем система даст один звуковой сигнал. Вы увидите сообщение типа:

```
Operating system not found
(Операционная система не обнаружена)
```

5. Когда операционная система найдена, процесс загрузки продолжается. Если на вашей материнской плате есть интегрированный хост-адаптер SCSI, возможно, вы увидите другие сообщения BIOS типа:

```
Press <Ctrl><A> to enter SCSI Utility
(Нажмите <Ctrl>+<A>, чтобы запустить утилиту SCSI)
```

6. Если, как в предыдущем примере, нажать комбинацию клавиш <Ctrl>+<A>, произойдет запуск программы настройки контроллера SCSI. В других материнских платах и версиях BIOS могут использоваться иные клавиши, но они в любом случае будут обозначены в сообщении. Если на сервере установлены устройства SCSI, программу SCSI нужно запустить. После ее запуска следуйте инструкциям на экране, чтобы произвести конфигурирование встроенного хост-адаптера SCSI и устройств на основе этого интерфейса. Если не запускать утилиту SCSI, процесс загрузки продолжится в нормальном режиме.
7. Нажмите клавишу <Esc> во время исполнения POST, чтобы после завершения этой программы открыть меню загрузки — в нем можно будет выбрать загрузочное устройство (т. е. диск C: или D:) или запустить настройку параметров CMOS.
8. После завершения цикла POST система дает один звуковой сигнал.
9. Теперь на экране появляется логотип операционной системы, и она начинает загружаться.

Примечание

Если система останавливается до завершения POST, динамик подает сигнал, указывающий на фатальную системную ошибку, которая требует незамедлительного внимания. Если POST инициализировала видеосистему, возможно, вы увидите сообщение на мониторе (а система может подать два звуковых сигнала). Зафиксируйте все звуковые или текстовые сообщения об ошибках.

Настройка параметров CMOS

Процедура настройки параметров CMOS Setup является компонентом BIOS материнской платы, и многие переменные, которые определяют конфигурацию системы, хранятся в оперативной памяти CMOS, работающей от аккумулятора, или во флэш-памяти. Запускать процедуру настройки параметров CMOS (иногда она называется BIOS Setup или просто Setup) нужно при модернизации серверной материнской

платы, замене резервного аккумулятора и других аппаратных изменениях, которые должны определяться на уровне аппаратного обеспечения системы. В документации системы, как правило, приводится подборка общих настроек. Ниже перечислено лишь несколько причин, по которым вам потребуется запустить процедуру настройки параметров CMOS:

- идентификация дисковода гибких дисков;
- выбор режима параллельного порта;
- включение и выключение последовательного порта;
- установка времени и даты;
- конфигурация жесткого диска на основе IDE (т. е. цилиндры, секторы, головки и т. д.);
- определение последовательности загрузочных устройств;
- включение SCSI BIOS (и хост-контроллера SCSI);
- установка скорости процессора;
- включение или выключение режима энергосбережения.

Примечание

Если значения, хранящиеся в оперативной памяти CMOS, не согласуются с аппаратным обеспечением, которое обнаруживает POST (уже после очистки оперативной памяти CMOS), появляется сообщение об ошибке. Во многих случаях можно либо повторно войти в CMOS, чтобы исправить ошибку, либо воспользоваться перемычкой очистки CMOS для восстановления заводских значений по умолчанию.

Утилита установки системы

Процедура настройки параметров CMOS материнской платы чрезвычайно важна для конфигурирования низкоуровневого аппаратного обеспечения сервера, но есть несколько важных пунктов, которые CMOS не затрагивает. Вместе с материнскими платами (типа L440GX+) поставляется утилита установки системы SSU на компакт-диске. Утилита установки системы обеспечивает высокоуровневую настройку сервера. К примеру, SSU распределяет ресурсы между устройствами на материнской плате и платами расширения до загрузки операционной системы. Она позволяет определить последовательность загрузочных устройств и настройки защиты системы вне установки параметров CMOS. Утилита установки системы предоставляет возможность просмотра (и чистки) журнала системных событий и обеспечивает представление на системном уровне устройств ввода/вывода сервера. Более того, в случае отказа операционной системы утилита установки системы позволяет осуществить поиск и устранение неисправностей на сервере. К помощи этой утилиты следует обращаться, если вам нужно:

- добавить или удалить платы, влияющие на распределение ресурсов, т. е. портов, памяти, IRQ или DMA;
- изменить последовательность загрузочных устройств сервера или настройки безопасности;
- изменить настройки сервера;

- сохранить настройки сервера;
- просмотреть или очистить журнал системных событий.

Традиционные устройства и устройства Plug-and-Play[1]

Утилита установки системы SSU должна соответствовать техническим условиям ISA устройств типа Plug-and-Play (PnP) — утилита установки системы взаимодействует с любыми соответствующими конфигурационными файлами (CFG) от производителей периферийных устройств. Как правило, при добавлении и удалении устройств ISA/PCI PnP запускать утилиту установки системы не нужно, однако при установке и извлечении традиционного ("унаследованного", Legacy) устройства ISA необходимо выполнить утилиту установки системы для настройки сервера.

Самотестирование при включении питания (POST) сопоставляет данные о конфигурации системы и фактическую конфигурацию аппаратного обеспечения. Если эти две конфигурации не согласуются, POST генерирует сообщение об ошибке. После ее появления вы должны запустить утилиту SSU, чтобы определить правильную конфигурацию до загрузки сервера. Утилита SSU позволяет задать настройки системы с помощью данных, содержащихся в файлах CFG, регистрах конфигурации, флэш-памяти; кроме того, вы имеете возможность ввести любую информацию вручную. SSU записывает эти данные во флэш-память. Изменения в конфигурации произойдут при загрузке сервера. SSU всегда сопровождает конфигурационные данные контрольной суммой, чтобы BIOS мог выявить любое потенциальное повреждение данных еще до проведения фактической настройки аппаратного обеспечения.

Запуск утилиты SSU

В большинстве случаев утилиту SSU можно запускать непосредственно с сопровождающего системную плату компакт-диска с ресурсами сервера; для этого следует запустить серверную систему с компакт-диска и выбрать **Utilities**. Запуск файла SSU.BAT на компакт-диске с ресурсами сервера запускает SSU (если сервер загружается непосредственно с носителя SSU, файл SSU.BAT исполняется автоматически). Когда SSU запускается в режиме локального исполнения (этот режим применяется по умолчанию), она принимает входные данные с клавиатуры и/или с мыши и выводит на основной монитор свой элементарный графический интерфейс пользователя (Graphical User Interface, GUI).

Примечание

Утилита SSU запускается с перезаписываемых, неперезаписываемых, съемных и несъемных носителей. Если запуск SSU производится с неперезаписываемого носителя (т. е. с привода компакт-дисков), пользовательские настройки сохранить нельзя.

---

[1] Принцип и спецификация быстрого подключения к компьютеру дополнительного оборудования и самостоятельного конфигурирования системы, поддерживаемая современными BIOS, операционными системами и аппаратными средствами. Операционная система обнаруживает вновь подключенное устройство, опрашивает его, оценивает предъявляемые им требования к системе, определяет и выполняет оптимальные установки для каждого устройства. — *Ред.*

SSU можно запускать удаленным методом с удаленного сервера, оборудованного платой SMM (Server Monitor Module — модуль контроля сервера) и локальной системой с программным обеспечением дистанционного управления. Плата SMM (т. е. LANDesk 2) предусматривает поддержку видеопамяти, клавиатуры и мыши для удаленного сервера, а соединение с ним устанавливается либо через модем, либо по каналу Ethernet. Так как SSU в таком случае будет работать исключительно на удаленном сервере, все файлы, необходимые для запуска этой утилиты, также должны присутствовать на нем (обычно они размещаются на съемном или несъемном носителе).

Процессоры

Процессор (другие названия: микропроцессор, центральный процессор) — это самый важный компонент компьютера. Это мощное программируемое логическое устройство обрабатывает все команды программ (и значительную часть данных) в системе, включая модули, приложения и файлы данных Windows. Специалисту необходимо разбираться в некоторых важнейших вопросах, связанных с процессорной технологией и ее реализацией в условиях настольного компьютера или сервера.

- *Производительность системы.* Отдельно взятый процессор, вероятно, является наиболее значительным фактором, определяющим производительность системы. Другие компоненты (память, набор микросхем, контроллер дисководов, сетевой адаптер и др.), несомненно, тоже влияют на общую производительность, но именно возможности процессора определяют результативность исполнения программных команд.
- *Поддержка программного обеспечения.* Процессор может работать только с определенным набором инструкций. К примеру, процессоры Intel и AMD, как правило, работают с программными продуктами типа x86 — DOS, Windows и Linux/UNIX, а программы другого типа не исполняются. Современные процессоры, обеспечивающие поддержку расширений инструкций типа MMX, 3DNow! и SME, работают с программным обеспечением, созданным с учетом этих специальных возможностей.
- *Надежность и стабильность.* Качество и конструктивная целостность процессора определяют надежность работы вашей системы (возможно, вы помните известный дефект первых процессоров Pentium). Функциональная надежность процессора зависит также от возраста процессора и степени потребления им энергии.
- *Потребление энергии и охлаждение.* Старые процессоры потребляли немного энергии (в сравнении с другими системными устройствами), но современные модели Pentium 4 или Xeon потребляют достаточно много энергии. Потребление энергии влияет на охлаждение системы и ее общую надежность.
- *Поддержка материнской платы.* Современным процессорам требуется всесторонняя поддержка со стороны BIOS и чипсета материнской платы. Это значит, что материнскую плату следует выбирать исходя из того, какими процессорами вы собираетесь пользоваться.

Понятие микросхемы

Как правило, знание основных физических характеристик микросхемы процессора оказывается полезным. Вопросы, связанные с проектированием и производством

самой физической микросхемы (Chip — кристалл), оказывают непосредственное влияние на ее размер, производительность, энергопотребление и тепловыделение. В конечном итоге все эти свойства влияют на применение процессора в системе.

Версии и спецификации

Процессор характеризуется крайне сложной конструкцией. Как и при проектировании любых других устройств, зачастую в процессорах обнаруживаются дефекты (например, дефект операций с плавающей точкой в первых процессорах Pentium). Это означает, что может существовать множество вариантов конструкции одного и того же процессора, причем в новых версиях исправляются дефекты более старых. В компании Intel для обозначения версии процессора употребляется термин *stepping* (пошаговое изменение), или S-step для обозначения спецификации процессора, которая, как правило, отмечается прямо на процессоре. Для обозначения версии процессора компания AMD использует номер модели. К примеру, процессор Intel Pentium III поздней модели может быть отмечен спецификацией SL3WA. Вам не нужно уметь определять характеристики спецификации процессора (или других маркировок версии процессора), т. к. это можно сделать по таблице производителя, в которой даны характеристики процессоров различных спецификаций.

Примечание

В большинстве случаев в более поздних версиях процессора не добавляют новые функции. В них лишь устраняются дефекты предыдущих версий и улучшаются параметры производительности.

В основном, спецификация процессора практически не влияет на производительность системы, но иногда это возможно. Сбой может произойти при использовании определенных версий процессоров с определенным сочетанием материнской платы и BIOS. Столкнувшись с трудностями, связанными с надежностью системы, обратитесь к производителю вашей материнской платы за объяснением возможных причин, связанных с версией вашего процессора. Кроме того, при использовании нескольких процессоров на одной материнской плате может оказаться важной совместимость версий процессоров.

Энергоснабжение и управление процессором

Процессоры потребляют довольно много электроэнергии. Для снижения потребности компьютера в электроэнергии и улучшения его производительности, традиционные +5 В рабочие напряжения прошлых лет уступили место гораздо более низким напряжениям, на которых теперь работают процессоры, вспомогательные микросхемы и устройства расширения. Первым этапом было снижение уровня рабочего напряжения до +3,3 В в более ранних процессорах Pentium. Современные процессоры еще больше понижают уровень напряжения, пользуясь схемой двойного напряжения (Dual voltage), или двойной шины питания (Split rail). Процессор такого типа использует два разных напряжения. Внешнее напряжение (или напряжение ввода/вывода), как правило, составляет +3,3 В и этим обеспечивается совместимость с другими микросхемами на материнской плате. Напряжение ядра (или опорное) несколько ниже (обычно оно составляет от +2,5 до +2,9 В, но последние модели процессоров работают уже с напряжением от +1,5 В). Напряжение ввода/вывода позволяет процессору взаимодействовать с материнской платой, в то время как на-

пряжение ядра предоставляет ему возможность непосредственно запускать собственный вентилятор.

Традиционно для определения нужного рабочего напряжения для конкретного процессора требовалось установить одну или несколько перемычек регулировки напряжения на материнской плате. Сегодня напряжения процессора устанавливаются автоматически — посредством сигналов выбора напряжения в самом процессоре; вам остается лишь подключить процессор и загрузить компьютер.

Так как энергопотребление процессора связано с его быстродействием и внутренней активностью, компания Intel разработала схему управления электропитанием, которая позволяет процессорам осуществлять сохранение энергии (тем самым увеличивая срок действия аккумулятора в портативных системах). Исходно управление электропитанием было реализовано в процессоре Intel 486SL (модернизированная версия процессора 486DX), но вскоре функции управления электропитанием были стандартизованы и внедрены во все процессоры линейки Pentium и последующие процессоры. Эти функции организованы в режиме системного управления (System Management Mode, SMM). Схема SMM интегрирована в физическую микросхему процессора, но работает независимо, и это позволяет ей контролировать энергопотребление процессора исходя из уровня его активности. SMM предоставляет системе возможность определения периодов времени, после которых питание процессора частично или полностью отключается. Кроме того, эта схема задействует функцию приостановки/возобновления, которая поддерживает современные режимы ожидания и спящий режим. Как правило, настройки SMM задаются в процедуре настройки параметров CMOS.

Охлаждение процессора

Миллионы транзисторов, работающих внутри процессора, выделяют небольшой объем тепла при каждом включении и выключении. В условиях, когда такие переключения происходят сотни миллионов раз каждую секунду, тепловыделение (и управление им) становится серьезной проблемой. Процессоры имеют предопределенный температурный диапазон, который отражает допустимые пределы изменения температуры при нормальной работе. Если процессор перегревается, как правило, это приводит к серьезным сбоям в работе системы: к произвольной перегрузке системы, ее зависанию или к полным отказам. Признаками того, что процессор перегрелся, могут стать ошибки памяти, ошибки приложений, проблемы с дисками и многое другое. Сильно (или многократно) перегретый процессор может и совсем выйти из строя, хотя это случается редко. Неисправности такого типа обычно очень сложно диагностировать, потому что зачастую они затрагивают другие компоненты системы. К примеру, полный отказ системы или ее зависание обычно ассоциируется с программной ошибкой или аппаратным конфликтом, но не с перегревом процессора.

Процессоры охлаждаются с помощью активных теплоотводов — быстрых вентиляторов, установленных на большом металлическом радиаторе со множеством ребер. Радиатор отводит тепло от процессора, а вентилятор в свою очередь охлаждает радиатор. Воздух, нагретый радиатором, выходит из корпуса (это тот самый теплый воздух, который вы можете почувствовать, если поднесете руку к задней стенке корпуса). Слабой стороной активных теплоотводов является то, что они зависят от вентилятора. Если вентилятор выйдет из строя, процессор перегреется очень быстро. Чтобы защитить процессор от случайного отказа вентилятора, на многих материн-

ских платах установлены тахометры, которые проверяют частоту вращения вентилятора, и термостаты, которые измеряют температуру корпуса процессора. Если вентилятор перестанет вращаться или температура процессора превысит предварительно установленный порог, специальное предупреждение обозначит неисправность и даст вам возможность заняться устранением этой проблемы еще до того, как произойдет сбой в работе системы или ее полный отказ.

Корпус процессора

Сами кристаллы (небольшая "матрица") не используются непосредственно — для этого они слишком хрупки и чувствительны. Кристалл помещается в защитный

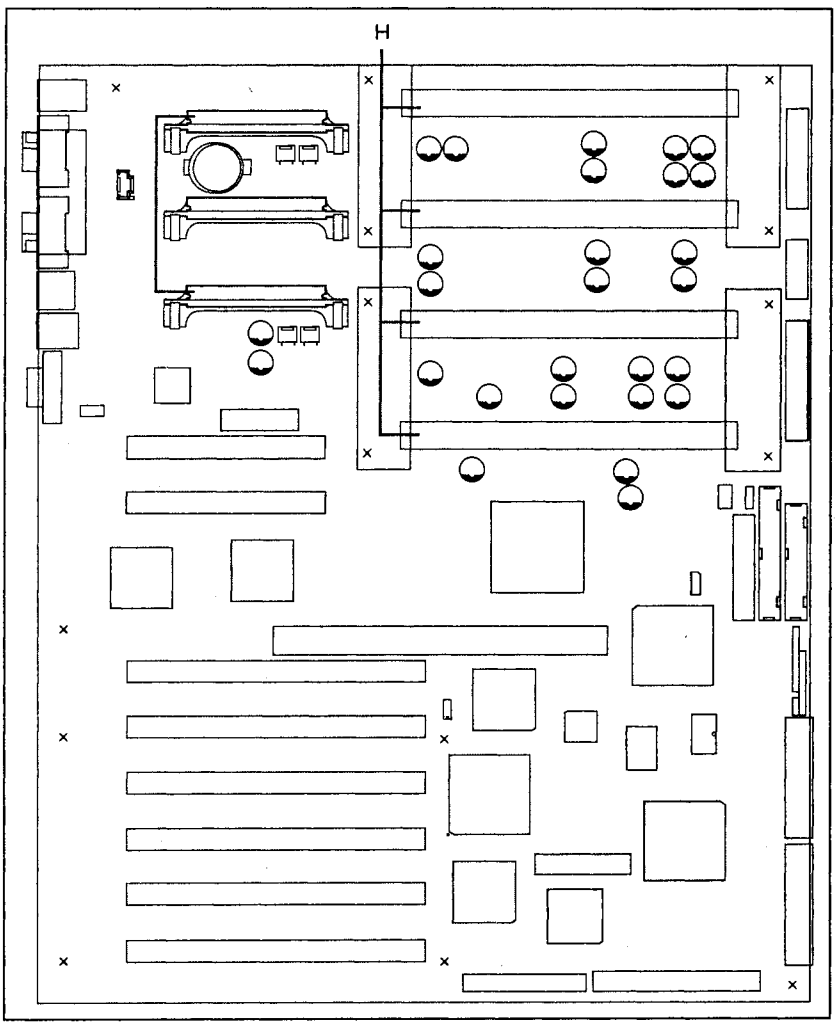


Рис. 9.9. Расположение процессоров на четырехпроцессорной серверной материнской плате Intel SKA4 (публикуется с разрешения Intel Corporation)

корпус, который помогает ему отводить тепло. Стандартный корпус, как правило, оформлен "под щелевой разъем" (слотовый) или "под квадратное гнездо" (сокетный). Слотовые процессоры обычно классифицируются по схеме: slot 1, slot 2 или slot A. Сокетные процессоры обозначаются как socket 370 или socket A. На рис. 9.9 изображены четыре коннектора slot 1 (элементы H) четырехпроцессорной серверной материнской платы Intel SKA4. Описание основных типов процессоров приводится ниже.

- Slot 1. Корпуса SEC (Single Edge Contact — односторонний краевой контакт) обычно предназначены для процессоров Pentium II и Pentium III компании Intel.
- Slot 2. Это немного более крупные корпуса SEC, предназначенные для процессоров Intel Pentium II/III Xeon, которые часто используются на серверных и многопроцессорных платформах.
- Slot A. Такие корпуса SEC (почти идентичные slot 1) используются для процессоров AMD Athlon.
- Socket 370. Эти 370-контактные корпуса применяются во многих процессорах Intel Celeron.
- Socket A. Эти 460-контактные корпуса (их иногда называют socket 460) применяются на процессорах AMD Athlon (Thunderbird) и Duron.
- Socket 423 и 478. Эти корпуса типа PGA (Pin Grid Array — корпус с матричным расположением контактов) применяются в современных процессорах Pentium 4.

О мультипроцессорной обработке

Многопроцессорная обработка — это методика работы системы с несколькими процессорами. Вы можете удвоить производительность системы с помощью двух процессоров вместо одного, увеличить производительность вчетверо — с помощью четырех процессоров и т. д. Практически это не всегда осуществимо, но в определенных условиях многопроцессорная обработка действительно может значительно повысить производительность. Чтобы эффективно использовать многопроцессорную обработку, на хосте должны присутствовать все нижеперечисленные элементы.

- *Поддержка со стороны материнской платы.* Вам нужна материнская плата, способная работать с несколькими процессорами. Это значит, что на ней должны быть разъемы для установки добавочных процессоров, а также набор микросхем, поддерживающих многопроцессорную конфигурацию.
- *Поддержка со стороны процессора.* Вам нужны процессоры, которые могут применяться в многопроцессорной системе. Для этого подходят не все процессоры; подобная конфигурация может состоять лишь из нескольких версий одного и того же процессора. За рекомендациями относительно выбора процессоров лучше всего обратиться к документации материнской платы.
- *Поддержка со стороны операционной системы.* Кроме того, вам нужна операционная система с поддержкой многопроцессорности, такая как Windows NT/2000 или UNIX. Другие операционные системы, в том числе Windows 98, не поддерживают многопроцессорность.

Многопроцессорная обработка наиболее эффективна в сочетании с прикладным программным обеспечением, разработанным в расчете именно на такую конфигура-

цию. Многопроцессорная обработка координируется операционной системой, которая распределяет различные задачи между процессорами в системе. Приложения, разработанные специально для многопроцессорной обработки, называются "поточными", т. к. они разбиты на отдельные подпрограммы, которые могут работать независимо друг от друга. В результате операционная система получает возможность запускать такие потоки одновременно на нескольких процессорах, и именно таким образом многопроцессорная обработка повышает производительность. Если приложение не предназначено для подобного применения, оно не может извлечь выгоду из наличия нескольких процессоров (при этом операционная система может воспользоваться дополнительными процессорами, если одновременно запущено несколько приложений).

Многопроцессорная обработка может быть *асимметричной* и *симметричной*. Эти термины обозначают то, как операционная система распределяет задачи между процессорами в системе. При асимметричной многопроцессорной обработке одни процессоры выполняют только системные задачи, а другие — только задачи приложений. Это жесткое распределение задач приводит к понижению производительности в случае, когда компьютеру необходимо выполнить больше системных задач, чем задач пользовательских (или наоборот). Симметричная многопроцессорная обработка (Symmetrical MultiProcessing, SMP) позволяет запускать любые системные и пользовательские задачи на любых процессорах. Это более гибкий метод, и поэтому при его использовании производительность повышается. Симметричная многопроцессорная обработка применяется на большинстве многопроцессорных материнских плат.

Чтобы процессор мог работать в многопроцессорной конфигурации, он должен поддерживать протокол многопроцессорной обработки, регулирующий процесс взаимодействия между процессорами и набором микросхем для реализации симметричной многопроцессорной обработки. В процессорах Intel, как правило, используется SMP-протокол под названием APIC, а наборы микросхем Intel, поддерживающие многопроцессорную обработку, сконструированы таким образом, что могут работать с такими кристаллами. APIC — это запатентованный стандарт Intel; поэтому хотя компании AMD и Cyrix могут производить Intel-совместимые процессоры, они не могут заставить их работать в конфигурациях SMP. AMD и Cyrix реализуют свой собственный SMP-стандарт под названием OpenPIC.

Режимы работы процессора

Процессоры способны работать в нескольких различных режимах. Термин *режим* обозначает способ (способы), с помощью которого процессор создает (и поддерживает) собственную рабочую среду. Режим процессора контролирует то, как процессор распознает и управляет системной памятью и ее задачами. Существует три различных режима работы процессора: реальный, защищенный и виртуально-реальный. Вам следует иметь хотя бы элементарные представления о каждом из них.

Реальный режим

Вначале компьютер типа IBM мог обращаться лишь к 1 Мбайт оперативного запоминающего устройства (ОЗУ). С тех пор каждый новый процессор должен был поддерживать режим, совместимый с кристаллом Intel 8088 — именно это называется

реальным режимом. Когда процессор работает в реальном режиме, он имеет преимущество в скорости, но его обращение к памяти ограничено возможностями кристалла 8088. Процессор может обратиться лишь к 1 Мбайт ОЗУ, что не позволяет воспользоваться 32-битовой обработкой, реализованной в современных процессорах. Все процессоры поддерживают реальный режим — компьютер обычно запускается именно в реальном режиме (DOS). Реальный режим применяется DOS и стандартными приложениями под DOS.

Защищенный режим

Начиная с IBM AT начал применяться новый режим работы процессора — *защищенный*. Этот режим обладает большими возможностями по сравнению с реальным, и он применяется во всех современных многозадачных операционных системах. У защищенного режима есть много преимуществ:

- защищенный режим обеспечивает полный доступ ко всей системной памяти (ограничения в 1 Мбайт для защищенного режима нет);
- защищенный режим может работать в многозадачной конфигурации, а это значит, что операционная система может управлять одновременным выполнением множества программ;
- защищенный режим обеспечивает поддержку виртуальной памяти, которая позволяет системе, используя жесткий диск, при необходимости эмулировать дополнительное системное ОЗУ;
- защищенный режим также предусматривает более быстрый (32-битовый) доступ к памяти, а также 32-битовые драйверы для обработки передач ввода/вывода.

Каждая работающая программа имеет выделенную ей память, что предотвращает конфликты с другими программами. Если программа пытается использовать адрес ячейки памяти, который ей не предоставлен, генерируется нарушение защиты. Все основные современные операционные системы, включая Windows 9x/ME, Windows NT/2000, OS/2 и Linux, используют защищенный режим. Даже DOS (система, которая обычно работает в реальном режиме) может обращаться к памяти в защищенном режиме с помощью интерфейса DPMI (DOS Protected Mode Interface — интерфейс защищенного режима DOS), что помогает играм под DOS превышать обычный для этой системы лимит памяти, который составляет 640 Кбайт. Процессоры 386 (и более поздние модели) могут сразу переключаться с реального на защищенный режим и обратно. Защищенный режим иногда называется расширенным режимом 386, т. к. повсеместное распространение он получил именно благодаря этому семейству процессоров.

Виртуально-реальный режим

Третий режим работы процессора фактически является усовершенствованной версией защищенного режима. Обычно защищенный режим применяется для работы с графическими многозадачными операционными системами типа Windows. Иногда в среде Windows возникает необходимость в запуске программ под DOS, но они могут работать только в реальном режиме, а защищенный режим для них не подходит. *Виртуально-реальный режим* был создан с целью разрешить именно эту проблему. В нем происходит эмуляция реального режима в защищенном режиме, что позволя-

ет работать программам DOS. Операционная система, работающая в защищенном режиме, типа Windows, на практике может создавать множество виртуальных машин, работающих в реальном режиме. Программное обеспечение, запущенное на такой виртуальной машине, рассматривает ее как единственную. Каждая виртуальная машина получает свое собственное адресное пространство емкостью в 1 Мбайт, образ реальных аппаратных процедур BIOS и т. д. Именно виртуально-реальный режим применяется в тех случаях, когда вы открываете окно DOS или запускаете игру DOS в среде Windows. При запуске приложения DOS Windows создает виртуальную машину DOS, в рамках которого оно будет исполняться.

Архитектура и производительность

За последние несколько лет произошел бурный рост технологий и методик, цель которых состоит в максимальном повышении производительности процессора. Проектировщики прилагали большие усилия к улучшению процессоров; сейчас, при запуске системы, мы считаем эти возможности процессоров обычными. В этой части главы описываются некоторые функции повышения производительности, использующиеся в современных микропроцессорах.

Суперскалярная архитектура

Команды программ обрабатываются с помощью схем, которые называются *исполнительным блоком*. Суперскалярная архитектура подразумевает применение нескольких таких схем, что позволяет процессору обрабатывать более одной команды одновременно. Это — форма многопроцессной обработки внутри процессора, когда одновременно происходит выполнение несколько команд. Большинство современных процессоров являются суперскалярными.

Организация суперконвейеров

Команды выполняются на конвейере, на каждой ступени которого осуществляется определенная их часть. Если конвейер сделать длиннее (т. е. добавить в него большее количество ступеней), на каждую стадию выполнения будет затрачено меньше усилий, и тактовую частоту процессора можно будет повысить. Этот принцип называется *суперконвейерной организацией* (superpipelining), и обычно он рассматривается как усовершенствование по отношению к организации обычных конвейеров.

Упреждающие исполнение команд и предсказание ветвлений

Некоторые процессоры могут исполнять несколько команд одновременно. Не все результаты исполнения команд будут использованы, т. к. изменения в ходе программы могут означать, что данная команда не будет исполняться в первую очередь. Это имеет место при ветвлении программы, когда происходит проверка условия и ход программы изменяется в зависимости от результатов. Ветвления являются серьезным препятствием при организации суперконвейера, т. к. нет уверенности в том, что команды будут поступать в линейной последовательности. Менее современный процессор может остановить конвейер, пока не станут известны результаты, и тем самым значительно снизить производительность. Более современные процессоры в любом случае упреждающе исполняют следующую команду. Предполагается, что

процессор сможет использовать результаты, если ветвление будет соответствовать предсказанию.

Самые современные процессоры сочетают этот принцип с предсказанием ветвления, при котором процессор фактически может предсказывать (причем довольно точно) направление ветвления, основываясь на предыстории. Предсказание ветвлений повышает эффективность обработки ветвлений за счет использования небольшого специального кэша под названием *целевого буфера ветвлений* (BTB, Branch Target Buffer). Когда процессор исполняет ветвь, информацию о ней он хранит в этой области. Если впоследствии процессор встречается с той же ветвью, он получает возможность делать обоснованные предположения о направлении этой ветви. Это помогает поддерживать на конвейере поток и повышает производительность.

Исполнение с изменением последовательности

Процессоры, которые пользуются несколькими исполнительными блоками, могут завершить обработку команд программы не по порядку. К примеру, команда 2 может быть выполнена еще до завершения команды 1. Такая универсальность повышает производительность, обеспечивая возможность исполнения команд с меньшим временем ожидания. Результаты исполнения перераспределяются в правильном порядке, что обеспечивает корректность исполнения программы. Обычно это делается блоком изъятия (стадия обработки команды в схеме процессора).

Переименование регистров и буферы записи

Переименование регистров — это метод обеспечения множественности выполняемых ветвей без конфликтов между различными исполнительными блоками, пытающимися использовать одни и те же регистры. Вместо одного набора регистров в процессор помещается несколько таких наборов. Это позволяет разным исполнительным блокам работать одновременно, не вызывая простоя конвейера. Буферы применяются для фиксации результатов исполнения команды до их записи в регистры или в ячейки памяти. Чем больше объем буфера, тем больше команд может выполняться без простоя конвейеров.

Контроль нагрева процессора

Тепло — злейший враг современного процессора, и поэтому контроль тепловыделения является важной задачей. Избежать проблем с перегревом процессора вам помогут следующие рекомендации.

- Применяйте высококачественный радиатор/вентилятор, соответствие которого вашему процессору должно быть выше среднего.
- Используйте тонкий слой термопасты, чтобы повысить интенсивность теплообмена между радиатором и процессором.
- Работая с очень горячими процессорами, старайтесь использовать модуль Пельтье (термоэлектрический охладитель) или подобный блок охлаждения.
- Выбирайте надежные вентиляторы на шарикоподшипниках с увеличенными сроками службы.

- Расположите кабели так, чтобы обеспечить свободную циркуляцию воздуха в нужных областях (например, поблизости от вентилятора процессора).
- Убедитесь в том, что радиатор/вентилятор процессора находится в близком контакте с поверхностью процессора (при необходимости можно использовать термопасту). Он должен быть прочно прикреплен к процессору или к процессору и разъему. Если это не так, купите новый радиатор/вентилятор.
- Пользуйтесь вентилятором с системой звуковой сигнализации, которая сможет предупредить вас в случае неисправности вентилятора или перегрева процессора.
- Если вы разгоняете свой процессор, поставьте более мощный радиатор/вентилятор или термоэлектрический охладитель Пельтье, чтобы компенсировать увеличенное тепловыделение.
- Хотя бы раз в год чистите лопасти вентилятора, его опорные стойки и поверхность радиатора, удаляя с них накопившуюся грязь. Для этого хорошо подходят сжатый воздух и щетки пылесосов.
- Обеспечьте усиленную приточно-вытяжную вентиляцию корпуса системного блока посредством дополнительного вентилятора.

Шинные архитектуры

Внутри корпуса компьютера данные передаются от устройства к устройству через группы взаимосвязанных путей прохождения сигналов, которые называются *шиной*. Центральные процессоры, память, наборы микросхем, интерфейсы накопителей и платы расширения — это лишь некоторые важнейшие устройства, использующие шины. В рамках компьютера существует множество уровней шин; это иерархия, в которой чем выше уровень, тем дальше он удален от процессора, но при этом все они соединены и выполняют функцию связывания различных компонентов компьютера. Каждый более высокий уровень, как правило, медленнее уровня, находящегося ниже него. Вот четыре основные уровня шин.

- *Шина процессора.* Это самая быстрая и самая низкоуровневая шина, применяемая материнской платой для управления интерфейсом "процессор-память" (который может работать на частотах 100, 133, 150 МГц и выше). В блок-схемах некоторых материнских плат эта шина может называться *шиной памяти.*
- *Шина кэша.* Во многих более мощных компьютерах (например, в системах Pentium Pro и Pentium II/III) для доступа к системному кэшу применяется специальная шина. Иногда она называется *внутренней шиной.* В некоторых современных материнских платах и наборах микросхем шина кэша интегрируется в стандартную шину памяти.
- *Локальная шина ввода/вывода.* Шина ввода/вывода работает на средних скоростях и выполняет функцию соединения важных для обеспечения производительности периферийных устройств с системной памятью, набором микросхем и процессором. К примеру, видеокарты, контроллеры дисков и сетевые адаптеры, как правило, подключаются через шину этого типа. Двумя наиболее распространенными локальными шинами ввода/вывода являются шина AGP (66 МГц) и шина PCI (33 МГц).

- *Стандартная шина ввода/вывода.* Самыми медленными шинными архитектурами являются шины ISA (8,3 МГц) и EISA (10 МГц) (Extended ISA — расширенная архитектура индустриального стандарта); они идеальны для соединения компьютера с более медленными периферийными устройствами (т. е. с мышью, модемом, обычной звуковой картой, а также с низкоскоростными сетевыми адаптерами).

Платы расширения используют стандартные разъемы шины ввода/вывода (т. е. локальные или стандартные), которые позволяют подключать к системе или серверу широкий спектр устройств (например, видеокарты и сетевые адаптеры). В этой части главы мы рассмотрим принципы работы шин расширения и подробнее остановимся на двух самых распространенных шинных архитектурах: PCI и AGP.

Сигналы шины

Каждая шина состоит из двух отдельных частей: шины данных и шины адреса. *Шина данных* представляет собой набор сигнальных линий, которые выполняют передачу данных между устройством расширения и системой. Говоря о шине, большинство людей имеют в виду именно шину данных. *Шина адреса* — это набор сигнальных шин, которые обозначают, куда или откуда (в памяти) должны быть переданы данные. Кроме того, есть несколько управляющих шин, которые контролируют работу шины и позволяют устройствам сигнализировать системе в случае доступности данных.

Другим важным понятием является разрядность (ширина) шины. Не забывайте, что шина — это канал, по которому проходят данные: чем шире шина, тем больше информации может по ней пройти. Разрядность шины ISA составляет 16 бит. Другие шины ввода/вывода (например, PCI и AGP) характеризуются разрядностью в 32 бит. Для сравнения, разрядность шин памяти и процессора на компьютерах Pentium (и в более современных системах) составляет 64 бита.

Примечание

Разрядность адресной шины можно определять независимо от разрядности информационной шины. Разрядность адресной шины обозначает количество доступных ячеек памяти, к которым можно обратиться.

Скорость и пропускная способность шины

Скорость шины характеризует количество бит данных, которое можно передать через отдельный проводник в течение одной секунды. Большинство стандартных шин обеспечивают передачу одного бита данных по одной информационной линии за один такт. Впрочем, новые высокопроизводительные шины наподобие AGP способны передавать два или четыре бита данных за каждый такт, таким образом, производительность увеличивается в два (или в четыре) раза. С другой стороны, более старые шины типа ISA передают один бит за два такта, тем самым в два раза снижая производительность. Для сравнения, пропускная способность шины — это общий объем данных, который теоретически можно передать по шине за одну единицу времени (измеряется в Мбайт/с). Теоретическая пропускная способность наиболее распространенных шин приводится в табл. 9.2.

Примечание

AGP работает в режимах "x2","x4" и "x8", которые позволяют шине передавать две, четыре или восемь единиц данных за такт; таким образом, эффективная скорость шины возрастает до 133, 266 или 533 МГц.

Таблица 9.2. *Сравнение пропускной способности наиболее распространенных шин*

Шина	Разрядность	Скорость шины (МГц)	Максимальная пропускная способность (Мбайт/с)
ISA (8 бит)	8	8,3	7,9
ISA (16 бит)	16	8,3	15,9
EISA	32	8,3	31,8
PCI (32 бит)	32	33	127,2
PCI (64 бит)	64	66	508,6
AGP	32	66	254,3
AGP (2X)	32	(66 × 2) 132	508,6
AGP (4X)	32	(66 × 4) 264	1017,2

Мосты между шинами

Когда в системе присутствует множество шин, материнская плата должна, во-первых, предусматривать схему их соединения, а во-вторых, обеспечивать устройствам на одной шине возможность доступа к устройствам на другой шине. Устройство, выполняющее эти функции, называется *мостом*. Наиболее распространенным мостом такого типа является мост PCI-ISA — набор микросхем на материнской плате. Шина PCI также имеет мост, соединяющий ее с шиной процессора. Все эти устройства вы можете найти в системных устройствах **System Devices** (Системные устройства) диспетчера устройств **Device Manager** для операционных систем Windows (рис. 9.10).

Управление шиной

Проблемы, которые являлись традиционными для архитектуры ПК, заключались в том, что процессору приходилось координировать все передачи данных в системе. Когда пропускная способность устройства увеличивалась, процессор был вынужден посвящать большую часть своего времени обслуживанию задач по передаче данных. С появлением шины PS/2 (и связанной с ней шины MicroChannel) от IBM отдельные устройства получили возможность самостоятельно контролировать шину и передачу данных. Это называется управлением шиной (bus mastering) или односторонним прямым доступом к памяти (first-party DMA). Устройства, которые могут выполнять эту задачу, называются хозяевами (мастерами) шины. В идеале, правильная

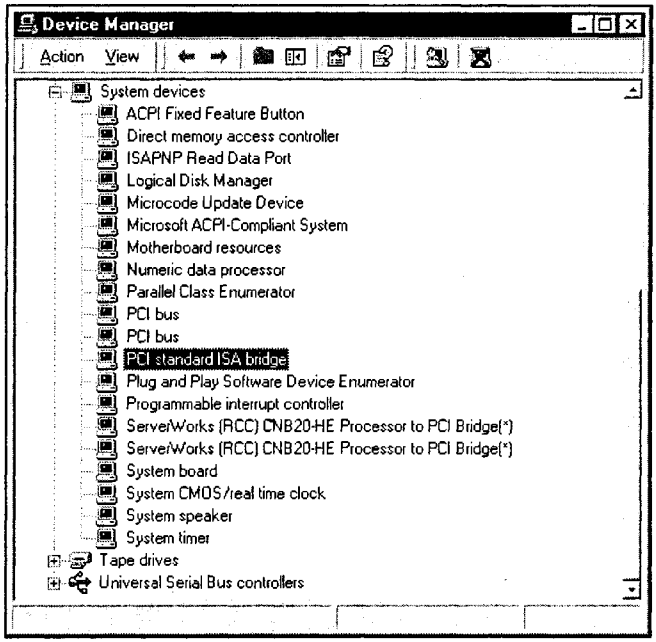


Рис. 9.10. Проверка моста PCI-ISA в Windows

организация управления шиной должна освободить процессор для выполнения других задач. Набор микросхем материнской платы выполняет арбитраж всех запросов взять на себя управление шиной. Наиболее современное управление шиной в ПК реализовано для устройств на шине PCI.

Шины ввода/вывода

Теперь, когда вы имеете некоторое представление о важнейших принципах работы шины, самое время рассмотреть некоторые шинные архитектуры, существующие в ПК и многих серверах. Важно не забывать, что встретить все эти шины на отдельно взятой материнской плате довольно сложно, но некоторые из них там будут присутствовать (например, гнездо ISA, от четырех до пяти гнезд PCI и гнездо AGP). На рис. 9.11 изображены некоторые из этих гнезд.

ISA (Industry Standard Architecture — стандартная промышленная архитектура)

Устаревший теперь разъем ISA был первой открытой архитектурой, применявшейся в персональных компьютерах типа IBM, и каждый производитель имел право воспользоваться этой архитектурой, уплатив небольшой лицензионный взнос. Так как ограничений, связанных с применением шины ISA, не существовало, они использовались в каждом последующем IBM-совместимом компьютере, вплоть до наших дней. Применение стандартной шины не только позволило тысячам производителей выпускать совместимые ПК и устройства расширения, но и помогло обеспечить

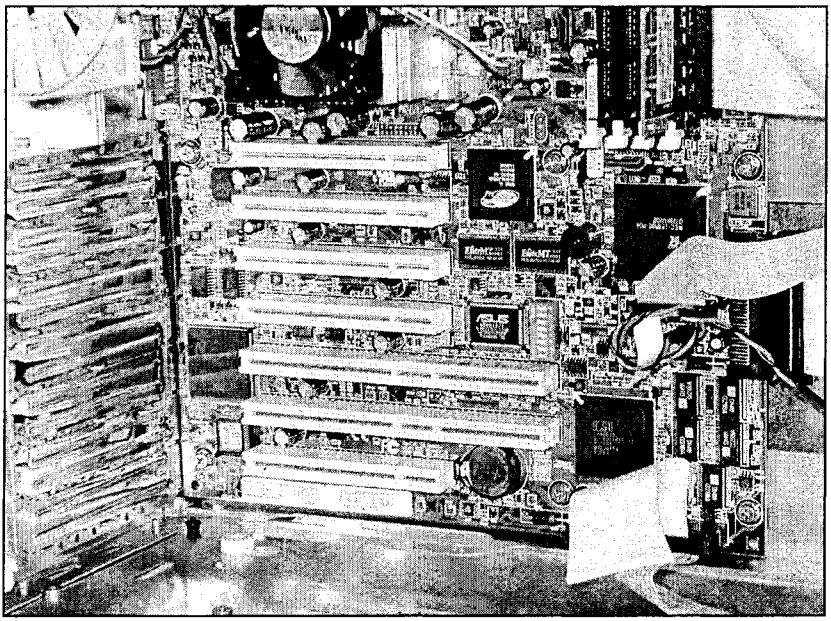


Рис. 9.11. Сервер можно без труда модернизировать, установив устройства в один или несколько слотов шины

использование однотипных операционных систем и прикладного программного обеспечения. Существуют 8- и 16-битовая версии шины ISA, хотя во всех материнских платах, выпущенных после середины 1980-х годов, 8-битовой XT-версии шины ISA производители предпочитали более быструю и гибкую 16-битовую AT-версию.

Применение 8-битовой шины ISA началось в 1982 году. 8-битовая шина ISA состоит из одного краевого разъема платы с 62 контактами. Эта шина предусматривает восемь информационных и двадцать адресных линий, которые позволяют плате находиться в пределах принятого в XT лимита в 1 Мбайт памяти. Кроме того, эта шина обеспечивает соединения для шести прерываний (IRQ2-IRQ7) и трех каналов прямого доступа к памяти (DMA0—DMA2). Шина XT работает на скорости, которая составляет 4,77 МГц. Хотя сама по себе эта шина довольно проста, IBM не удалось опубликовать точные временные соотношения для информационных, адресных и управляющих сигналов. Эта неопределенность вынудила производителей того времени подыскивать нужные временные соотношения методом проб и ошибок.

Ограничения 8-битовой шины ISA вскоре стали очевидными. Притом что гибкий диск и жесткий диск забирали два из шести доступных прерываний, COM3 и COM4 доставалось еще два (IRQ3 и IRQ4), а порт LPT забирал IRQ7, схватка за оставшиеся прерывания была ожесточенной. Из трех доступных каналов прямого доступа к памяти гибкий и жесткий диски забрали два, так что свободным оставался лишь один. Обращение могло производиться к адресному пространству объемом всего лишь в 1 Мбайт, а 8 информационных битов создавали серьезное узкое место при передачах данных. Имело смысл разработать с чистого листа совершенно новую шину, но это сделало бы все оборудование и разработки системы XT морально устаревшими.

Следующий логический этап в развитии шины наступил в 1984/85 гг. вместе с официальным представлением процессора 80286 в составе IBM PC/AT. В ней были добавлены дополнительные системные ресурсы, но при этом платы XT могли работать на модернизированной шине. В результате появилось то, что сегодня нам известно как 16-битовая ISA. Исходный 62-контактный коннектор был оставлен без изменений, но к нему был добавлен дополнительный 36-контактный коннектор. Дополнительные 8 бит данных в совокупности с уже существовавшими в шине составили 16 бит. В нее были включены пять прерываний и четыре канала прямого доступа к памяти. Кроме того, были предусмотрены пять дополнительных адресных линий, а также несколько новых управляющих сигналов. Тактовая частота в шине AT увеличилась до 8,33 МГц. Важно отметить, что теоретически на шине AT должны работать все платы XT, однако на практике бывают исключения.

Примечание

В настоящее время шина ISA уже практически не используется; предпочтение отдают более быстрой и универсальной шине PCI. Во многих современных материнских платах единственный разъем ISA предусматривается лишь в целях обратной совместимости со старыми платами расширения Большинство материнских плат серверного типа вообще не используют разъем ISA

EISA (Extended (enhanced) ISA — расширенная стандартная промышленная архитектура)

EISA — это 32-битовая шина, разработанная в 1988/89 гг. в целях удовлетворения все возраставшей потребности в более высокой скорости и производительности периферийных устройств расширения, которая была вызвана применением процессоров 80386 и 80486. Кроме того, было неразумно оставлять весь рынок 32-битовых шин за MCA (MicroChannel Architecture — микроканальная архитектура) от компании Intel. Несмотря на то, что шина EISA работает на той же тактовой частоте 8,33 МГц, 32-битовый информационный канал удваивает пропускную способность данных между материнской платой и платой расширения. В отличие от шины MCA EISA гарантирует обратную совместимость с существующими периферийными устройствами ISA и программным обеспечением. Шина EISA спроектирована с учетом полной совместимости с платами ISA. Она автоматически переключается между 16-битовым (ISA) и 32-битовым (EISA) режимами работы с помощью второго ряда краевых разъемов плат и специализированных сигнальных шин. Таким образом, платы EISA имеют доступ ко всем сигналам плат ISA, а также ко второму ряду сигналов EISA.

EISA поддерживает организацию управления передачей данных по шине и автоматическую конфигурацию плат, что упрощает установку новых плат. Шина EISA может обращаться к пятнадцати уровням прерывания и семи каналам DMA. Для обеспечения обратной совместимости с платами расширения ISA прямая поддержка шиной аудио и видео отсутствует (в шине MCA она реализована). Так как тактовая частота EISA составляет 8,33 МГц, как и в ISA, потенциальная пропускная способность платы EISA примерно вдвое больше аналогичного показателя у плат ISA. Системы EISA на рубеже 1980—1990-х гг. использовались как сетевые серверы, рабочие станции и высокопроизводительные системы ПК. В свое время шина EISA рассматривалась как профессиональный стандарт для систем типа сетевых серверов; фактически она так и не использовалась в недорогих потребительских системах.

PCI (Peripheral Component Interconnect — соединение периферийных компонентов)

К концу 1980-х гг. распространение 32-битовых процессоров и операционных систем с широким применением графики показало со всей очевидностью, что шина ISA с тактовой частотой 8,33 МГц устарела. Производители ПК начали разрабатывать альтернативные архитектуры, которые должны были обеспечить повышение производительности. В середине 1992 г. Intel Corporation и представительный консорциум производителей объявили о создании шины PCI. В то время как старая шина VLB (VESA Local Bus — локальная шина стандарта VESA (Video Electronics Standards Association — Ассоциация по стандартам в области видеоэлектроники)) была разработана специально для усовершенствования видеосистем ПК, 188-контактная шина PCI ориентировалась на будущее процессоров (и компьютеров в целом), т. к. она предусматривала шинную архитектуру с поддержкой периферийных устройств наподобие контроллеров жестких дисков, сетевых адаптеров и т. д. В PCI была реализована шинная архитектура с фиксированной тактовой частотой 33 МГц, способная передавать данные со скоростью 132 Мбит/с, что существенно превышало скорость передачи данных по 16-битовой шине ISA. Другим важным преимуществом PCI были возможности автоматической конфигурации периферийных устройств без переключателей и перемычек. Автоконфигурация (основа технологии Plug-and-Play) берет на себя заботу обо всех адресах, запросах прерывания и назначениях DMA, используемых периферийным устройством PCI.

Примечание

Хотя наиболее распространенной является 32-битовая реализация PCI, существует и 64-битовая версия шины PCI. 32- и 64-битовые платы можно устанавливать либо в 64-, либо в 32-битовый слоты. Когда 64-битовая плата установлена в 32-битовый слот, лишние контакты просто ни к чему не подключаются.

Шина PCI поддерживает *линейный пакетный режим* (Linear Bursts) — метод передачи данных, гарантирующий постоянное заполнение шины информацией. Периферийные устройства ожидают получения данных из основной памяти системы в соответствии с линейным порядком их адресов. Это значит, что большие объемы данных считываются или записываются с использованием единственного начального адреса, который затем автоматически увеличивается на единицу для каждого последующего байта в потоке. Линейный пакетный режим — это одно из уникальных свойств шины PCI, т. к. оно выполняет как пакетное считывание, так и пакетную запись. С его помощью данные по шине передаются на каждом такте. Это удваивает пропускную способность PCI по сравнению с шинами без поддержки линейного пакетного режима.

Примечание

Хотя реализация PCI с частотой 33 МГц является наиболее распространенной, существует версия PCI с частотой 66 МГц.

Устройства, поддерживающие PCI, характеризуются небольшим временем ожидания, таким образом, период времени, необходимый для предоставления периферийному устройству контроля над шиной после поступления запроса, уменьшается. К примеру, предположим, что в буфер платы контроллера Ethernet, подключенной

к локальной сети, поступают большие файлы данных из сети. Ожидая доступ к шине, плата Ethernet не имеет возможности передать данные процессору настолько быстро, чтобы избежать переполнения буфера; в результате ей приходится временно помещать содержимое файла в добавочном ОЗУ. Так как устройства стандарта PCI поддерживают более высокие скорости доступа, плата Ethernet получает возможность своевременно отправить данные процессору.

Шина PCI поддерживает управление передачей данных по шине, что позволяет одному из интеллектуальных периферийных устройств получать контроль над шиной с целью ускорения выполнения высокоприоритетной задачи, требующей значительной пропускной способности. Архитектура PCI также обеспечивает поддержку *параллелизма* — методики, которая гарантирует функционирование микропроцессора одновременно с хозяевами и позволяет избежать их ожидания. Например, параллелизм позволяет процессору производить вычисления с плавающей точкой в электронной таблице, когда плата Ethernet и локальная сеть осуществляют контроль над шиной. Архитектура PCI разрабатывалась с расчетом на двойное напряжение. В нормальном состоянии такая шина, как и все остальные, потребляет +5 В постоянного тока, но она может работать под напряжением +3,3 В постоянного тока (т. е. в низковольтном режиме).

Прерывания PCI и управление передачей данных по шине

Шина PCI использует свою собственную систему прерываний при обработке запросов от плат, находящихся на шине PCI. Эти прерывания обозначаются как #A, #B, #C и #D (а иногда нумеруются от #1 до #4), чтобы избежать путаницы с обычной нумерацией системных прерываний. Эти уровни прерываний, как правило, незаметны для пользователя; исключением является меню **PCI Configuration** программы настройки параметров CMOS (CMOS Setup), где ими можно воспользоваться для управления работой плат PCI. Для прерываний PCI задается соответствие с обычными прерываниями (обычно от IRQ9 до IRQ12). Слоты PCI в большинстве систем можно соотнести максимум с четырьмя обычными прерываниями. В системах, содержащих более четырех слотов PCI (или в системах, в которых присутствуют четыре слота и USB-контроллер), два или несколько устройств PCI совместно используют одно и то же прерывание IRQ.

Если вы работаете в Windows 98 или в более поздней версии этой ОС, то увидите в списке Device Manager (Диспетчер устройств) дополнительные записи устройств PCI — для каждого такого устройства добавляется запись, обозначающая "владельца прерывания IRQ, который управляется PCI-прерываниями" (соответствующий экран Windows 2000 показан на рис. 9.12). Управление PCI является частью стандарта Plug-and-Play и позволяет операционной системе контролировать прерывания устройств PCI, чтобы избежать конфликтов на уровне ресурсов. Существование в списке прерываний нескольких владельцев для одного IRQ не означает, что в системе существует конфликт на уровне ресурсов.

Шина PCI поддерживает прямое управление, поэтому устройства на шине PCI могут получать контроль над шиной и выполнять передачу данных напрямую, без непосредственного вмешательства системного процессора. PCI — это первый вид шины, в котором управление шиной стало обычным явлением; возможно, это произошло потому, что впервые появились операционные системы и наборы микросхем, действительно способные извлечь из этой методики пользу. PCI предусматри-

вает управление одновременно несколькими устройствами, находящимися на одной шине, а набор микросхем материнской платы гарантирует невозможность блокировки одним устройством на шине (включая процессор) любого другого устройства. В то же время, PCI позволяет любому устройству использовать полную пропускную способность шины, если другие устройства не нуждаются в передаче данных.

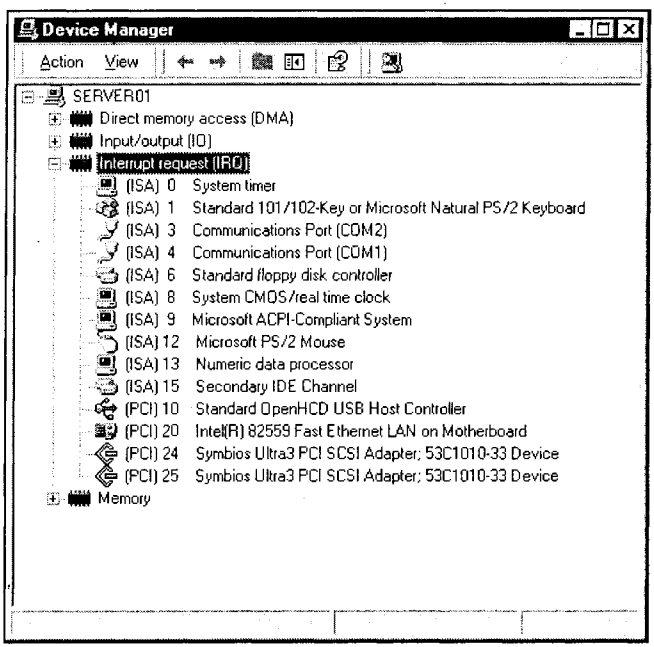


Рис. 9.12. Распределение прерываний для шины PCI не является необходимым, если на сервере нет других устройств PCI

Шина PCI позволяет установить в качестве хозяина подходящий для этих целей IDE/ATA-накопитель на жестком диске. При наличии всех необходимых свойств, PCI IDE в режиме прямого управления шиной может повысить производительность по сравнению с использованием традиционных режимов передачи данных PIO (которые являются принимаемыми по умолчанию средствами передачи данных жесткими дисками IDE/ATA). Если разрешен режим хозяина для PCI IDE, устройства IDE/ATA вместо PIO используют для передачи данных режимы DMA. Для правильного функционирования хозяина шины PCI необходимы все перечисленные ниже элементы.

- *Системное аппаратное обеспечение с поддержкой прямого управления шиной.* Оно включает материнскую плату, набор микросхем (чипсет), шину и BIOS. В качестве хозяина шины IDE поддерживают практически все современные материнские платы с наборами микросхем для Pentium II/III или AMD Athlon.
- *Жесткий диск с поддержкой прямого управления шиной.* Это означает, что жесткий диск должен выполнять передачу данных в режиме DMA 2. Его поддерживают все жесткие диски Ultra ATA (т. е. UDMA/33, UDMA/66 и UDMA/100).

- *32-разрядная операционная система с многозадачностью.* Как правило, под этим подразумевается Windows NT/2000, Windows 95/98/ME и Linux.
- *Драйверы управления передачей данных по шине.* В операционной системе должен присутствовать специальный драйвер, который обеспечит поддержку управления передачей данных по шине.

Примечание

Помните, что организация управления передачей данных по шине не сможет обеспечить значительного повышения производительности в среде DOS и в операционных системах без многозадачности (например, в Windows 9x/ME).

AGP (Accelerated Graphics Port — ускоренный графический порт)

Видеосистемы персональных компьютеров постоянно наращивают глубину цвета и разрешение. Современная видеоинформация образует гигантские объемы данных. Эти данные требуют не только значительных затрат памяти, но и большой пропускной способности шины, которая должна обеспечить их передачу на видеоплату. Шина AGP открывает путь графической информации, а особенно для трехмерных приложений и программ визуализации. К примеру, высокая скорость выполнения операций с плавающей точкой в современных процессорах позволяет сгладить прорисовку трехмерных сопряжений и анимационных эффектов, а также усилить глубину трехмерного изображения . Следующий шаг — сделать такое изображение максимально реалистичным ("живым"). Для этого компьютер должен формировать трехмерное изображение, добавляя текстуры, эффекты прозрачности, текстурное отображение, подсветку и прочие эффекты. Технология AGP повышает производительность графических средств, предусматривая специальную высокоскоростную шину для перемещения крупных блоков текстурных трехмерных данных между графическим контроллером и системной памятью. AGP позволяет графическому контроллеру с аппаратным ускорением исполнять текстурные карты непосредственно из системного ОЗУ (без их кэширования в сравнительно небольшой локальной видеопамяти). Эта шина также помогает повысить скорость потока декодированного видео из процессора в графический контроллер. Освобождение шины PCI от этих значительных объемов данных позволяет ей координировать передачу данных с дисков и других контроллеров.

Высокая пропускная способность — это секрет улучшенных возможностей AGP. 32-битовый 66-мегагерцевый интерфейс AGP расположен между набором микросхем и графическим контроллером. Такая архитектура значительно увеличивает пропускную способность, доступную графическому ускорителю. В основном, AGP обеспечивает пропускную способность, равную 266 Мбайт/с (что в два раза больше пропускной способности PCI). Эта базовая версия AGP носит название AGP 1X. В случае применения более сложных методов обработки данных, можно добиться передачи 2 байт за каждый такт AGP и в результате обеспечить пропускную способность в 532 Мбайт/с (этот вариант называется AGP 2X). Дальнейшие усовершенствования системы обработки данных AGP и применение новых наборов микросхем приводят к тому, что посредством передачи 4 байт за каждый такт AGP мы получаем пропускную способность, превосходящую 1 Гбайт/с (AGP 4X). 32-битовая шина AGP берет свое начало в спецификации локальной шины PCI, но при этом реализует некоторые значительные усовершенствования и дополнения, призванные опти-

мизировать AGP для высококачественной трехмерной графики. Наиболее заметным различием является тактовая частота. Если в PCI тактовая частота составляет 33 МГц, то в AGP — 66 МГц. Есть и другие существенные различия, включающие:

- конвейерные операции чтения и записи в память, которые компенсируют время ожидания доступа к памяти;
- демультиплексирование адреса и данных на шине, что позволяет добиться почти 100%-ной эффективности ее применения;
- новая временная диаграмма импульсного типа для существующей электрической спецификации на напряжение питания 3,3 В, которая предусматривает одну (AGP 1X) или две (AGP 2X) передачи данных за один 66-мегагерцевый такт; таким образом, реальная пропускная способность превышает 500 Мбайт/с;
- новая низковольтная спецификация, которая предусматривает четыре (AGP 4X) передачи данных за один 66-мегагерцевый такт, в результате чего реальная пропускная способность превышает 1 Гбайт/с;
- в гнезде шины AGP применяется новая основа коннектора, несовместимая с разъемом PCI; по этой причине платы PCI и AGP не являются механически взаимозаменяемыми.

Чтобы система могла воспользоваться преимуществами AGP, необходимо соблюдение нескольких приведенных ниже условий.

- Видеокарта AGP. Вам понадобится видеоадаптер на слот AGP.
- Материнская плата с набором микросхем, поддерживающим AGP. Материнская плата должна быть полностью совместима с AGP, включая набор микросхем, слот шины и BIOS.
- Поддержка со стороны операционной системы. Чтобы обеспечить полную поддержку AGP, следует работать в Windows 98 или более поздней версии этой операционной системы.
- Поддержка со стороны драйвера AGP. Вам понадобятся драйверы, поддерживающие функции AGP чипсета материнской платы, а также видеодрайверы для платы AGP.

I^2O (Intelligent I/O — интеллектуальный ввод/вывод)

В основе компьютерных технологий заложена потребность в увеличения вычислительных мощностей и увеличении скорости операций ввода/вывода. К сожалению, скорости ввода/вывода отстают от скорости процессора, в результате чего неминуемо образуется узкое место, ограничивающее поток данных. Пытаясь повысить пропускную способность подсистемы ввода/вывода, мы увеличиваем количество прерываний, отсылаемых главному процессору. Прерывание происходит всякий раз, когда дисковая система, сетевой адаптер или любое другое устройство ввода/вывода выполняет запрос. При выполнении любой отдельно взятой операции устройство ввода/вывода может прерывать процессор много раз. Хотя процессоры достаточно быстро выполняют обычные вычислительные операции, они не предназначены для выполнения команд, связанных с прерываниями. Решение проблемы заключается в том, чтобы дать процессору возможность делать то, что он умеет лучше всего — управлять приложениями; при этом его нужно освободить от выполнения операций

ввода/вывода путем реализации интеллектуальной обработки ввода/вывода (ее называют I²O).

Термин "интеллектуальный ввод/вывод" чаще всего обозначает любую серверную систему, в которой обрабатывающий элемент используется как часть подсистемы ввода/вывода. Процессор ввода/вывода выполняет задачи, которые в обычной ситуации выполняет центральный процессор, тем самым уменьшается нагрузка на CPU. В результате частичной разгрузки процессора общее время отклика системы уменьшается, а пропускная способность ввода/вывода увеличивается. I²O позволяет специализированному процессору ввода/вывода освобождать процессор от выполнения некоторых задач. Благодаря I²O запросы могут приходить с одного устройства PCI, уходить на другое такое устройство, минуя процессор. Процессор I²O распознает эти запросы и обрабатывает их локально. Кроме того, он позволяет организовать очередь запросов, пока центральный процессор работает над выполнением других задач.

С момента первой реализации интеллектуальных подсистем производители начали проектировать серверы с более высокой пропускной способностью ввода/вывода. Но с ростом потребностей разработчики программного обеспечения старались успевать за множеством драйверов, которые выполняли функцию связующего звена с различными операционными системами. Возросла потребность в аппаратном стандарте, который мог бы работать с различными операционными системами и их версиями. В 1996 г. Intel и другие ведущие производители сформировали специальную группу, которая занялась разработкой стандартного интерфейса для интеллектуальных систем ввода/вывода. То, что получилось, назвали I²O. В результате производители периферийных устройств освободились от необходимости написания драйверов для различных операционных систем. Вместо этого требуется создать лишь один драйвер для архитектуры I²O, и операционная система будет работать с подсистемой I²O. Кроме того, архитектура I²O упрощает задачу создания периферийных устройств, снижая запросы к платам ввода/вывода за счет того, что значительная часть операций, которая ранее производилась на плате, теперь выполняется процессором I²O.

Драйверы I²O делятся на два модуля: модуль служб OSM (OS services module, — модуль служб операционных систем) и модуль HDM (Hardware Device Module — модуль аппаратных устройств). Модуль OSM служит средством связи с операционной системой, а модуль HDM осуществляет взаимодействие с аппаратным устройством. Эти два модуля обмениваются информацией посредством двухуровневой системы связи, в которой уровень сообщений устанавливает сеанс связи, а транспортный уровень определяет совместное использование информации. Модули осуществляют взаимодействие, не располагая данными о нижележащих шинных архитектурах или топологиях.

Серверная память

Системная память, называемая ОЗУ (RAM), содержит программный код и данные, которые обрабатываются процессором (процессорами) сервера. Производительность компьютера обусловлена столь тесным взаимодействием памяти и процессора. Постоянно появляются все более быстрые и сложные процессоры и, чтобы воспользоваться их мощностью, регулярно разрабатывается все более сложное программное

обеспечение. В свою очередь, чем сложнее программное обеспечение, тем больше быстрой памяти ему нужно. Сети и сетевые серверы должны предоставлять файлы и приложения многим пользователям одновременно (а иногда пользователей бывает очень много) — именно поэтому серверам требуются большие объемы памяти. Эти запросы привели к распространению типов памяти, выходящих далеко за рамки простых, традиционных динамических запоминающих устройств (DRAM). Конвейерно-пакетный кэш, быстрая синхронная динамическая память (SDRAM) и другие редкие разновидности памяти типа Rambus DRAM (RDRAM) теперь соревнуются за внимание технических специалистов. С другой стороны, новые стандарты памяти несут с собой и новые проблемы. В этой части главы представлены данные о распространенных типах памяти и ее настройках, о вопросах, связанных с ее установкой и устранением неисправностей.

Быстродействие памяти

Компьютерная индустрия постоянно находится в поиске равновесия между ценой и производительностью. Более высокие цены, как правило, соответствуют более высокой производительности, но низкая цена делает персональный компьютер доступным для большинства людей. Что касается памяти, снижение цены обычно подразумевает применение более дешевых (и более медленных) запоминающих устройств. К сожалению, при использовании медленной памяти процессор вынужден простаивать. Одна из основных характеристик памяти — это ее скорость или *время доступа*. Время доступа представляет собой задержку между успешной адресацией данных в памяти и успешной передачей этих данных на информационную шину. Обычно время доступа исчисляется в наносекундах (нс), а время доступа в современных стандартах памяти составляет 50—60 нс; для сравнения, время доступа в 70 нс было широко распространено в старых системах i486. SDRAM представляет собой исключение из этого правила и, в основном, характеризуется длительностью цикла, а не временем доступа. *Длительность цикла* — это минимальный период времени между доступами. Средняя длительность цикла в запоминающих устройствах типа SDRAM составляет 12 нс, но есть устройства, в которых этот показатель равен 10 и 8 нс (а бывает и меньше).

Как правило, можно использовать более быструю память, чем рекомендует производитель. При этом система продолжит нормально работать, но замена памяти на более быструю редко повышает производительность. Как вы узнаете из последующих разделов, память и архитектуры обычно рассчитаны на конкретный уровень производительности. Применение более быстрой памяти не повредит и не окажет негативного влияния на производительность системы, но это обойдется дороже, а заметного повышения производительности не произойдет, т. к. данная система не обладает возможностью максимально использовать преимущества быстрой памяти. Такая замена имеет смысл только в случае, если ваша система устарела, а вы хотели бы, чтобы новую память можно было использовать на новой, более быстрой материнской плате, которую вы планируете установить позднее.

Определение быстродействия памяти

При поиске неисправностей или подборе комплектующих важно проверить модули памяти на соответствие скоростным характеристикам (т. е. времени доступа или, если речь идет о SDRAM, длительности цикла). К сожалению, в точности опреде-

лить быстродействие памяти исходя из маркировки чипов может быть очень сложно. Обычно оно обозначается неявно — путем добавления некоего числа в конец номера изделия. К примеру, окончание номера чипа на -6 часто обозначает время в 60 нс, -7 — 70 нс, а -8 — 80 нс. В маркировке модулей памяти SDRAM -12 может обозначать длительность цикла в 12 нс, -10 — 10 нс, а -8 — 8 нс. Как бы то ни было, единственный способ определить быстродействие памяти — это сверить номер изделия (запоминающего устройства) с каталогом производителя и узнать характеристики из описания устройства в этом каталоге (например, 4M × 32 50 нс EDO).

Мегабайты и организация памяти

Теперь самое время разъяснить принцип байтов и мегабайтов. Все очень просто: байт равен 8 битам (двоичным единицам и нулям), а мегабайт — это миллион таких байтов (точнее, M=1 048 576 байт, но производители часто округляют значение приблизительно до ближайшего миллиона). Единица измерения памяти вашего компьютера — мегабайт (Мбайт). К примеру, если модуль SIMM организован как 1M по 8 бит, значит, в нем 1 Мбайт. Если SIMM разбит как 4M по 8 бит, значит, в нем 4 Мбайт. К сожалению, со времен IBM XT память не разбивалась по 8 бит. Более практичной является 32-разрядная память (процессоры 486 и совместимые) и 64-разрядная (процессоры Pentium II/III/4) схема памяти. Даже если "ширина" памяти превышает один байт, она все равно измеряется в мегабайтах. К примеру, модуль памяти SIMM с организацией 1M × 32 бит (4 байта) обозначается как 4 Мбайт (емкость устройства равна 4 Мбайт), в то время как модуль SIMM с организацией 4M × 32 бит составит 16 Мбайт. Следовательно, при покупке 8-мегабайтового 72-контактного модуля SIMM, вероятнее всего, вы приобретете два модуля 32-битовой памяти по 4 Мбайт.

Автоматическое обнаружение памяти

Другой функцией современных запоминающих устройств является ряд сигналов, применяемых для автоматического обнаружения памяти. Если настроить сигналы автоматического обнаружения, компьютер получит возможность мгновенно выявлять характеристики установленных модулей памяти и в соответствии с ними настаивать самого себя. Автоматическое обнаружение памяти, как правило, определяет три рабочие характеристики памяти: объем, схему устройства и скорость. Многие современные запоминающие устройства используют последовательные микросхемы EEPROM (Electrically Erasable Programmable Read-Only Memory — электрически перепрограммируемая постоянная память) для передачи материнской плате во время запуска данных автоматического обнаружения памяти (Serial Presence Detect, SPD — последовательное обнаружение присутствия).

Регенерация памяти

Электрические заряды, помещенные в каждую запоминающую ячейку ОЗУ, должны пополняться (или обновляться) каждые несколько миллисекунд. Без регенерации (Refresh) данные ОЗУ теряются (именно поэтому ОЗУ называют энергозависимой памятью). В принципе, регенерация подразумевает, что каждая запоминающая ячейка может быть считана и перезаписана назад в массив памяти. Обычно эта за-

дача выполняется путем единовременного считывания и перезаписи целой строки массива. Каждая строка, состоящая из битов, последовательно передается усилителю считывания/регенерации (он является частью кристалла памяти), который перезаряжает соответствующие запоминающие конденсаторы, а затем перезаписывает каждый бит строки в массиве. На практике, строка битов автоматически обновляется при каждом выборе строки массива — весь массив можно обновить путем считывания каждой его строки каждые несколько миллисекунд.

Ключом к регенерации является способ адресации ОЗУ. В отличие от других кристаллов памяти, на которые все адресные сигналы подаются одновременно, обращение к ОЗУ представляет собой двухэтапную последовательность. Общий адрес разделяется на строчный (младший) и столбцовый (старший) адреса. Биты адреса строки помещаются на адресную шину DRAM в первую очередь, а в линию "-Row Address Select" (-RAS — выбор строчного адреса) посылается импульсный сигнал нулевого уровня для мультиплексирования битов в схему декодирования адресов микросхемы. Младшая часть адреса активирует целую строку массива и инициирует считывание и обновление каждого бита в строке. Логические нули остаются нулями, а логические единицы перезаряжаются до их полного значения.

Затем биты адреса столбца помещаются на адресную шину DRAM, а в линию "-Column Address Select" (-CAS — выбор адреса столбца) посылается импульсный сигнал нулевого уровня. Столбцовая часть адреса определяет соответствующий бит в пределах выбранной строки. При выполнении операции считывания выбранные биты поступают через буфер данных на информационную шину. Во время операции записи линия считывания/записи должна находиться в состоянии логического нуля, а входные данные должны поступить на микросхему еще до прихода сигнала стробирования -CAS. Далее новые биты данных помещаются в выбранные ячейки массива памяти.

Даже если обращения к микросхеме для записи или считывания не происходит, память все равно обновляется, обеспечивая целостность данных. Регенерацию можно осуществить путем прерывания микропроцессора для выполнения им процедуры обновления, которая просто последовательно проходит по каждому адресу строки (при простом обновлении адреса столбцов выбирать не нужно). Такой строчный метод регенерации увеличивает скорость общего процесса обновления. Хотя необходимость регенерации ОЗУ каждые несколько миллисекунд может показаться существенным ограничением, все же до наступления момента прерывания с целью обновления компьютер может выполнить довольно много команд. Как правило, операции по регенерации выполняются набором микросхем материнской платы. Зачастую проблемы, связанные с памятью (особенно ошибки четности), которые нельзя решить путем замены модуля памяти, можно отнести к отказу регенерации на материнской плате.

Типы памяти

Чтобы компьютер мог работать, процессор должен принимать команды программ и обмениваться данными непосредственно с памятью. Следовательно, память не должна отставать от процессора (в противном случае процессору придется ее ждать). Теперь, когда скорость работы процессоров крайне высока (и каждые несколько месяцев повышается), традиционные архитектуры памяти уступают место специализированным запоминающим устройствам, приспособленным для выполнения опре-

деленных функций в рамках ПК. При модернизации и восстановлении различных систем вы без сомнения встретитесь с некоторыми из новейших наименований памяти, приведенных ниже (в алфавитном порядке).

DDR SDRAM

Одним из ограничений SDRAM является теоретический предел архитектуры, составляющий 125 МГц (хотя благодаря технологическому прогрессу этот показатель повысился до 133 и 150 МГц), но для того, чтобы пропускная способность памяти соответствовала скорости современных процессоров, скорость шины должна быть выше этих пределов. Вскоре могут появиться несколько новых стандартов памяти, но для большинства из них требуются специальные разъемы, уменьшение разрядности шин и другие конструктивные особенности. Тем временем память DDR SDRAM (Double Data Rate SDRAM, SDRAM с двойной скоростью передачи данных) позволяет выполнять операции вывода как по нарастающему, так и по ниспадающему фронту тактового импульса. В настоящее время только нарастающий фронт сигнализирует событие, так что DDR SDRAM может реально удвоить скорость операций, доведя ее по крайней мере до 200 МГц (первый кандидат для материнских плат под AMD Athlon). Уже есть один набор микросхем Socket A, обеспечивающий поддержку DDR SDRAM, и если производители решат сделать этот тип памяти доступным, вскоре последуют и другие.

PC100/PC133 SDRAM

Когда компания Intel приняла решение официально представить скорость шины в 100 МГц, было понятно, что большинство модулей SDRAM, существовавших на тот момент, не могли нормально работать на скорости выше 83 МГц. Чтобы обеспечить поддержку скорости шины в 100 МГц, Intel выпустила спецификацию PC100 — руководство, предназначенное для производителей, в котором содержались данные о принципах изготовления модулей, которые будут нормально функционировать на 100-мегагерцевых наборах микросхем (например, на 440BX). Вместе со спецификацией PC100 Intel составила несколько инструкций, касающихся длины, ширины и разводки, количества слоев печатных схем, спецификаций программирования EEPROM и т. д. PC100 SDRAM на частоте 100 МГц (и выше) обеспечивает повышение производительности системы Socket 7 на 10 и 15%, т. к. внешний кэш работает на скорости системной шины. В системах Pentium II/III существенного повышения производительности не произойдет, потому что их внешний кэш работает на половине частоты процессора (естественно, за исключением микросхем Celeron, в которых кэш отсутствует).

Примечание

Возможно, вы встретитесь с более быстрыми типами сертифицированной памяти SDRAM, включая PC133 (133 МГц) и PC150 (150 МГц).

RDRAM (Rambus DRAM)

Большинство вариантов памяти до настоящего времени являлись разновидностями одной и той же основной архитектуры. Компания Rambus, Inc. (объединение разработчиков EDRAM) сконструировала новую архитектуру памяти под названием

Rambus channel. Процессор или специализированная микросхема используется как ведущее устройство, а модули RDRAM — как ведомые. 16 бит данных отсылаются в обоих направлениях по каналу Rambus со скоростью 600, 711 или 800 МГц (PC800 RDRAM), что теоретически позволяет повысить скорость передачи данных до 1,6 Гбайт/с (этому соответствует время доступа в 1 нс). Недостаток RDRAM заключается в том, что микросхемы этой памяти вырабатывают очень много тепла (требуя использования теплоотвода или теплораспределителя) на модуле Rambus. Хотя некоторые высокопрофессиональные наборы микросхем в настоящее время поддерживают RDRAM, уровень производительности модулей Rambus оказался ниже, чем предполагалось. Поэтому традиционные модули SDRAM DIMM остаются распространенным типом операционной памяти для серверов и других высокопроизводительных компьютеров. Подробную информацию о технологиях Rambus можно получить по адресу **www.rambus.com/developer/getting_started.html**.

SDRAM (синхронная или синхронизированная память DRAM)

Обычная память может передавать данные только во время определенных периодов такта. В SDRAM принцип функционирования памяти изменяется, и передача данных возможна в любой момент такта. Само по себе это не очень важно, но SDRAM предусматривает конвейерно-пакетный режим, который позволяет начинать последующий доступ еще до завершения предыдущего. Такой непрерывный доступ к памяти обеспечивает время доступа до 8 нс, а скорость передачи данных при этом возрастает до 100 Мбит/с. Модули SDRAM в настоящее время широко используются на материнских платах и поддерживаются микросхемами Intel VX (и более поздними версиями), VIA 580VP, 590VP и 680VP (и более поздними версиями). Как и BEDO (Burst EDO-пакетный EDO (Enhanced Data Out — ускоренный ввод/вывод)), SDRAM может передавать данные по схеме 5-1-1-1, но при этом поддерживает скорость материнской платы до 100 МГц, что идеально подходит для 75- и 82-мегагерцевых материнских плат, а также для 100-мегагерцевых материнских плат для систем Pentium II/III. Современные типы SDRAM способны обеспечивать скорость шины в 133 и 150 МГц. Более подробная информация о SDRAM размещается по адресу **www.ti.com/sc/docs/memory/brief.htm**.

SRAM (Static Random Access Memory — статическое ОЗУ)

SRAM является классической архитектурой памяти, появление которой предшествовало DRAM. SRAM не требует проведения регулярных операций регенерации и может работать на скорости доступа, значительно превосходящей DRAM. Но для хранения одного бита в SRAM применяется шесть или более транзисторов. В результате плотность SRAM снижается, а уровень потребления электроэнергии возрастает (это основная причина, по которой технология SRAM так и не получила повсеместного распространения в компьютерной среде). Тем не менее высокая скорость SRAM утвердила эту технологию в виде внешнего (L2) кэша процессора. Возможно, вы встретитесь с тремя типами схем кэша SRAM: асинхронной, синхронно-пакетной и конвейерно-пакетной.

- Память ASRAM (Asynchronous Static RAM — асинхронное статическое ОЗУ). Это стандартная память внешнего кэша, впервые появившаяся в системах i386. Ничего выдающегося в ней нет, за исключением того, что обращение к ее содержимому может происходить намного быстрее (20, 15 или 12 нс), чем к DRAM.

ASRAM не обеспечивает производительности, достаточной для синхронного доступа и уже давно заменена более эффективными типами памяти.

- Память SBSRAM (Synchronous Burst Static RAM — синхронно-пакетное статическое ОЗУ). Очень часто этот тип внешнего кэша оценивается как самый оптимальный для материнских плат, работающих на средних скоростях (~60—66 МГц). Обеспечивая время доступа, равное 8,5 или 12 нс, SBSRAM способна работать с синхронными пакетами данных кэша по схеме 2-1-1-1 (т. е. два такта на первый доступ, затем один такт на один доступ, синхронно с тактовым импульсом процессора). Впрочем, при превышении материнскими платами скорости в 66 МГц (т. е. в архитектурах, работающих на частотах 75 и 83 МГц) SBSRAM утрачивает свои преимущества по отношению к конвейерно-пакетной памяти.
- Память PB SRAM (Pipelined Burst Static RAM — конвейерно-пакетное статическое ОЗУ). Наиболее быстрая форма высокопроизводительного кэша с временем доступа от 4,5 до 8 нс; в настоящее время подходит для материнских плат со скоростью от 75 МГц. PB SRAM требуется дополнительный такт для открытия, но затем она работает синхронно с тактовой частотой материнской платы (с распределением типа 3-1-1-1) в широком диапазоне ее частот.

VRAM (Video RAM — видеопамять)

Традиционно для видеопамяти использовались микросхемы DRAM, но с постоянно растущими запросами на быструю обработку видеоданных (на мониторах SVGA с высоким разрешением) возросла потребность в более эффективном способе передачи данных в видеопамять и из нее. Память VRAM, разработанная компанией Samsung Electronics, обеспечивает увеличение скорости за счет использования сдвоенной информационной шины. В простой памяти применяется одна информационная шина — данные поступают в память и отсылаются из нее с помощью одного набора сигналов. В памяти VRAM используются входящая и исходящая информационные шины. В результате появляется возможность одновременного считывания данных из VRAM и записи в нее. Следует учитывать то, что преимущества VRAM могут быть реализованы только в условиях профессиональных видеосистем с разрешением 1024 × 768 × 256 (или выше), где производительность по сравнению с видеоадаптером, использующим DRAM, может повыситься на 40%. При использовании памяти VRAM в менее мощных системах вы не почувствуете никаких положительных изменений.

WRAM (Window RAM — "оконная" память)

Компания Samsung Electronics позиционирует WRAM как новое запоминающее устройство со специализацией на видеосигналах. В WRAM есть множество битовых матриц, подсоединенных к протяженной внутренней шине, и высокоскоростные регистры, способные осуществлять передачу данных практически непрерывно. Другие специализированные регистры поддерживают такие свойства, как цвет изображения, цвет фона, управляющие биты блокирования записи и истинно-побайтовое маскирование. Samsung утверждает, что WRAM позволяет развивать скорость передачи данных до 640 Мбайт/с (что на 50% превышает показатели VRAM), но устройства WRAM стоят дешевле, чем их VRAM-аналоги. За последние несколько лет тех-

нология WRAM подверглась тщательному анализу и в видеосистемах предпочтение отдается, как правило, SDRAM.

Техника работы с памятью

Вместо дополнительных расходов на специальные запоминающие устройства производители персональных компьютеров зачастую используют недорогие, хорошо себя зарекомендовавшие типы памяти в архитектурах, которые создаются с целью извлечения максимума возможностей из памяти с низкой производительностью. Практически в любых системах вы можете встретиться с одной из трех распространенных архитектур — это страничная память, расслоенная память и кэш.

Страничная память (paged memory)

Эта технология разделяет системную память на небольшие группы (или страницы) длиной от 512 байт до нескольких килобайт. Схема управления памятью на материнской плате позволяет осуществлять последовательные доступы к памяти на одной странице с нулевыми периодами ожидания. Если последующий доступ выполняется вне текущей страницы, до момента нахождения новой страницы может пройти один или несколько периодов ожидания. Этот принцип аналогичен режиму быстрого страничного обмена DRAM, рассмотренному ранее. Постраничные архитектуры реализованы в высокопроизводительных моделях i286, PS/2 (в модели 70 и 80), а также во многих системах i386.

Расслоенная память (Interleaved Memory)

По сравнению со страничной памятью эта технология обеспечивает более высокую производительность. Расслоенная память объединяет два блока памяти в один. Первая часть является четной, вторая — нечетной; в результате содержимое памяти распределяется между этими двумя областями. Это позволяет выполнять доступ к памяти во второй части еще до завершения доступа в первой. Расслоение способно удвоить производительность памяти. Особенность технологии расслоенной памяти заключается в том, что в виде согласованных пар необходимо предоставить вдвое больше памяти. Большинство компьютеров, использующих эту технологию, позволяют за один раз добавлять один модуль памяти, но при этом расслоение отключается и производительность системы снижается.

Кэш

Это наиболее распространенная архитектура памяти. *Кэшем* называется небольшой (от 8 Кбайт до 2 Мбайт) объем памяти SRAM, который представляет собой интерфейс между процессором и обычным системным ОЗУ. Как правило, время доступа к SRAM составляет порядка 5—15 нс; этого достаточно, чтобы не отставать от процессора с нулевыми периодами ожидания. Микросхема контроллера кэша на материнской плате отслеживает часто запрашиваемые ячейки памяти (и прогнозируемые ячейки памяти) и копирует их содержимое в кэш. Когда процессор выполняет считывание из памяти, в первую очередь он проверяет кэш. Если необходимое содержимое в кэше присутствует (результативное обращение в кэш), считывание данных происходит при нулевых периодах ожидания. Если же в кэше нужных данных нет (нерезультативное обращение в кэш), они считываются непосредственно из DRAM,

что сопровождается одним или несколькими периодами ожидания. Небольшой объем очень быстрого кэша (он называется маркировочной памятью) выполняет функцию указателя, записывая различные ячейки, данные которых хранятся в кэше. Удачно спроектированная система кэширования способна обеспечить 95% результативности, т. е. в 95% случаев работа памяти не сопровождается периодами ожидания.

В современных компьютерах есть два уровня кэша. Процессоры начиная с i486 располагают небольшим внутренним кэшем (кэш L1 или кэш процессора), а внешний кэш (память SRAM, установленная на материнской плате в виде модулей DIP (Dual-In-line Package — корпус с двухрядным расположением выводов) или COAST (Cache On A Stick — модуль кэш-памяти)) обычно обозначается как кэш L2. В процессорах i386 внутренний кэш отсутствует (хотя в IBM 386SLC предусматривается кэш L1 объемом в 8 Кбайт). В большинстве процессоров семейства i486 есть внутренний кэш размером в 8 Кбайт. Первые процессоры Pentium оснащены двумя внутренними кэшами по 8 Кбайт каждый: один для данных и один для команд. В современных процессорах Pentium II/III Slot 1 кэш L2 объемом в 256—512 Кбайт находится на самом картридже процессора. В процессорах Xeon, предназначенных для использования в серверных системах, объем кэша L2 может составлять до 2 Мбайт.

RAID-кэш — это еще одна разновидность кэша, которая позволяет плате контроллера RAID записывать данные в кэш (ОЗУ) на самом контроллере RAID (а не на диски). Сервер может обращаться к кэшу контроллера RAID (называемому ускорителем массива) более чем в 100 раз быстрее, чем к диску. После кэширования данных в ускорителе массива контроллер RAID записывает эти данные в дисковый массив, когда контроллер бездействует. Применение RAID-кэширования повышает производительность сервера во время считывания данных с диска путем предупреждения запросов на считывание (упреждающее считывание). Эти ожидаемые данные передаются ускорителю массива и находятся в готовности еще до поступления запроса. Когда контроллер RAID получает запрос на считывание кэшированных данных, он может сразу передать их ОЗУ на скорости шины PCI.

Кэширование данных процессора и дисков часто реализуется как фоновая (write back) и прямая (write through) запись. В кэше фоновой записи (кэш фонового копирования) новые данные, которые записываются в кэш (например, в кэш процессора L1), в память (или на диск) записываются не сразу. Это происходит в перерыве обработки, когда появляется время на запись данных. Это обеспечивает повышенную производительность фонового кэширования, т. к. не нужно ждать, пока система сохранит данные из кэша — их запись происходит в фоновом режиме. Недостатком такого кэша является вероятность сбоя в системе, если ее полный отказ произойдет до сохранения содержимого кэша. Прямое кэширование сразу сохраняет данные, находящиеся в кэше, так что содержимое кэша соответствует содержимому памяти (или диска). Этот метод немного медленнее, но зато он более надежен (это особенно важно в системах повышенной надежности).

Теневая память

Постоянное запоминающее устройство (ПЗУ) (ПЗУ BIOS на материнской плате или микросхема ПЗУ на плате расширения) работает чрезвычайно медленно, и время доступа к нему зачастую превышает несколько сотен наносекунд. Доступ к ПЗУ

требует большого количества периодов ожидания, что снижает производительность системы. Кроме того, к процедурам, хранящимся в BIOS (особенно в ПЗУ BIOS видеокарты), обращения происходят чаще всего.

Начиная с систем i386 в некоторых конструкциях использовалась технология под названием *теневая память*. Содержимое ПЗУ во время инициализации системы загружается в область быстрого ОЗУ, а затем компьютер отображает быстрое ОЗУ в ячейках памяти, используемых устройствами ПЗУ. При необходимости доступа к процедурам ПЗУ информация извлекается из теневого ПЗУ, а не из реальной интегральной схемы ПЗУ. Производительность ПЗУ, таким образом, повышается по меньшей мере на 300%.

Теневая память используется также устройствами ПЗУ, которые не полностью реализуют доступную разрядность шины. Например, в 16-битовой вычислительной системе может содержаться плата расширения с 8-битовой интегральной схемой ПЗУ. Чтобы извлечь из ПЗУ одно 16-битовое слово, системе приходится обращаться к ПЗУ не один, а два раза. В 32-битовой вычислительной системе для извлечения полного 32-битового слова нужно четыре раза обратиться к 8-битовому устройству ПЗУ. Представьте, какие серьезные задержки происходят при выполнении подобных задач. Предварительная загрузка ПЗУ в теневую память практически исключает такие задержки. Как правило, режим использования теневой памяти можно включить или отключить через процедуры CMOS Setup.

Модули памяти

Появление новых стандартов памяти всегда способствовало созданию новых интегральных схем. Это не только привело к реализации больших объемов памяти в очень компактных микросхемах, но и обусловило сохранение сравнительно высоких цен на память. Обычно в компьютерах небольшие объемы ОЗУ были встроены в материнскую плату, и предусматривались дополнительные слоты модулей ОЗУ. Сегодня практически все материнские платы используют в качестве системной памяти стандартные модули памяти. Рассмотрим три основных типа модулей памяти: SIMM, DIMM и RIMM.

SIMM и DIMM

Когда системы 386 получили наибольшее распространение, от специализированных модулей памяти компьютерная индустрия уже отказалась. На смену им пришел стандартный 30-выводной модуль памяти. Модуль SIMM легок, компактен, при этом содержит сравнительно крупный блок памяти, но, вероятно, огромным преимуществом SIMM является стандартизация — благодаря стандартному расположению выводов модуль SIMM можно установить почти на любом компьютере. 30-выводной модуль SIMM предусматривает 8 информационных бит и, как правило, содержит до 4 Мбайт ОЗУ. 30-выводной SIMM доказал свою полезность в системах 386 и ранних вариантах 486, но его объем оказался недостаточным для компьютеров более современных моделей. Немного более крупный 72-выводной модуль SIMM заменил 30-выводной SIMM; он предусматривает 32 информационных бита и может содержать до 32 Мбайт (и более) оперативной памяти.

Помимо SIMM, существуют устройства под названием DIMM. Складывается впечатление, что модули DIMM практически не отличаются от SIMM (рис. 9.13), но

физически модули DIMM крупнее. В то время как пары контактных площадок, расположенные на разных сторонах печатной платы модуля SIMM электрически связаны друг с другом, в модуле DIMM они автономны, таким образом количество контактов в устройстве фактически удваивается. Например, если посмотреть на 72-выводной модуль SIMM, можно увидеть по 72 электрических контакта на обеих сторонах устройства (всего 144 контакта), но они соединены, так что сигналов лишь 72 (несмотря на то, что контактов 144). А в DIMM эти контакты электрически изолированы (кроме того, в модуль DIMM обычно добавляется несколько дополнительных контактов, чтобы по ошибке не перепутать DIMM и SIMM). Сегодня практически все версии DIMM предусматривают 168 выводов (по 84 на каждой стороне). Впервые модуль DIMM появился в высокопроизводительных системах с 64-битовой информационной шиной (типа Pentium, PentiumPro и рабочих станций PowerPC RISC). По мере развития компьютерных систем модули DIMM полностью вытеснили SIMM, став предпочтительным устройством расширения, а на сегодняшний день типичные модули DIMM способны обеспечить 128 или 256 Мбайт очень быстрой памяти (типа PC133 SDRAM). Таким образом, сервер можно укомплектовать 512 Мбайт ОЗУ с помощью всего лишь нескольких модулей.

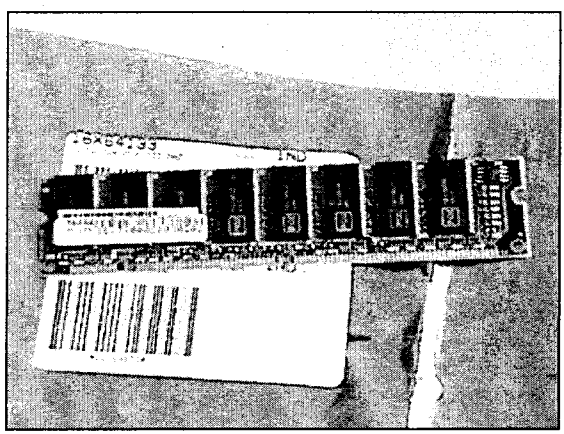


Рис. 9.13. Стандартные модули DIMM используются во многих компьютерах, серверах и рабочих станциях

Наконец, вы можете встретиться с тем, что модули SIMM и DIMM обозначаются как составные и несоставные. Иногда эти термины используются для обозначения технологического уровня модуля памяти. К примеру, в составном модуле применяется старая память низкой плотности, и поэтому для достижения необходимой емкости требуется больше кристаллов. Напротив, в несоставном модуле используется более современная технология памяти, так что для достижения той же емкости необходимо меньше кристаллов. Поэтому если вы встретите модуль SIMM высокой плотности с всего лишь несколькими кристаллами памяти, вероятнее всего, этот модуль является несоставным.

RIMM

В модулях RIMM используется память RDRAM. Модули RIMM сходны с DIMM, но они немного больше по размеру (металлические контакты разделены небольши-

ми промежутками). В первых реализациях RIMM было 168 выводов, но современные RIMM с частотой 600, 711 и 800 МГц (PC800) имеют 184 вывода. На рис. 9.14 показан типичный модуль RIMM, а также теплоотвод (или теплораспределитель), необходимый для борьбы с высокой температурой кристаллов RDRAM. В табл. 9.3 представлена расшифровка типичной маркировки модулей RIMM.

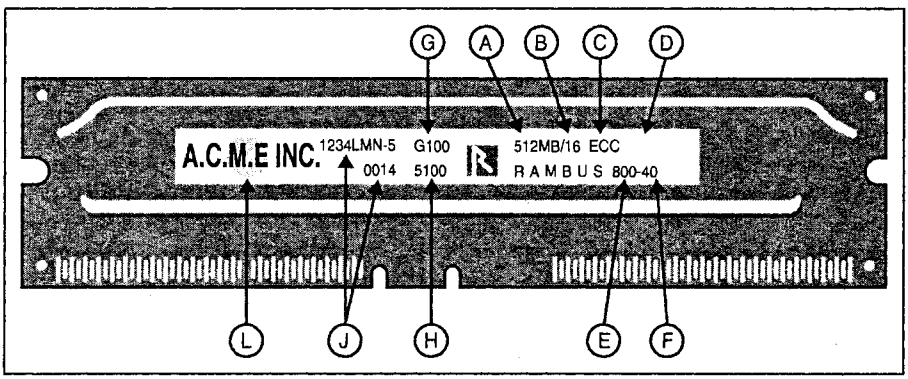


Рис. 9.14. Стандартный модуль RIMM (публикуется с разрешения Rambus)

Таблица 9.3. *Маркировка типичного модуля RIMM*

Элемент	Обозначение	Описание	Стандартные величины
A	Емкость памяти	8-битовая или 9-битовая емкость памяти RDRAM в модуле RIMM	512, 256, 128, 64 Мбайт
B	Устройства RDRAM	Количество устройств (кристаллов) RDRAM в модуле RIMM	16, 8, 4, 2
C	Поддержка ECC	Указывает на поддержку (или отсутствие поддержки) модулем RIMM кода ECC	Маркировка отсутствует: 8 бит без ECC; ECC: 9 бит
D	Зарезервировано	Зарезервировано для последующего применения	
E	Быстродействие памяти	Скорость передачи данных устройством RDRAM в модуле RIMM	800, 711 или 600 МГц
F	t_{RAC}	Время доступа к строке (факультативно)	–40, –45, –50 или –53 нс
G	Версия Gerber	Пересмотр файла PCB Gerber в модуле RIMM (факультативно)	Rev 1.00 = G100
H	Версия SPD	Версия кода SPD (факультативно)	Rev 1.00 = S100

Таблица 9.3 (окончание)

Элемент	Обозначение	Описание	Стандартные величины
J	Производитель	Номер детали, код даты или производителя — данные зависят от поставщика	
L	Производитель	Область логотипа поставщика или обозначения страны-производителя	

Память буферизованная, небуферизованная и регистрируемая

Есть три типа модулей памяти: небуферизованная, буферизованная и регистрируемая. Различие между ними заключается в методе обработки электрических сигналов, а выбор того или иного модуля влияет на максимальный объем ОЗУ, который можно установить на серверной материнской плате. Небуферизованная память содержит только запоминающие устройства, и обработка поступающих данных не ускоряется буферами самого модуля.

Небуферизованные модули работают быстро, потому что в них нет схемы буферизации, которая могла бы замедлять сигналы; стоят они немного меньше, что делает их привлекательными для обычных компьютеров. К сожалению, небуферизованные электрические сигналы подвержены затуханию, так что одновременно возможно использование лишь нескольких (как правило, одного или двух) небуферизованных модулей.

Усиление входящих и выходящих электрических сигналов производится путем добавления буферов или регистров в модуль памяти. При этом производительность модуля снижается на несколько наносекунд, но зато становится возможным использование дополнительных модулей памяти — таким образом, материнская плата может обеспечить поддержку большего объема памяти (это особенно важно для систем с большим объемом памяти типа сетевых серверов). Для модулей памяти EDO и FPM (Fast Page Mode — быстрый постраничный режим) процесс передвижения сигналов памяти называется *буферизацией*. Для модулей памяти SDRAM этот процесс называется *регистрацией*. Регистрация похожа на буферизацию, но при регистрации данные входят на модуль и выходят из него с помощью системного тактового генератора. Микросхема контроллера памяти на материнской плате определяет тип необходимых модулей памяти, поэтому совместное использование модулей небуферизованной и буферизованной (с регистрами) памяти в одной системе невозможно (более того, архитектура этих модулей памяти не допустит их установки на несовместимой материнской плате).

Четность и корректирующий код

Очень важно обеспечить безошибочность данных и команд программ. Всего лишь один неправильный бит, порожденный электрическими помехами или отказом компонента, может привести к аварийному отказу компьютера, повредить данные на

диске, вызвать сбой видеосигнала и стать причиной множества других неисправностей. Разработчики, обратившись к проблеме целостности памяти, создали метод контроля по четности (он же применяется для проверки целостности последовательных данных). Уже позднее в компьютерах (особенно в системах повышенной надежности типа серверов) была реализована более мощная и универсальная схема контроля ошибок под названием кода ECC.

Принцип четности

Основная идея четности проста: каждый байт, записываемый в память, проверяется, и к нему добавляется девятый бит (контрольный бит четности), выполняющий функции проверки. Когда позже ячейка памяти считывается процессором, схема проверки памяти в материнской плате вычисляет ожидаемый контрольный бит четности и сравнивает его с тем битом, который фактически считывается из памяти. Таким образом, система получает возможность постоянно диагностировать системную память, проверяя целостность ее данных. Если считанный контрольный бит четности соответствует ожидаемому, данные (и косвенно ОЗУ) признаются действительными, и процессор может продолжить выполнение своих задач. Если считанный и ожидаемый контрольные биты четности не совпадают, система регистрирует ошибку и приостанавливается. Контрольный бит четности присваивается каждому байту, так что в 32-битовой системе на каждый адрес ячейки приходится по 4 бита четности. В 64-битовой системе на каждый адрес будет приходиться по 8 таких битов и т. д.

Несмотря на то, что контроль по четности зарекомендовал себя как простое и эффективное средство постоянной проверки памяти, с ним связано два серьезных ограничения. Во-первых, контроль по четности может выявить ошибку, но не может ее исправить, потому что у него нет способа определить, какой бит поврежден. Именно поэтому при обнаружении ошибки четности система приостанавливается. Во-вторых, контроль по четности не способен выявлять многобитовые ошибки. К примеру, если в пределах одного байта единица случайно станет нулем, а нуль — единицей, условия четности будут, тем не менее, соблюдены. К счастью, вероятность многобитовой ошибки в рамках одного байта чрезвычайно низка. В принципе, использовать проверку четности совершенно необязательно, и в современных настольных системах довольно распространены модули памяти без контроля по четности. Но серверы как системы повышенной надежности требуют реализации проверки ошибок, которая могла бы уберечь их от больших (и дорогостоящих) ошибок данных.

ECC и EOS

В мире персональной вычислительной техники контроль по четности признается устаревшей технологией. Ее можно было бы заменить более сложными методиками типа кода ECC или кода ECC на SIMM (ECC On SIMM — EOS). Код ECC (методика, в настоящее время распространенная в профессиональных системах ПК и на файловых серверах) заключается в применении математического процесса в сочетании с контроллером памяти материнской платы и добавлении нескольких битов ECC к битам данных. Когда данные считываются из памяти, контроллер памяти ECC выполняет их проверку. Методика ECC обладает двумя важными преимуществами по сравнению с контролем по четности. Во-первых, она действительно может

сразу исправлять однобитовые ошибки, и пользователь даже не узнает об их наличии. Кроме того, код ECC может успешно выявлять двух-, трех- и четырехбитовые ошибки, что делает ее очень мощным средством обнаружения ошибок. При обнаружении многобитовой ошибки код ECC не может исправить ее, но появится сообщение об ошибке, и система приостанавливается.

Для успешной реализации кода ECC к каждой ячейке необходимо добавлять 7 или 8 бит. В 32-битовой системе нужно использовать модули SIMM x39 или x40 (т. е. 8Mx39 или 8Mx40). Это сравнительно новые обозначения, но, если вы с ними встретитесь, знайте, что они обозначают SIMM с ECC. В качестве альтернативы в некоторых 64-битовых системах применяются два 36-битовых модуля SIMM; в результате получается 72 бита — 64 бита для данных и 8 бит для информации кода ECC (в противном случае они были бы заняты контролем по четности).

EOS — это сравнительно новая (и довольно дорогостоящая) технология, которая передает функции кода ECC самому модулю памяти, но предоставляет результаты кода ECC в виде четности, — таким образом, в то время как модуль памяти выполняет код ECC, материнская плата продолжает контроль четности. Это довольно интересный эксперимент, но вряд ли технология EOS сможет завоевать значительную долю рынка. Оснащение систем, использующих контроль по четности, памятью четности обойдется вам гораздо дешевле, чем установка памяти EOS.

Общие принципы поиска неисправностей

Несмотря на то, что большинство серверных материнских плат надежно работают в течение многих лет, все же существует множество потенциальных неисправностей материнских плат и периферийных устройств. Работа с серверами является настоящим вызовом для технических специалистов, т. к. неисправности на сервере влияют на всю сеть, а вышедший из строя сервер может причинить компании с активным оборотом убытки в несколько тысяч долларов за каждый час простоя. Для вас, как для специалиста, чрезвычайно важно разбираться в неисправностях сервера и быть готовым справиться с ними как можно скорее.

Перезагрузка системы

Некоторые сбои в работе сервера могут происходить вследствие влияния внешних факторов типа перепадов напряжения или сбоев программного обеспечения; их можно без труда исправить путем простой перезагрузки сервера. Есть три варианта перезагрузки сервера: горячая перезагрузка, полный сброс и холодный пуск.

- При *горячей перезагрузке* очищается системная память и перезапускается операционная система. Чтобы запустить горячую перезагрузку, нажмите сочетание клавиш <Ctrl>+<Alt>+<Del>.
- При *полном сбросе* очищается системная память, перезапускается POST и перезагружается операционная система. Этот вариант может потребоваться, если полный отказ системы блокирует клавиатуру (делая безрезультатным нажатие <Ctrl>+<Alt>+<Del>). Чтобы выполнить полный сброс, нажмите кнопку Reset.
- При *холодном пуске* очищается системная память, перезапускается POST, перезагружается операционная система и прекращается подача питания всем перифе-

рийным устройствам. Выполнение холодного пуска может потребоваться после осуществления аппаратных обновлений или изменений. Нажмите кнопку Power.

Проблемы при запуске системы

Сервер должен загрузиться, пройти этап POST и запустить операционную систему; только после этого он сможет обслуживать сеть. Если сервер не загрузился, сеть будет находиться в автономном режиме до тех пор, пока вы не обнаружите и не устраните причину сбоя. К счастью, сбои при запуске системы, как правило, связаны с неправильной установкой (или настройкой) устройств. Данный список поможет вам выявить причины неисправности.

- ❒ Убедитесь в том, что шнуры питания системы надежно подключены.
- ❒ Нажмите кнопку Power на передней панели корпуса и убедитесь в том, что светится индикатор питания. Кроме того, проверьте работу охлаждающих вентиляторов.
- ❒ Проверьте правильность подключения и фиксации всех внутренних и внешних кабелей.
- ❒ Проверьте, надежно ли установлены процессоры в слотах на материнской плате. На незанятых слотах должны быть установлены заглушки.
- ❒ Убедитесь в том, что все платы PCI надежно установлены в слотах и прочно закреплены на корпусе.
- ❒ Убедитесь в том, что все переключатели и перемычки на материнской плате установлены правильно.
- ❒ Проверьте правильность установки всех перемычек и переключателей на платах расширения и периферийных устройствах.
- ❒ Проверьте правильность установки всех модулей DIMM. Тип, скорость и схема исправления ошибок модулей DIMM должны соответствовать вашей материнской плате. Некоторые материнские платы не позволяют запустить систему, если заняты не все слоты, отведенные для модулей DIMM.
- ❒ Проверьте правильность установки всех периферийных устройств.
- ❒ Если в системе есть накопитель на жестких дисках, зайдите в CMOS Setup и проверьте правильность его разбиения, форматирования и настройки.
- ❒ Проверьте правильность установки всех драйверов устройств. Возможно, для улучшения производительности вам придется загрузить обновленные версии драйверов основных устройств (например, драйверы хост-адаптера SCSI или сетевого адаптера).
- ❒ Убедитесь в правильности всех настроек SSU.
- ❒ Проверьте, нормально ли загружается операционная система.

Проблемы, связанные с программным обеспечением

- ❒ В дополнение к аппаратным проблемам, препятствовать нормальному функционированию сервера могут и сбои программного обеспечения (его дефекты и слу-

чаи несовместимости программ). Убедитесь в том, что система отвечает минимальным аппаратным требованиям для всего установленного программного обеспечения.

- ❒ Убедитесь в том, что вы используете зарегистрированную версию программы (а не модифицированную или OEM-версию).
- ❒ Проверьте качество носителя, с которого производилась первоначальная установка (попробуйте заведомо исправный установочный компакт-диск).
- ❒ Убедитесь в том, что компакт-диск не поврежден и не поцарапан.
- ❒ Проверьте правильность установки программного обеспечения (проведите повторную проверку установки).
- ❒ Удостоверьтесь в том, что установлены все необходимые драйверы устройств.
- ❒ Проверьте правильность настройки программного обеспечения по отношению именно к вашей системе.
- ❒ Обратитесь к документации программного обеспечения и убедитесь в правильности своих действий.

Когда возникают проблемы

Даже когда системное программное и аппаратное обеспечение готово к работе, сбои в работе сервера могут произойти и в процессе работы сервера. Если сбой произошел после некоторого времени безотказной работы аппаратного и программного обеспечения, то причиной его обычно является неисправность устройств (например, выход из строя накопителя или контроллера). К аппаратным неисправностям могут привести обновления и изменения в системе. В большинстве случаев неисправности аппаратуры сервера можно легко обнаружить и устранить. Данный список поможет вам выявить наиболее очевидные неисправности.

- ❒ Если вы запускаете программу с дискеты, попробуйте воспользоваться другой дискетой с ее копией; кроме того, можно попытаться освободить дисковод гибких дисков, а затем повторно вставить в него дискету.
- ❒ Если вы запускаете программу с компакт-диска, попробуйте воспользоваться другим компакт-диском, чтобы узнать, сохранится ли неисправность при других дисках; попробуйте вставить компакт-диск в другой дисковод, очистите сомнительный дисковод или замените подозрительный диск.
- ❒ Если вы запускаете программу с жесткого диска, попробуйте запустить ее с дискеты или с компакт-диска. Если в этом случае программа работает нормально, значит, проблема связана с той ее копией, которая записана на жестком диске. Переустановите программу на жестком диске и попытайтесь запустить ее еще раз. Убедитесь в том, что все необходимые файлы были установлены.
- ❒ Если неисправности в системе носят периодический характер, вполне возможно, что они вызваны неплотным креплением кабеля или платы расширения, недостаточным энергоснабжением или сбоем другого компонента системы. Чтобы выявить конкретную проблему, проведите диагностику или проанализируйте выводимые сообщения об ошибках.

- Если не удается ввести данные с помощью клавиатуры или мыши, то причиной этого может быть загрязнение этих устройств; почистив их, вы можете продолжать ими пользоваться.
- Если вы считаете, что произошел перепад напряжения, нарушение или снижение энергоснабжения, перезапустите программное обеспечение (или перезагрузите систему) и попытайтесь выполнить запуск системы. Симптомами перепадов напряжения является мерцание изображения на мониторе, внезапные перезагрузки системы и ее отказ реагировать на команды пользователя.

Примечание

Если вы сталкиваетесь со случайными ошибками в данных, возможно, что файлы были повреждены перепадами напряжения на линии переменного тока. В такой ситуации между розеткой и шнурами питания системы имеет смысл установить новый стабилизатор напряжения.

Анализ сообщений журнала системных событий

Программа SEL (System Event Log — журнал системных событий) — это интерфейс, который предоставляет пользователям и техническим специалистам возможность доступа к журналу системных событий. Обратиться к этому интерфейсу можно как с порта EMP, так и с помощью утилиты настройки системы (SSU). Программа просмотра извлекает данные из журнала системных событий и представляет их пользователю в шестнадцатеричном или расширенном формате. Пользователи могут также сохранять текущие данные журнала системных событий в файле (для последующего анализа) и очищать его текущие записи на сервере. В этой части главы мы рассмотрим типичные коды журнала системных событий, относящиеся к серверным материнским платам типа L440GX+. Администратор или технический специалист может использовать данные журнала для текущего контроля предупреждений серверной системы (например, об открытии корпуса системного блока) или потенциально опасных неисправностей (например, выхода из строя процессора или превышения температурного порога). В современных серверных системах контроль событий может производиться контроллером BMC (Baseboard Management Controller — контроллер управления материнской платой), контроллером HSC (Hot Swap Controller — контроллер горячей замены) и BIOS.

Сенсорные события

Сенсоры часто применяются для определения нескольких событий в сервере и за его пределами (уровень напряжения и температуры, работа вентилятора и проникновение в корпус системного блока). Когда сенсор фиксирует наступление события, это событие регистрируется в журнале системных событий. К примеру, если температура задней панели сервера превысила установленный предел, температурный сенсор регистрирует это событие как "01 01" (в шестнадцатеричном формате). В табл. 9.4 приводятся типы сенсоров и числа, которые обычно им соответствуют.

События BIOS

Базовая система ввода/вывода (BIOS) отвечает за мониторинг и регистрацию некоторых системных событий, ошибок памяти и критических прерываний. BIOS отсылает

контроллеру BMC сообщение запроса события с целью регистрации этого события. Некоторые ошибки (например, неисправность процессора) регистрируются на ранней стадии POST. Когда событие выявляется BIOS, оно регистрируется в журнале системных событий. К примеру, если происходит событие загрузки системы, BIOS регистрирует его как "12 EF E7 01" (в шестнадцатеричном формате). В табл. 9.5 приведены типичные для сервера события BIOS.

Таблица 9.4. *Стандартные события сенсоров журнала системных событий*

Тип сенсора		Число сенсора	Имя сенсора	Обозначение генератора
Расширенный	**Шестнадцатеричный**			
Температурный	01h			
		01h	Температура задней панели	HSC
		17h	Температура первичного процессора	BMC
		18h	Температура вторичного процессора	BMC
		19h	Температура материнской платы 1	BMC
		1Ah	Температура материнской платы 2	BMC
Напряжение	02h			
		01h	Материнская плата, 5 В	BMC
		02h	Материнская плата, 3,3 В	BMC
		03h	Первичный процессор	BMC
		04h	Вторичный процессор	BMC
		05h	Процессор, 2,5 В	BMC
		06h	Резервное питание, 5 В	BMC
		07h	SCSI-W LVDS Term1	BMC
		08h	SCSI-W LVDS Term2	BMC
		09h	Резервное питание, 3 В (Wake On LAN)	BMC
		0Ah	Материнская плата –12 В	BMC
		0Bh	Материнская плата SCSI-W SGL Term	BMC
		0Ch	Процессор, 1,5 В	BMC
		0Dh	Материнская плата –5 В	BMC
		0Eh	Материнская плата –12 В	BMC

Таблица 9.4 *(продолжение)*

Тип сенсора		Число сенсора	Имя сенсора	Обозначение генератора
Расширенный	**Шестнадцатеричный**			
Вентилятор	04h			
		0Ch	Вентилятор задней панели 1	HSC
		0Dh	Вентилятор задней панели 2	HSC
		0Fh	Вентилятор материнской платы 0	BMC
		10h	Вентилятор материнской платы 1	BMC
		11h	Вентилятор процессора 0	BMC
		12h	Вентилятор процессора 1	BMC
		1Fh	Цифровой вентилятор 1	BMC
		20h	Цифровой вентилятор 2	BMC
		21h	Цифровой вентилятор 3	BMC
		22h	Цифровой вентилятор 4	BMC
Физическая безопасность	05h			
		26h	Проникновение в корпус системного блока	BMC
Безопасного режима	06h			
		27h	Пароль порта EMP	BMC
		28h	Сенсор безопасного режима	BMC
Процессор	07h			
		1Bh	Состояние первичного процессора	BMC
		1Ch	Состояние вторичного процессора	BMC
Память	0Ch			
		EFh	Повреждение памяти	BMC
Слот (отсек) диска	0Dh			
		02h	Состояние слота диска 0	HSC
		03h	Состояние слота диска 1	HSC

Таблица 9.4 (окончание)

Тип сенсора		Число сенсора	Имя сенсора	Обозначение генератора
Расширенный	Шестнадцатеричный			
		04h	Состояние слота диска 2	HSC
		05h	Состояние слота диска 3	HSC
		06h	Состояние слота диска 4	HSC
		07h	Наличие слота диска 0	HSC
		08h	Наличие слота диска 1	HSC
		09h	Наличие слота диска 2	HSC
		0Ah	Наличие слота диска 3	HSC
		0Bh	Наличие слота диска 4	HSC
Ошибки POST	0Fh			
		25h	Системная ошибка *(см. табл. POST)*	
Схема самоконтроля	11h			
		1Dh	Схема самоконтроля BMC	BMC
Системное событие	12h			
		EFh	Системная ошибка	
Критическое прерывание	13h			
		1Eh	NMI передней панели	BMC

***Таблица 9.5.** Стандартные события журнала системных событий BIOS*

Тип сенсора	Номер сенсора	Описание события (шестнадцатеричный формат)	Тип события
12	EF	---	---
		E7 01	Событие загрузки системы
		E7 00	Изменение настройки системы
0C	EF	---	---
		E7 40 [DIMM#]	Однобитовая ошибка памяти
		E7 41 [DIMM#]	Многобитовая ошибка памяти
		E7 02	Ошибка четности памяти

Таблица 9.5 (окончание)

Тип сенсора	Номер сенсора	Описание события (шестнадцатеричный формат)	Тип события
13	28	---	---
		E7 00	NMI передней панели
13	EF	---	---
		E7 01	Блокировка шины по времени
		E7 02	Проверка ввода/вывода
		E7 03	Программное NMI
		E7 04	PERR PCI

События POST

Критические ошибки в важнейших устройствах (например, неисправность процессора) регистрируются на ранней стадии POST. Когда событие обнаруживается BIOS в начале POST, оно регистрируется в журнале системных событий. К примеру, если происходит отказ жесткого диска, BIOS регистрирует это событие как "0F — 00 02" (в шестнадцатеричном формате). Удобно, что ошибки, относящиеся к POST и регистрируемые в журнале системных событий, можно просмотреть без платы считывания POST. В табл. 9.6 приводятся события POST, которые обычно регистрируются BIOS.

***Таблица 9.6.** Стандартные события POST*

Тип события	Объяснение
00 02	Аварийный жесткий диск
00 81	Отказ BIST процессора 0
01 04	Недействительные данные настройки системы — запустите утилиту настройки
01 06	Изменение настройки устройства
01 81	Отказ BIST процессора 1
02 06	Ошибка настройки — устройство заблокировано
03 04	Конфликт на уровне ресурсов
04 04	Конфликт на уровне ресурсов
04 05	Конфликт на уровне ресурсов
04 81	Сбой из-за внутренней ошибки (IERR) процессора 0
05 04	Расширительное ПЗУ не инициализировано
05 05	Расширительное ПЗУ не инициализировано

Таблица 9.6 *(продолжение)*

Тип события	Объяснение
05 81	Сбой из-за внутренней ошибки (IERR) процессора 1
06 04	Предупреждение: линия IRQ не настроена
06 05	Предупреждение: линия IRQ не настроена
06 81	Отказ системы термоконтроля процессора 0
07 81	Отказ системы термоконтроля процессора 1
08 81	Отказ сторожевого таймера во время последней загрузки
0A 81	Сбой инициализации процессора 1 во время последней загрузки
0B 81	Неудача инициализации процессора 0 во время последней загрузки
0C 81	Процессор 0 блокирован, система находится в однопроцессорном режиме
0D 81	Процессор 1 блокирован, система находится в однопроцессорном режиме
0E 81	Отказ таймера FRB 3-го уровня на процессоре 0
0F 81	Отказ таймера FRB 3-го уровня на процессоре 1
10 02	Запавшая (нажатая) клавиша
10 81	Не работает интерфейс SMI (Server Management Interface — интерфейс управления сервером)
11 02	Ошибка клавиатуры
12 02	Отказ контроллера клавиатуры
13 02	Клавиатура заблокирована — снимите блокировку
20 02	Тип монитора не соответствует CMOS — запустите Setup
20 81	Подсистема ввода/вывода нефункциональна
30 02	Отказ системного ОЗУ на смещении <xxxxx>
31 02	Отказ теневой памяти на смещении <xxxxx>
32 02	Отказ расширенного ОЗУ на смещении <xxxxx>
50 02	Батарея материнской платы не действует — замените и запустите Setup
50 81	Энергонезависимое ОЗУ очищена перемычкой
51 02	Недействительная контрольная сумма системного CMOS — применяется конфигурация по умолчанию
51 81	Ошибка контрольной суммы энергонезависимого ОЗУ — энергонезависимая память очищена
52 81	Данные энергонезависимого ОЗУ недействительны — энергонезависимая память очищена

Таблица 9.6 (окончание)

Тип события	Объяснение
60 02	Ошибка системного таймера
62 01	BIOS не может применить свои обновления к процессору 1
63 01	BIOS не может применить свои обновления к процессору 2
64 01	BIOS не поддерживает текущее пошаговое исполнение для процессора 1
65 01	BIOS не поддерживает текущее пошаговое исполнение для процессора 2
70 02	Ошибка часов реального времени (RTC)
97 02	Ошибка памяти ECC при тестировании базовой (расширенной) памяти в блоке <xx>
B2 02	Неверный тип дисковода A: — запустите Setup
B3 02	Неверный тип дисковода B: — запустите Setup
D0 02	Ошибка системного кэша — кэш заблокирован
F5 02	Сбой при тестировании DMA
F6 02	Отказ программного NMI

Коды и сообщения POST

Когда происходят критические ошибки, загрузка материнской платы может не завершиться; в результате запуск операционной системы или диагностического программного обеспечения будет невозможен. Но во время процесса загрузки BIOS посылает двузначные шестнадцатеричные коды (они называются кодами POST) в порт ввода/вывода 80h. Если установить ISA-плату считывания POST, эти коды можно будет просмотреть. Если система останавливается на определенном коде, то по этому коду можно вычислить состояние POST и определить последний успешно завершенный этап. В табл. 9.7 приводится стандартный набор кодов POST для современных BIOS серверного типа. Если система загружается до момента инициализации видеосистемы, ошибки могут отображаться в виде четырехзначных кодов, показанных в табл. 9.8. Чтобы расшифровать точное значение каждого кода, вам понадобится документация к материнской плате вашего сервера.

Таблица 9.7. Типичные коды POST

Код	Звуковые сигналы	Ошибка
02h		Подтвердить реальный режим
04h		Установить тип процессора
06h		Инициализировать системное аппаратное обеспечение
08h		Инициализировать регистры набора микросхем посредством исходных значений POST

Таблица 9.7 (продолжение)

Код	Звуковые сигналы	Ошибка
09h		Установить флаг POST
0Ah		Инициализировать регистры процессора
0Bh		Активировать кэш процессора
0Ch		Инициализировать кэш до исходных значений POST
0Eh		Инициализировать ввод/вывод
0Fh		Инициализировать локальную шину IDE
10h		Инициализировать управление режимом электропитания
11h		Загрузить резервные регистры посредством исходных значений POST
12h		Восстановить контрольное слово процессора в ходе горячей перезагрузки
14h		Инициализировать контроллер клавиатуры
16h	1-2-2-3	Контрольная сумма ПЗУ BIOS
18h		Инициализация таймера 8254
1Ah		Инициализация DMA-контроллера 8237
1Ch		Восстановить программируемый контроллер прерываний 0
20h	1-3-1-1	Проверить обновление DRAM
22h	1-3-1-3	Проверить контроллер клавиатуры 8742
24h		Приравнять регистр сегмента ES к 4 Гбайт
28h	1-3-3-1	Выполнить автоматическую регулировку размеров DRAM
2Ah		Очистить 512 Кбайт базового ОЗУ
2Ch	1-3-4-1	Отказ ОЗУ на адресной линии <xxxx>
2Eh	1-3-4-3	Отказ ОЗУ на информационных битах <xxxx> младшего байта шины памяти
30h	1-4-1-1	Отказ ОЗУ на информационных битах <xxxx> старшего байта шины памяти
32h		Выполнить тестирование тактовой частоты шины процессора
34h		Выполнить тестирование CMOS
35h		ОЗУ инициализирует резервные регистры набора микросхем
36h		Приостановление горячей перезагрузки
37h		Выполнить повторную инициализацию набора микросхем материнской платы
38h		Теневое ПЗУ системной BIOS

Таблица 9.7 (продолжение)

Код	Звуковые сигналы	Ошибка
39h		Выполнить повторную инициализацию кэша материнской платы
3Ah		Выполнить автоматическую регулировку размеров кэша
3Ch		Выполнить настройку расширенных регистров набора микросхем
3Dh		Загрузить резервные регистры с помощью значений CMOS
40h		Установить новую начальную скорость процессора
42h		Инициализировать векторы прерываний
44h		Инициализировать прерывания BIOS
46h	2-1-2-3	Проверить уведомление об авторских правах на ПЗУ
47h		Инициализировать диспетчер для расширительных ПЗУ на PCI
48h		Сверить видеоконфигурацию с CMOS
49h		Инициализировать шину и устройства PCI
4Ah		Инициализировать все видеоадаптеры в системе
4Bh		Вывести экран QuietBoot
4Ch		Теневое ПЗУ видео-BIOS
4Eh		Вывести уведомление об авторских правах
50h		Вывести тип и скорость процессора
51h		Инициализировать плату EISA
52h		Выполнить тестирование клавиатуры
54h		Задать нажатие клавиши, если она не заблокирована
56h		Активировать клавиатуру
58h	2-2-3-1	Выполнить поиск непредвиденных прерываний
5Ah		Вывести строку "Press F2 to enter Setup"
5Ch		Протестировать ОЗУ между 512 и 640 Кбайт
60h		Провести тестирование расширенной памяти
62h		Провести тестирование адресных линий расширенной памяти
64h		Перейти к UserPatch1
66h		Выполнить настройку расширенных регистров кэша
68h		Включить внешний кэш и кэш процессора

Таблица 9.7 *(продолжение)*

Код	Звуковые сигналы	Ошибка
6Ah		Вывести размер внешнего кэша
6Ch		Вывести теневое сообщение
6Eh		Вывести несвободные сегменты
70h		Вывести сообщение (сообщения) об ошибке
72h		Выполнить проверку на предмет ошибок настройки
74h		Выполнить проверку часов реального времени
76h		Выполнить тестирование клавиатуры
7Ah		Выполнить проверку блокировки клавиши
7Ch		Задать аппаратные векторы прерывания
7Eh		Выполнить проверку сопроцессора, если он установлен
80h		Обнаружить и установить внешние порты RS232
82h		Обнаружить и установить внешние параллельные порты
85h		Инициализировать ISA-устройства, совместимые со стандартом Plug-and-Play
86h		Провести повторную инициализацию встроенных портов ввода/вывода
88h		Провести инициализацию области данных BIOS
8Ah		Провести инициализацию расширенной области данных BIOS
8Ch		Инициализировать контроллер гибких дисков
90h		Инициализировать контроллер жестких дисков
91h		Инициализировать контроллер жестких дисков на локальной шине
92h		Перейти к UserPatch2
93h		Построить MPTABLE для многопроцессорных плат
94h		Отключить адресную линию A20
95h		Установить CD-ROM для загрузки
96h		Очистить большой регистр сегмента ES
98h	1-2	Провести поиск расширительных ПЗУ. Два коротких звуковых сигнала при неудаче контрольной суммы
9Ah		Теневые расширительные ПЗУ
9Ch		Настроить управление режимом электроснабжения
9Eh		Включить аппаратные прерывания

Таблица 9.7 *(окончание)*

Код	Звуковые сигналы	Ошибка
A0h		Установить время суток
A2h		Проверить установку времени
A4h		Инициализировать частоту повторения
A8h		Стереть подсказку <F2>
Aah		Провести сканирование на предмет нажатия клавиши <F2>
Ach		Войти в Setup
Aeh		Снять флаг in-POST
B0h		Провести поиск ошибок
B2h		POST выполнено — подготовиться к загрузке операционной системы
B4h		Один короткий звуковой сигнал перед boot0
B5h		Вывести меню MultiBoot
B6h		Проверить пароль (необязательно)
B8h		Очистить таблицу глобального дескриптора
BCh		Очистить блоки проверки четности
Beh		Очистить экран (необязательно)
BFh		Проверить напоминания о вирусах и резервных копиях
C0h		Провести попытку загрузки с интервалом 19
D0h		Ошибка обработчика прерываний
D4h		Ошибка задержки прерывания
D6h		Инициализировать ошибку расширительного ПЗУ
D8h		Ошибка отключения
Dah		Перемещение расширенного блока
DCh		Ошибка отключения 10
FFh		Завершение POST

Таблица 9.8. *Стандартные сообщения об ошибках POST*

Код	Ошибка
0162	BIOS не может применить свои настройки к процессору 1
0163	BIOS не может применить свои настройки к процессору 1
0164	BIOS не поддерживает текущее пошаговое исполнение для процессора 1

Таблица 9.8 *(продолжение)*

Код	Ошибка
0165	BIOS не поддерживает текущее пошаговое исполнение для процессора 2
0200	Сбой: жесткий диск
0210	Запавшая (нажатая) клавиша
0211	Ошибка клавиатуры
0212	Сбой контроллера клавиатуры
0213	Клавиатура заблокирована — разблокируйте клавиатуру
0220	Тип монитора не соответствует настройкам CMOS — запустите Setup
0230	Сбой системного ОЗУ на смещении <xxxxx>
0231	Сбой теневого ОЗУ на смещении <xxxxx>
0232	Сбой расширенного ОЗУ на смещении <xxxxx>
0250	Батарея материнской платы не работает — замените батарею и запустите Setup
0251	Неверная контрольная сумма CMOS (применена конфигурация по умолчанию) — замените микросхему ОЗУ CMOS
0260	Сбой системного таймера
0270	Сбой часов реального времени
0297	Сбой памяти ECC при тестировании базовой (или расширенной) памяти в блоке <xx>
02B2	Ошибка дисковода A: — запустите Setup
02B3	Ошибка дисковода B: — запустите Setup
02D0	Сбой системного кэша — кэш заблокирован
02F5	Сбой при тестировании DMA
02F6	Сбой программного NMI
0401	Неверные данные о настройках системы — запуск утилиты настройки
0403	Конфликт на уровне ресурсов
0404	Конфликт на уровне ресурсов
0405	Расширенное ПЗУ не инициализировано
0406	Предупреждение: линия IRQ не настроена
0504	Конфликт на уровне ресурсов
0505	Расширенное ПЗУ не инициализировано
0506	Предупреждение: линия IRQ не настроена
0601	Конфигурация устройства изменена
0602	Ошибка конфигурации — устройство заблокировано

Таблица 9.8 (окончание)

Код	Ошибка
8100	Отказ системы BIST процессора 1
8101	Отказ системы BIST процессора 2
8104	Сбой из-за внутренней ошибки процессора 1
8105	Сбой из-за внутренней ошибки процессора 2
8106	Отказ системы термоконтроля процессора 1
8107	Отказ системы термоконтроля процессора 2
8108	Отказ сторожевого таймера во время последней загрузки
810A	Сбой инициализации процессора 2 во время последней загрузки
810B	Сбой инициализации процессора 1 во время последней загрузки
810C	Процессор 1 заблокирован, система находится в однопроцессорном режиме
810D	Процессор 2 заблокирован, система находится в однопроцессорном режиме
810E	Отказ таймера загрузки FRB 3-го уровня на процессоре 1
810F	Отказ таймера загрузки FRB 3-го уровня на процессоре 2
8110	Не работает интерфейс SMI
8120	Подсистема ввода/вывода не работает
8150	Энергонезависимое ОЗУ очищено переключателем
8151	Ошибка контрольной суммы энергонезависимого ОЗУ — энергонезависимое ОЗУ очищено
8152	Данные энергонезависимого ОЗУ неверны — энергонезависимое ОЗУ очищено

Служебный раздел

Служебный раздел — это специальный раздел жесткого диска; он создается во время первой настройки сервера и содержит утилиты, диагностические средства и прочее программное обеспечение, необходимое для удаленного управления. Служебный раздел не помечается как активный, и загрузку с него сервер производит только по специальному запросу. Обычно пользователь его не видит, т. к. в нем используется специальный нестандартный тип раздела, который не проявляется в виде доступной файловой системы. Тем не менее низкоуровневые дисковые утилиты могут видеть этот раздел и рассматривать его как неизвестную область. Как правило, создавать служебный раздел следует до установки операционной системы. Организация служебного раздела выполняется следующим образом:

1. Загрузитесь с компакт-диска серверного ПО.
2. После появления меню **Server Board** (Пульт сервера) компакт-диска выберите меню **Utilities** (Утилиты) и нажмите клавишу <Enter>.

3. Выберите **Run Service Partition Administrator** (Запустить Администратор служебного раздела) и нажмите клавишу <Enter>.
4. Выберите **Create service partition** (Создать служебный раздел).
5. Следуйте инструкциям по выбору жесткого диска для установки служебного раздела.
6. Перезагрузитесь с программного компакт-диска сервера.
7. После появления меню **Server Board** компакт-диска выберите меню **Utilities** и нажмите клавишу <Enter>.
8. Выберите **Run Service Partition Administrator** и нажмите клавишу <Enter>.
9. Выберите **Format service partition and install software** (Форматировать служебный раздел и установить ПО).
10. Следуйте инструкциям по форматированию служебного раздела и установке программ в этот раздел.

Примечание

Служебный раздел используется не во всех системах. В документации к вашему серверу должно быть указано, разрешен ли он в вашей системе.

Ремонт разъемов DIMM/RIMM

Если в архитектуре DIMM и RIMM и есть слабое звено, так это разъем, который соединяет эти модули с материнской платой. Модуль памяти должен сначала без усилий устанавливаться в этот разъем, а затем мягко извлекаться; при этом, находясь в разъеме, он удерживается двумя зажимами с обеих сторон. На самом деле, чтобы установить модуль в слот, на него нужно надавить. Вытаскивать его не менее сложно. В результате разъемы часто ломаются, и ваша дополнительная память становится совершенно бесполезной.

Теоретически лучше всего было бы снять поврежденный разъем и установить новый. Но это не так просто. Во-первых, для снятия старого разъема вам нужно снять материнскую плату и выпаять поврежденный разъем, а затем впаять новый (который можно приобрести в универсальном магазине электроники типа DigiKey). Если за дело примется опытный технический специалист, располагающий нужными инструментами, для него эта задача не будет представлять особой трудности. Но дело в том, что печатная плата чрезвычайно хрупка, малейший перегрев может легко повредить тонкие многослойные соединения и тем самым окончательно испортить материнскую плату.

К счастью, есть несколько приемов, которые могут вам помочь. Если один или оба зажима модуля согнулись или сломались, возьмите резиновую ленту средней упругости, длина которой примерно на 1 дюйм меньше длины разъема. Обмотайте этой резинкой модуль и разъем, это поможет удержать модуль на месте. Если какая-либо часть разъема треснет или сломается, ее можно будет починить (или по крайней мере усилить) качественной эпоксидной смолой. Если вы решите воспользоваться этим материалом, обеспечьте хорошую вентиляцию и дайте эпоксидной смоле достаточно времени, чтобы высохнуть. Если это не решит проблему, то хотя бы остановит ее развитие и даст материнской плате возможность прослужить вам еще долго.

Коррозия контактов

Коррозия может появиться на контактах SIMM/DIMM/RIMM, если разъемы модуля и слота сделаны из разных металлов. В конечном итоге контакт будет нарушен. Сначала следует проверить, из каких материалов сделаны контакты модуля и слота (обычно это олово или золото). Возможно, вам удастся быстро справиться с этой проблемой, вручную подчистив контакты от следов коррозии, воспользовавшись для этих целей ватной палочкой и очистителем контактов для электронных промышленных изделий. Впрочем, если вы обнаружите, что металлы на разъеме и модуле различны, попробуйте уговорить компанию, продавшую вам память, обменять ее на другую.

Ошибки четности

Ошибки четности составляют значительную часть ошибок памяти, с которыми вам, как техническому специалисту, придется столкнуться. Как вы уже знаете, четность является важным компонентом самоконтроля компьютера. Ошибки в памяти заставляют систему приостанавливаться; это делается для того, чтобы, продолжив работу фактически вслепую, не натолкнуться на ошибку с критическими последствиями. Но появление ошибок четности вызывает не только память. На четность может влиять конфигурация системы. Ниже перечислены основные причины появления ошибок четности:

- один или несколько бит памяти неустойчивы или полностью повреждены;
- отсутствие хорошего контакта в разъемах памяти SIMM/DIMM/RIMM;
- в настройках BIOS введено слишком мало периодов ожидания (память слишком медленна по сравнению с процессором);
- в системе питания произошел внезапный сбой;
- выполняется ошибка программы, компьютерный вирус или какие-либо другие опасные программы;
- в интегральной схеме контроллера памяти или в BIOS произошел сбой.

Когда вы сталкиваетесь с ошибкой четности после обновления памяти, логично предположить наличие проблемы с периодами ожидания или настройками типа памяти в CMOS Setup, поэтому именно это нужно проверить в первую очередь. Если периоды ожидания и другие настройки памяти правильны, попробуйте методично снимать каждый модуль памяти, прочищать контакты и осторожно устанавливать модуль обратно. Если ошибки будут продолжаться, попытайтесь снять один банк модулей памяти одновременно (возможно, память неисправна). Быть может, вам придется перераспределить память, чтобы банк 0 оставался заполненным. Если после этого ошибка исчезнет, значит, снятая память действительно была неисправной.

Когда ошибки четности происходят непредвиденно (без явной причины), для начала нужно почистить и переустановить каждый модуль памяти. Так вы убедитесь в том, что причина заключается не в плохих контактах. После этого следует проверить выходы электропитания — низкий уровень выходного сигнала и содержащиеся в нем помехи могут приводить к случайным ошибкам в сигналах. Возможно, если блок питания перегружен, его придется заменить. Попытайтесь загрузить систему

Симптом 9.3. Во время запуска система не подает звуковые сигналы

Обычно при успешном прохождении POST из динамика сервера транслируется один звуковой сигнал. Если такого сигнала не последовало, но система работает нормально, то, вероятно, динамик неисправен или плохо подсоединен к материнской плате. Проверьте соединение динамика и при необходимости замените его. Если сигнал не поступил и система не отвечает, возможно, неисправно электроснабжение (источник питания). Кроме того, неисправность может быть связана с материнской платой или с первичным процессом (система не может завершить POST).

Симптом 9.4. Система подает звуковой код ошибки

BIOS отслеживает текущее состояние тестирования системы во время POST путем вывода двузначного шестнадцатеричного кода на порт 80h. При наличии платы считывания POST она отображает двузначный код на паре семисегментных светодиодов. Когда POST сталкивается с неисправностью, система, как правило, издает звуковой сигнал, тем самым извещая вас о проблеме, и, воспользовавшись платой считывания POST, вы можете определить последний успешно завершенный этап POST. Сравнивая последний этап POST с перечнем кодов для вашей версии BIOS (в документации к материнской плате), вы сможете определить, в какой момент произошел сбой POST, и сделать предположение относительно возможной неисправности. Во многих случаях значительные сбои, обнаруженные с помощью POST, можно устранить путем замены материнской платы.

Симптом 9.5. Система выводит сообщение об ошибке POST

Если системе удалось инициализировать видеосистему, числовой код любой ошибки будет выведен на монитор. Сравнивая код ошибки POST с перечнем кодов для вашей версии BIOS, вы сможете определить, в какой момент произошел сбой POST, и сделать предположение относительно возможной неисправности. Во многих случаях серьезные неисправности, о которых система уведомляет вас в форме сообщений об ошибках POST, можно устранить путем замены материнской платы.

Симптом 9.6. Вы испытываете затруднения при использовании различных процессоров на серверной материнской плате

В большинстве случаев процессоры, применяемые на серверах, должны относиться к одному семейству; одновременно использовать разные процессоры не запрещено, но проверить надежность каждой их комбинации невозможно. Чтобы подобрать приемлемое сочетание, придерживайтесь следующих рекомендаций.

- Ни при каких условиях нельзя совмещать в одной системе процессоры Pentium II, Pentium III и Pentium 4.
- В рамках одной системы нельзя сочетать разные ядра процессоров и скорости шин (к примеру, процессоры с частотой 900 МГц и 1,2 ГГц, как правило, вместе не работают).
- В рамках одной системы нельзя использовать запоминающие устройства с поддержкой ECC и без нее.
- В рамках одной системы нельзя смешивать процессоры с разными размерами кэша L2.

Симптом 9.3. Во время запуска система не подает звуковые сигналы

Обычно при успешном прохождении POST из динамика сервера транслируется один звуковой сигнал. Если такого сигнала не последовало, но система работает нормально, то, вероятно, динамик неисправен или плохо подсоединен к материнской плате. Проверьте соединение динамика и при необходимости замените его. Если сигнал не поступил и система не отвечает, возможно, неисправно электроснабжение (источник питания). Кроме того, неисправность может быть связана с материнской платой или с первичным процессом (система не может завершить POST).

Симптом 9.4. Система подает звуковой код ошибки

BIOS отслеживает текущее состояние тестирования системы во время POST путем вывода двузначного шестнадцатеричного кода на порт 80h. При наличии платы считывания POST она отображает двузначный код на паре семисегментных светодиодов. Когда POST сталкивается с неисправностью, система, как правило, издает звуковой сигнал, тем самым извещая вас о проблеме, и, воспользовавшись платой считывания POST, вы можете определить последний успешно завершенный этап POST. Сравнивая последний этап POST с перечнем кодов для вашей версии BIOS (в документации к материнской плате), вы сможете определить, в какой момент произошел сбой POST, и сделать предположение относительно возможной неисправности. Во многих случаях значительные сбои, обнаруженные с помощью POST, можно устранить путем замены материнской платы.

Симптом 9.5. Система выводит сообщение об ошибке POST

Если системе удалось инициализировать видеосистему, числовой код любой ошибки будет выведен на монитор. Сравнивая код ошибки POST с перечнем кодов для вашей версии BIOS, вы сможете определить, в какой момент произошел сбой POST, и сделать предположение относительно возможной неисправности. Во многих случаях серьезные неисправности, о которых система уведомляет вас в форме сообщений об ошибках POST, можно устранить путем замены материнской платы.

Симптом 9.6. Вы испытываете затруднения при использовании различных процессоров на серверной материнской плате

В большинстве случаев процессоры, применяемые на серверах, должны относиться к одному семейству; одновременно использовать разные процессоры не запрещено, но проверить надежность каждой их комбинации невозможно. Чтобы подобрать приемлемое сочетание, придерживайтесь следующих рекомендаций.

- Ни при каких условиях нельзя совмещать в одной системе процессоры Pentium II, Pentium III и Pentium 4.
- В рамках одной системы нельзя сочетать разные ядра процессоров и скорости шин (к примеру, процессоры с частотой 900 МГц и 1,2 ГГц, как правило, вместе не работают).
- В рамках одной системы нельзя использовать запоминающие устройства с поддержкой ECC и без нее.
- В рамках одной системы нельзя смешивать процессоры с разными размерами кэша L2.

- Как правило, сочетание разных шагов процессора функционирует нормально, но различие между ядрами в двух процессорах на сервере не должно превышать один шаг. Первичный процессор должен отличаться от вторичного не более чем на один шаг в одну или другую сторону.

Симптом 9.7. Данные SPD перезаписаны

Некоторые сочетания серверного аппаратного обеспечения могут привести к повреждению данных SPD (Serial Presence Detect — последовательное обнаружение присутствия) памяти DIMM EEPROM. При этом некоторые биты 256-байтовой области данных SPD перезаписываются. Искажение данных может происходить только в области данных SPD — в основной памяти это невозможно. Данные SPD с EEPROM считываются только во время загрузки системы. Если данные SPD модуля DIMM повреждены, то блок памяти, содержащий DIMM, будет заблокирован, и в результате произойдет сбой:

- если установлен только один блок памяти, система не загрузится (по причине блокировки всей памяти);
- если установлено несколько блоков памяти, общий ее объем будет уменьшен в соответствии с количеством блокированных блоков (вплоть до всего объема памяти включительно).

Создается впечатление, что неисправна вся плата с модулями памяти, а вызвана эта неисправность неправильным терминированием выходов схемы, которая отвечает за выбор блока памяти. Возможность перезаписи данных SPD EEPROM, вероятно, существует лишь на открытых (с разрешением записи) модулях DIMM EEPROM, т. к. данные могут быть записаны в незащищенную 256-байтовую область данных SPD. В закрытой SPD-памяти EEPROM подобных сбоев не бывает, т. к. она защищена от перезаписи. Если вы столкнетесь с такой ситуацией, попробуйте воспользоваться другими модулями памяти или свяжитесь с производителем материнской платы для получения обновлений BIOS.

Симптом 9.8. В журнале системных событий зарегистрированы события сбоя напряжения

Некоторые серверные материнские платы регистрируют события, связанные с порогами напряжения, и они фиксируются в журнале системных событий. Такие события регистрируются для шин питания +12 В, +5 В и +1,5 В (и многочисленных компонентов). Есть возможность поступления ложных сигналов, на них можно не обращать внимания. Для устранения этой неисправности вы можете сменить источник питания или воспользоваться источником бесперебойного питания.

Симптом 9.9. Область настройки PCI на сервере не обновляется должным образом

Некоторые серверные системы могут зависать или работать неисправно после установки некоторых плат расширения PCI с микропроцессором ввода/вывода Intel i960. Это часто наблюдается в системах с некоторыми серверными материнскими платами и RAID-платой AMI MR493 (возможны и другие сочетания устройств). Кроме того, после включения во время конфигурации системы "горячей" установки устройств PCI (PCI Hot Plug, PHP) установка Windows 2000 может дать сбой, и эта операционная система будет зависать.

Эта неисправность определяется как сбой распределения ресурсов PCI в системе BIOS. Причина ее заключается в том, что процедура BIOS создает 1-мегабайтовую апертуру памяти на основной стороне моста PCI-PCI, который не имеет возможности должным образом закрыть эту апертуру. Возможно, вам понадобится изменить аппаратную конфигурацию (обычно удаляются подозрительные устройства PCI) и установить устройства, в которых этой неисправности не зафиксировано; с другой стороны, вы можете проверить наличие обновления BIOS, которое, возможно, устранит эту неисправность (или вообще заменить материнскую плату).

Симптом 9.10. При нахождении сервера в режиме ожидания происходит отказ включения питания

Это может случиться в системах с некоторыми серверными материнскими платами, использующими определенные источники питания. В режиме ожидания (когда переменный ток подается в систему еще до включения питания) сигнал Power OK может не соответствовать спецификации ATX, которая требует, чтобы этот сигнал подавался на низком уровне (т. е. при напряжении менее +0,4 В). На неисправных источниках питания подача сигнала Power OK была замечена при напряжениях от +0,6 до +2,0 В. Именно это непостоянство сигнала не дает материнской плате возможность включиться. Замените источник питания моделью, которая была протестирована/рекомендована для применения с данной системой или свяжитесь с производителем материнской платы, чтобы узнать о наличии процедуры проверки других источников питания.

Симптом 9.11. При проверке точности часов реального времени серверные диагностические средства блокируются

При выполнении теста точности часов реального времени на серверной плате он зависает (требуется перезапуск системы). В большинстве случаев неисправность заключается в модуле тестирования часов реального времени. В некоторых ситуациях она генерирует непредвиденные прерывания, которые не поддерживаются BIOS материнской платы. Проверьте наличие исправленного или обновленного теста точности часов реального времени. Других способов устранения этой неисправности нет, поэтому постарайтесь не использовать тест точности часов реального времени.

Симптом 9.12. При наличии переменного тока на сервер не подается питание

Убедитесь в том, что шнур подачи переменного тока надежно укреплен в источнике питания и в розетке. Если питание осуществляется через источник бесперебойного питания или шину питания, проверьте, включен ли источник. На задней стенке некоторых источников питания ATX, рядом с вентилятором, есть основной выключатель питания. Если устройство вашего источника питания такое же, проверьте положение этого выключателя. Кроме того, убедитесь в том, что кабель выключателя питания на передней панели плотно подсоединен к соответствующим контактам на материнской плате.

Если ваш источник питания совместим с SSI, убедитесь в том, что к вспомогательному сигнальному коннектору подключен подходящий коннектор источника питания. Чтобы обеспечить питанием вспомогательные устройства, источнику питания SSI требуется сигнал считывания в +3 В. Если в вашем источнике питания есть SSI-коннектор, проверьте надежность его установки во вспомогательном сигнальном коннекторе.

Снимите все расширительные платы и посмотрите, будет ли сервер загружаться только со встроенными компонентами. Если загрузка произойдет, меняйте платы расширения по одной и попытайтесь выявить подозрительное устройство (устройства). Снимите процессор (и все заглушки на разъемы под процессоры) и тщательно установите их снова. Снимите и переустановите все модули памяти (попробуйте установить заведомо исправные модули памяти с другого работающего сервера). Кроме того, проверьте, достаточно ли в системе модулей памяти (для работы некоторых серверов необходимо наличие четырех модулей памяти).

Симптом 9.13. Система загружается после установки адаптера PCI

Среди функций управления сервером есть функция постоянного "резервного" электроснабжения — это значит, что питание подается компонентам системы даже в том случае, если пользователь отключил систему с помощью переключателя электропитания на передней панели. Кроме того, в коннекторах PCI есть сигналы, которые инициируют загрузку системы (обычно они используются адаптерами управления сервером или сетевыми адаптерами/модемами в функциях Wake on LAN/Wake on Ring). Подключение адаптера в условиях, когда через шнур питания подается напряжение, может вызвать передачу ложных сигналов, которые приведут к загрузке системы. Поэтому перед установкой устройства PCI следует отсоединить шнур подачи переменного тока.

Симптом 9.14. Система автоматически загружается после подачи напряжения на шину питания

Возможно, вы неправильно выключили систему. Некоторые серверы обычно сохраняют последнее известное состояние электроснабжения с момента последнего подключения к источнику переменного тока. Если вы отсоединили шнур подачи переменного тока до отключения системы с помощью переключателя электропитания на передней панели, система автоматически попытается возвратиться к состоянию "включено" после возобновления подачи переменного тока. Выполните полное включение, а затем и отключение системы, используя переключатель электропитания на передней панели.

Симптом 9.15. Сервер слишком долго загружается

Это распространенная неисправность, причины появления которой могут быть самым разными. Чтобы устранить ее, необходимо иметь представление о процессе загрузки. Он состоит из нескольких этапов.

- Самотестирование BIOS при включении питания (BIOS POST). На этом этапе происходит подсчет памяти, проверка клавиатуры/мыши и дисковода IDE.
- Загрузка ПЗУ. Каждое устройство может загрузить в память часть своего рабочего кода. Вероятно, вы обращали внимание на сообщения, указывающие на устройства типа контроллера SCSI BIOS.
- Загрузка операционной системы. После инициализации сервера управление им передается операционной системе, которая выполняет все проверки/установки, необходимые для ее работы. К примеру, вы можете увидеть экран-заставку Windows.

Большой объем памяти может замедлить загрузку. Для проверки памяти может потребоваться несколько минут. Расширенные тесты памяти можно отключить в

CMOS Setup; в результате процесс загрузки будет происходить быстрее (особенно если выполняется служба, требующая нескольких перезагрузок). Но для нормальной работы системы тестирование памяти должно быть включено. Время загрузки может также увеличиться за счет нескольких адаптеров SCSI. Много времени занимает загрузка их расширительного ПЗУ и исполнение кода сканирования дисков. Обнаружение и загрузка ПЗУ также связана с дополнительными временными затратами.

Симптом 9.16. При наличии одного процессора система не загружается

Проверьте соответствие скорости процессора системной шине. Возможно, серверная плата поддерживает процессоры только с определенной скоростью шины. К примеру, серверная плата Intel 5KA4 поддерживает только процессоры Pentium III для системной шины с частотой 100 МГц. Убедитесь в том, что процессор установлен в слот для первичного процессора.

Проверьте наличие заглушки на слоте для вторичного процессора. Архитектура процессоров Pentium III требует установки заглушек на незанятые слоты под процессоры. Иначе сигналы могут приводить к ошибкам. Некоторые серверные платы не будут загружаться, если не обнаружат заглушки. Проверьте надежность установки процессора и заглушки. Механизмы фиксации предназначены для того, чтобы процессор и заглушка были плотно зафиксированы в разъемах; поэтому необходимо проверить фиксацию этим механизмом обоих устройств.

Симптом 9.17. Механизм фиксации не подходит к вашему процессору с картриджем

На некоторых серверных платах для установки процессоров Pentium III используются закрепленные на плате механизмы фиксации(GRM). Новые модели GRM обеспечивают поддержку только процессоров, произведенных в компоновке SECC2. Старые модели процессоров Pentium II/III, исполненные в картридже SECC, не подходят к этим новым механизмам фиксации GRM. Для установки процессоров в компоновке SECC пользуйтесь универсальными механизмами фиксации (URM). Установите URM, или смените тип процессора.

Симптом 9.18. При извлечении процессора из механизма фиксации его можно повредить

При извлечении процессоров Pentium III из механизмов фиксации, применяемых на некоторых серверных платах, необходимо соблюдать осторожность. Если не придерживаться процедуры извлечения процессора, жесткая фиксация механизма может повредить сам механизм фиксации, серверную плату, слот процессора и даже сам процессор. Проще всего снять процессор с серверной платы, установленной в корпусе — это поможет избежать деформирования серверной платы. Поставьте системной блок на бок, снимите боковую крышку и затем осторожно извлеките процессор из механизма фиксации.

Симптом 9.19. Ваша материнская плата не поддерживает быстрые процессоры Pentium III

Это происходит на серверных материнских платах типа L440GX+ в сочетании с Pentium III/600E и более быстрыми процессорами. Вы можете заметить, что процессоры Pentium III можно установить на устаревшую серверную плату, но в таком со-

четании устройств сервер будет работать нестабильно, что может обернуться повреждениями серверной платы или процессора. В большинстве случаев эта неисправность возникает из-за того, что несовместимая с процессором серверная плата не располагает модулем VRM (Voltage Regulation Module — модуль стабилизатора напряжения), необходимым для работы быстрых процессоров. Можно заменить модуль VRM на модуль, приспособленный к быстрым процессорам, или модернизировать материнскую плату, чтобы она была совместима с теми процессорами, которыми вы хотите воспользоваться.

Симптом 9.20. При установке плат расширения в слоты PCI 5 или 6 серверная материнская плата может быть заблокирована

Когда платы расширения устанавливаются в слоты PCI от 1 до 4, все работает нормально. С блокировкой некоторых серверных систем вы можете столкнуться после установки в слоты PCI 5 или 6 плат PCI, требующих высокой пропускной способности ввода/вывода (например, контроллера SCSI RAID). Сбой может произойти после завершения POST во время загрузки операционной системы или в ходе выполнения операций с данными на вторичной шине PCI с помощью программы "стрессовой" нагрузки на систему. В большинстве подобных случаев вы обнаружите вертикальную переходную стыковочную плату (riser card) PCI в слоте PCI 5. Кроме того, эта неисправность может возникнуть при подключении плат расширения PCI к вертикальным стыковочным платам. Она не имеет отношения ни к операционной системе, ни к какой-либо конкретной плате расширения, зато, как правило, она связана с материнской платой. Эта неисправность часто обусловливается производственными дефектами, которые неблагоприятно воздействуют на работу схем интерфейса шины. Попробуйте установить обновление BIOS или замените серверную материнскую плату.

Симптом 9.21. При обновлении микропрограммного обеспечения контроллера BMC происходит сбой в его работе

После быстрого обновления микропрограммного обеспечения контроллера BMC он может прекратить работать. С отключением контроллера BMC блокируются все функции управления сервером. К примеру, вы теряете возможность отключать систему с передней панели, прекращается регистрация событий в журнале системных событий, а программное обеспечение управления сервером не может взаимодействовать с встроенными сенсорами. Дело в том, что метод обновления микропрограммного обеспечения разрушительным образом воздействует на средства фиксации информации во флэш-микросхеме. В результате микропрограммное обеспечение контроллера BMC повреждается, и происходит сбой в его работе — сразу после обновления микропрограммного обеспечения или некоторое время спустя. Прежде чем проводить быстрое обновление микропрограммного обеспечения контроллера BMC, убедитесь в том, что вы используете последнюю из выпущенных производителем версию флэш-загрузчика. Если это не поможет, замените материнскую плату.

Симптом 9.22. Сервер с резервным энергоснабжением не загружается в сочетании с данной материнской платой

При использовании корпуса сервера с резервным энергоснабжением вместе с серверной платой (например, с Intel L440GX+) система загружаться не будет. Вероятно,

ваша серверная материнская плата и функция резервного энергоснабжения корпуса несовместимы. Устранить неисправность может установка более поздней версии материнской платы или отключение резервного энергоснабжения.

Дополнительные ресурсы

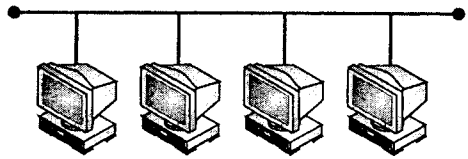
Gateway: **www.gateway.com**.

Intel: **developer.intel.com/design/servers/**.

Compaq: **www.compaq.com**.

Hewlett-Packard: **www.hp.com**.

Dell: **www.dell.com**.



ГЛАВА 10

Сетевые адаптеры и поиск неисправностей в сетях

Сети позволяют компьютерам совместно использовать файлы, принтеры, приложения, доступ к Интернету и прочие ресурсы. Чтобы компьютеры могли работать в сети, они должны быть соединены друг с другом. Участие компьютера в сетевой среде обеспечивается при помощи *сетевого адаптера* (Network Interface Card, NIC), как показано на рис. 10.1. Как правило, на серверах используется один или несколько многопортовых сетевых адаптеров, а для рабочей станции/настольной системы нужен всего один однопортовый сетевой адаптер. Если вам приходится иногда работать в сетевой среде, скорее всего, вы столкнетесь с необходимостью модернизации или замены сетевого адаптера. В этой главе даны характеристики типичного

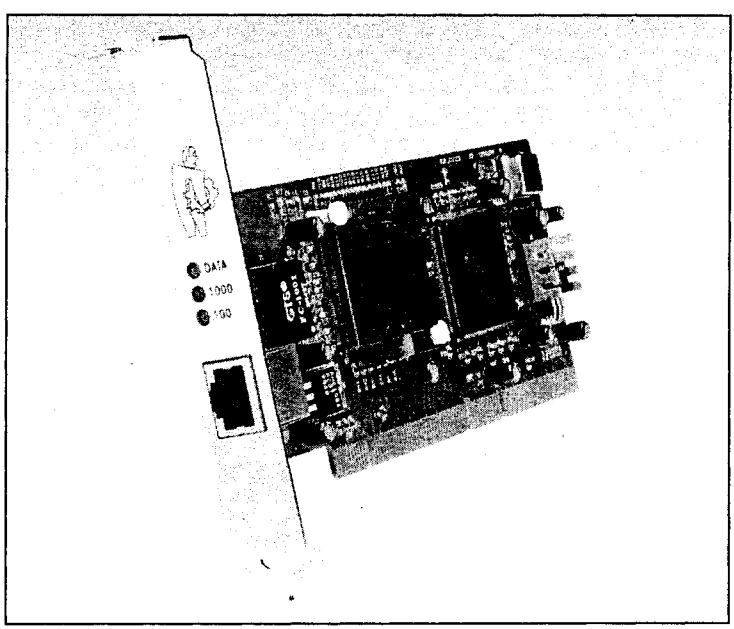


Рис. 10.1. Сетевой адаптер Netgear GA622T Gigabit Ethernet (публикуется с разрешения Netgear)

сетевого адаптера, рассматривается процесс его установки, и приводятся некоторые полезные указания относительно поиска и устранения неисправностей.

Понятие сетевого адаптера

Сетевой адаптер — это плата расширения, которая устанавливается в компьютер и обеспечивает его соединение с сетью. Выбор сетевого адаптера определяется тем, работаете ли вы с рабочей станцией/настольной системой или с сервером. Сетевой адаптер для настольной системы устанавливается на настольном персональном компьютере или на рабочей станции и обслуживает лишь одного пользователя (т. е. является однопортовым). Серверный сетевой адаптер применяется в серверных системах; он обеспечивает сетевое соединение множеству пользователей. Следовательно, серверный сетевой адаптер обычно (но не всегда) является многопортовым; он должен быть более функциональным и обеспечивать повышенную надежность и пропускную способность в сети, снижать нагрузку на центральный процессор и увеличивать общую эффективность соединений сети. Если серверный сетевой адаптер не соответствует потребностям сети (или выходит из строя), то он снижает производительность и эффективность целой рабочей группы, отдела или компании. Обратите внимание на различия в функциях двух типов сетевых адаптеров, представленные в табл. 10.1.

Примечание

Чаще всего на сервере установлено несколько сетевых адаптеров (или один многопортовый). Сервер может работать и с обычной однопортовой сетевой платой, но в условиях повышенной активности сети это может привести к ее перегрузке.

Сетевые адаптеры обеспечивают физическое взаимодействие между компьютером (сервером или рабочей станцией) и сетевым кабелем. Сетевой адаптер осуществляет преобразование данных, поступающих с внутренней шины компьютера, в последовательные сигналы для их передачи по коаксиальному, оптоволоконному кабелю и витой паре. Перед установкой и настройкой сетевого адаптера нужно понять принципы адресации и распределения системных ресурсов (прерывания, устройства ввода/вывода и памяти) в сети. Кроме того, нужно знать факторы, которые оказывают воздействие на производительность сетевого адаптера в сети. Сетевой адаптер выполняет четыре основные функции:

- он преобразует параллельные данные с шины хоста (сервера или рабочей станции) в последовательные данные, пригодные для передачи по сетевому кабелю;
- он передает последовательные данные другим компьютерам в сети;
- он контролирует поток данных между компьютером и сетевым кабелем;
- он получает из сетевого кабеля входящие последовательные данные и преобразует их в параллельные данные, которые передаются в шину компьютера и обрабатываются центральным процессором системы.

Примечание

В строгом мире сетей сетевой адаптер выполняет функции управления логическим соединением и доступом к среде на канальном уровне модели OSI.

Таблица 10.1. Сравнение сетевых адаптеров

Характеристика	Серверный сетевой адаптер	Пользовательский сетевой адаптер
Однопортовый сетевой адаптер	X	X
Многопортовый сетевой адаптер	X	
Наличие нескольких сетевых адаптеров в системе	X	
Агрегирование портов/распределение нагрузки	X	
Подключение 32-битовой шины PCI	X	X
Подключение 64-битовой шины PCI	X	
Автоматическое обнаружение сбоев портов	X	
Автоматическое восстановление после отказа с переключением на резервный порт	X	

Адресация сетевого адаптера в сети

Сетевой адаптер сообщает остальной части сети свое местоположение (или адрес), чтобы его можно было отличить от других сетевых адаптеров сети. Институт инженеров по электротехнике и радиоэлектронике (IEEE) определил каждому производителю сетевых плат блок адресов, и каждый изготовитель вносит эти адреса в свои адаптеры. Каждая сетевая плата (а следовательно, каждый компьютер) обладает уникальным адресом в сети. Если в компьютере установлено несколько сетевых адаптеров, каждый из них имеет свой адрес. Физический адрес (MAC-адрес), как правило, представляет собой 6-байтовое шестнадцатеричное число (например, 00:04:5A:D1:9D:25). Извлекая данные из компьютера и готовя их к передаче по сетевому кабелю, сетевой адаптер выполняет еще несколько функций.

- Между компьютером и сетевым адаптером должна быть установлена связь, которая и обеспечивает передачу данных от компьютера к сетевому адаптеру. Если ваш сетевой адаптер способен передавать данные на основе прямого доступа к памяти, компьютер выделяет сетевому адаптеру участок области памяти.
- Затем сетевой адаптер подает компьютеру сигнал и запрашивает его данные.
- Шина компьютера передает данные из ОЗУ (оперативное запоминающее устройство, Random Access Memory, RAM) сетевому адаптеру.

Так как довольно часто скорость передачи данных по шине компьютера и сетевому кабелю превышает возможности сетевого адаптера по их обработке, данные отправляются во встроенный буфер, т. е. зарезервированную для сетевого адаптера часть ОЗУ. В этом буфере информация временно хранится в процессе передачи и приема данных в сети.

Согласование данных

До того как сетевой адаптер передает данные в сеть, он проводит сложный электронный диалог с принимающим сетевым адаптером для согласования следующих пунктов:

- максимальный размер отсылаемых блоков данных;
- объем данных, который будет отправлен до получения подтверждения приема;
- промежуток времени между отсылкой порций данных;
- время ожидания до отправки подтверждения;
- объем данных, который максимально может вместить буфер каждого сетевого адаптера;
- скорость передачи данных (например, 10/100/1000 Мбит/с).

К примеру, если более современный и быстрый сетевой адаптер взаимодействует с сетевым адаптером предыдущих моделей, эти устройства должны согласовать общую скорость передачи и другие параметры. Многие современные сетевые адаптеры содержат схемы, которые позволяют более быстрому сетевому адаптеру работать на скорости более медленного адаптера. Каждый сетевой адаптер сообщает другому адаптеру свои параметры и принимает или приспосабливается к параметрам другого адаптера, чтобы прийти к "наименьшему общему знаменателю". После согласования всех параметров взаимодействия два сетевых адаптера начинают обмен данными.

Восстановление порта после отказа

Восстановление после отказа (Failover) — это метод резервирования, обеспечивающий защиту от сбоев серверных систем, в которых выполняются ответственные приложения. Во время сбоя порта система восстановления после отказа поддерживает соединение с сервером, перемещая весь трафик неисправного сегмента на резервный сетевой адаптер или порт адаптера. При обнаружении отказа порта он блокируется, а его нагрузка передается другому порту, что обеспечивает бесперебойную работу сети. Операция восстановления после отказа производится при потере связи в сети (например, Ethernet), по истечении времени охранного таймера, возникновении аппаратного прерывания, говорящего о сбое, а также при ненормированном показателе счетчиков отправки/приема в сегменте (например, слишком много коллизий или ошибок).

Агрегирование портов

Агрегирование портов — это функция сетевого адаптера с программной поддержкой, которая обеспечивает резервирование сетевого маршрута и увеличивает пропускную способность для сетевых (типа Fast Ethernet) серверов, на которых выполняются ответственные приложения. Принцип агрегирования портов заключается в распределении пропускной способности между несколькими портами. С помощью агрегирования портов можно создать виртуальный порт, сгруппировав вместе несколько портов. Подобное группирование способствует распределению сетевой нагрузки при совместном использовании ресурсов всех портов группы. В группе агрегирования портов один порт становится первичным, а его MAC-адрес присваивается

протоколу. Вся группа работает как единый интерфейс, позволяя программному обеспечению эффективно управлять ее объединенными ресурсами. В случае сбоя одного порта оставшиеся смогут справиться с нагрузкой и обеспечить бесперебойную работу сети.

Агрегирование портов поддерживается не всеми сетевыми адаптерами и сетевыми операционными системами. К примеру, программа агрегирования портов Adaptec Duralink64 совместима с однопортовыми сетевыми адаптерами Adaptec ANA-69011/TX и ANA-62011/TX, с двухпортовыми сетевыми адаптерами ANA-62022 и четырехпортовым сетевым адаптером ANA-62044. Программа агрегирования портов Duralink64 поддерживает Windows NT 4.0 и 3.51, а также серверы на базе Novell NetWare 4.x и 5.0 (Windows 95/98/SE не поддерживает агрегирование портов). Сервер с агрегированием портов Duralink64 включает в одну агрегированную группу до 12 портов Adaptec PCI Fast Ethernet (при 1,2 Гбит/с на группу). Если один из портов определенной группы выйдет из строя, он будет исключен из группы, а нагрузка перераспределяется между остальными портами группы. Сочетание технологий восстановления после отказа и агрегирования портов помогает организовать быструю и отказоустойчивую сеть.

FEC (Fast EtherChannel)

Fast EtherChannel (FEC) — это технология, разработанная компанией Cisco Systems (на основе стандарта Fast Ethernet) с целью обеспечения дополнительной пропускной способности, необходимой современным сетевым магистралям. Технология FEC объединяет два или четыре канала Fast Ethernet в единое логическое соединение, способное обеспечивать дуплексную пропускную способность сети на скорости 800 Мбайт/с. Помимо наращиваемой пропускной способности эта технология предусматривает отказоустойчивость и гибкость, защищая сеть от простоя из-за неисправности каналов. Технология FEC позволяет группировать порты или сетевые адаптеры и полностью использовать доступную пропускную способность (до 800 Мбит/с). Возможна группировка до четырех однопортовых сетевых адаптеров, двух двупортовых и одного четырехпортового адаптера. Эта технология предусматривает выравнивание нагрузки и управление каждой линией связи, распределяя трафик между множеством линий в пределах канала. К примеру, программа Adaptec Duralink64 v4.2 и все сетевые адаптеры Adaptec DuraLAN поддерживают технологию FEC и обеспечивают резервирование и высокоскоростное агрегирование между коммутаторами и серверами.

Примечание

Применение технологии FEC возможно на коммутаторах Cisco Catalyst и маршрутизаторах Cisco. За получением дополнительной информации о технологии FEC компании Cisco посетите Web-сайт компании Cisco Systems: **http://www.cisco.com/warp/public/729/fec**.

Полный дуплекс

Поддержка полнодуплексного режима позволяет сетевому адаптеру одновременно отправлять и принимать данные, что удваивает доступную пропускную способность сети. Чтобы активировать в сети дуплексный режим, необходимо, чтобы сетевой

адаптер и коммутатор (маршрутизатор или любое другое устройство связи) поддерживали дуплексный режим. Дуплексный режим можно активировать при двухточечном соединении, в котором вместо коммутатора применяется кабель перекрестного соединения (кроссовер).

Примечание

BNC-соединения не поддерживают дуплексный режим.

Технология кластеризации Microsoft

Технология кластеризации (clustering) Microsoft — это реализация технологии серверной кластеризации, разработанная в компании Microsoft. Термин "кластеризация" обозначает группу независимых систем, которые работают как единая система. Отказоустойчивость является встроенным компонентом технологии кластеризации. Если система в рамках кластера выйдет из строя, кластерная программа распределит ее операции между оставшимися системами кластера. Технология кластеризации не является заменой функций современных отказоустойчивых систем, хотя она и обеспечивает значительное повышение производительности.

Поддержка кадров увеличенного размера

Обычно кадры Ethernet увеличенного размера (Jumbo Frames) рассматриваются как ошибки, но некоторые современные сетевые адаптеры (например, плата SCM EtherPower II Gigabit Ethernet) можно настроить на применение макрокадров. Таким образом, максимальный размер кадра в сетях Ethernet фактически увеличивается с 1514 до 9014 байт. Использование макрокадров существенно снижает нагрузку центрального процессора, связанную с обработкой пакетов, и при передаче больших объемов данных может увеличить пропускную способность на 300 процентов. Но для применения макрокадров оба взаимодействующих компьютера должны быть оборудованы сетевыми адаптерами, которые поддерживают эту функцию. Сетевые устройства (концентраторы, коммутаторы и маршрутизаторы), соединяющие два компьютера, также должны поддерживать применение макрокадров, иначе неизбежны сбои связи.

Поддержка виртуальных сетей

Некоторые современные сетевые адаптеры (например, сетевая карта SMC EtherPower II 1000) поддерживают стандарт виртуальных сетей (VLAN) IEEE 802.1Q и могут быть настроены на участие в сети с другими устройствами, которые работают на технологии VLAN. VLAN IEEE 802.1Q — это группа портов, которые могут быть расположены в любой области сети, но обмен информацией осуществляют так, как будто находятся в одном физическом сегменте. VLAN упрощают управление сетью, т. к. они позволяют перемещать устройства в другие VLAN, не изменяя существующие физические соединения. VLAN можно организовывать в соответствии со структурой отделов (например, отдел маркетинга и отдел исследований и разработок) или групп пользователей (к примеру, пользователей электронной почты или видеоконференций).

VLAN не только повышают эффективность сети, уменьшая широковещательный трафик, но также позволяют выполнять изменения в сети, не обновляя IP-адреса или IP-подсети. Неотъемлемым свойством VLAN является высокий уровень сетевой безопасности, т. к. для передачи в другую VLAN трафик должен пройти через маршрутизатор или коммутатор. Как правило, конфигурация VLAN производится на коммутаторах, поддерживающих данную технологию и соответствующих стандарту IEEE 802.1Q, а идентификация принадлежности компьютера к виртуальной локальной сети производится на основании номера порта коммутатора. Впрочем, современные сетевые адаптеры способны преодолеть это ограничение, позволяя проводить конфигурацию до 16 идентификаторов VLAN непосредственно на сетевом адаптере. С помощью этой функции сетевой сервер, подключенный к порту коммутатора, настроенного на совмещение VLAN, получает возможность совместного использования своих ресурсов с 16 VLAN, тем самым существенно уменьшая задержку передачи между клиентами и сервером.

Примечание

Идентификаторы VLAN, настраиваемые на сетевом адаптере, должны во всей сети соответствовать идентификаторам на коммутаторах, совместимых с IEEE 802.1Q.

Современные сетевые адаптеры с поддержкой VLAN также поддерживают стандарт IEEE 802.1p "Качество обслуживания". Каждой VLAN присваивается уровень приоритета в таблице идентификаторов. Определение уровней приоритета на сетевом адаптере позволяет ему взаимодействовать с другими сетевыми устройствами с целью первоочередной доставки высокоприоритетных пакетов. Помните, что стандарт IEEE 802.1p должен поддерживаться всеми другими устройствами сети.

Примечание

Более подробную информацию об особенностях стандартов IEEE можно получить на сайте **standards.ieee.org**.

Конфигурация сетевого адаптера

Так как сетевой адаптер является внутренним устройством, он должен быть настроен на использование аппаратных ресурсов компьютера (т. е. прерывания, адреса ввода/вывода, области памяти и типа приемопередатчика). Стандартное использование технологии Plug-and-Play (PnP) BIOS и операционных систем обеспечивает автоматическую конфигурацию сетевого адаптера на использование доступных ресурсов компьютера. Но сетевые адаптеры более ранних моделей и платы, применяемые на старых платформах, нужно конфигурировать вручную с помощью перемычек и DIP-переключателей. Есть несколько вариантов распределения ресурсов, о которых вам следует иметь представление.

Назначение ресурсов

Линии IRQ — это аппаратные сигнальные линии, по которым устройства типа портов ввода/вывода, клавиатуры, контроллеров жестких дисков и сетевых адаптеров

отправляют запросы на обслуживание центральным процессором компьютера. Линии IRQ доступны с шины, и каждой из них присваивается определенный уровень приоритета с тем, чтобы центральный процессор мог определить относительную важность входящих запросов на обслуживание. Чем ниже уровень линии запроса прерывания, тем выше приоритет. К примеру, системный процессор обслужит сначала IRQ3, а затем IRQ12, даже если их сигналы пришли одновременно. Учитывая важность функций сетевого адаптера, следует попытаться присвоить ему как можно более низкую линию IRQ. В большинстве случаев для этих целей вполне подойдет IRQ3 или IRQ5. Как правило, IRQ5 является рекомендованной установкой (если эта линия доступна), и в большей части систем она принимается по умолчанию.

Прерывание может привлечь внимание процессора, но должны существовать и способы передачи команд и данных между сетевой платой и компьютером. Определяя базовый порт ввода/вывода, сетевой адаптер организует канал связи с системой.

Прямой доступ к памяти (DMA) — это методика, которая позволяет перемещать данные в компьютере между системной памятью и буфером сетевого адаптера без прямого управления со стороны центрального процессора компьютера. Иначе процессор должен был бы координировать каждую передачу данных. Это называется программируемым вводом/выводом (PIO). Поддержка передачи данных на основе прямого доступа к памяти осуществляется не всеми сетевыми адаптерами, но сетевые адаптеры, поддерживающие эту функцию, обеспечивают более высокую производительность системы.

Примечание

Важно отметить, что каждое устройство в компьютере использует различное распределение ресурсов линии IRQ, адреса ввода/вывода, DMA и области памяти. Если один и тот же ресурс используется несколькими устройствами, происходит программный конфликт, в результате которого сетевой адаптер или другие системные устройства могут повести себя неадекватно.

Многие сетевые платы используют определенную часть пространства ОЗУ в качестве буфера — временной области хранения, которая обрабатывает входящие и исходящие *кадры данных* (информационные пакеты, передающиеся по сети как единое целое). Установив базовый адрес ОЗУ (иногда он называется начальным адресом ОЗУ), вы можете контролировать область ОЗУ, занимаемую сетевым адаптером. Базовым адресом ОЗУ для сетевого адаптера зачастую является D0000h, но при этом, как правило, существует некая совокупность возможных адресов, из которых можно выбирать (например, D8000h).

Аналогичная ситуация складывается и с адресным пространством ПЗУ (постоянное запоминающее устройство, Read Only Memory, ROM). Большинство сетевых адаптеров в микросхеме ПЗУ BIOS содержат встроенные команды (или микропрограммное обеспечение). Помните, что BIOS есть и на материнской плате, BIOS часто используется и другими устройствами системы (к примеру, видео-BIOS или BIOS контроллера SCSI). Это значит, что вы должны правильно определить базовый (начальный) адрес ПЗУ, чтобы сетевой адаптер занял ту область памяти, которая не используется другими устройствами в системе. Базовым адресом ПЗУ для сетевого адаптера довольно часто является D0000h, но при этом, как правило, есть определенная совокупность возможных адресов, из которых можно выбирать (например, D8000h).

Примечание

Сетевой адаптер, не использующий системное ОЗУ, не имеет и настройки базового адреса памяти. Впрочем, некоторые сетевые адаптеры предусматривают настройку, которая позволяет определять блоки памяти для хранения кадров данных. К примеру, некоторые адаптеры позволяют зарезервировать 16 или 32 Кбайт памяти. Конфигурация с большим объемом памяти обеспечивает лучшую производительность сети, но оставляет меньше ресурсов памяти для выполнения других задач.

Выбор приемопередатчика

Наконец, некоторые сетевые адаптеры содержат один внешний и один встроенный *приемопередатчик* (схема, которая управляет сетевым кабелем). Когда вы подсоединяете кабель напрямую к сетевому адаптеру, вы используете встроенный приемопередатчик адаптера. Напротив, если сначала к сетевому адаптеру подключить модуль приемопередатчика, а к этому модулю подсоединить кабель, то будет задействован внешний приемопередатчик. Если ваша модель сетевого адаптера предусматривает возможность такого выбора, вам придется решить, каким из этих приемопередатчиков воспользоваться, а затем выполнить соответствующую настройку на самом адаптере с помощью перемычки или DIP-переключателя (впрочем, некоторые модели сетевых адаптеров способны выбирать приемопередатчик автоматически).

Стандартные настройки сетевого адаптера

После ознакомления с элементами конфигурации сетевого адаптера рассмотрим настройки сетевого адаптера, принимаемыми по умолчанию. Имейте в виду, что эти настройки устанавливаются по умолчанию и их можно изменить как вручную (с помощью перемычек и DIP-переключателей), так и автоматически (посредством технологии Plug-and-Play).

- *Прерывание*: IRQ5 (или второй вариант — IRQ2).
- *DMA*: DMA1 или DMA3 (при использовании 16-битовых сетевых адаптеров стоит попробовать DMA5).
- *Порт ввода/вывода*: как правило, подходит 300h.
- *Базовый адрес*: D0000h или выше.
- *Адрес ПЗУ*: D0000h или выше.

Помните, что драйверы режима готовности (DOS) должны быть приведены в соответствие с физической конфигурацией сетевого адаптера. Сетевые операционные системы создают эти драйверы разными способами. К примеру, 3Com (и многие другие производители) настраивает программный драйвер в CONFIG.SYS с помощью факультативных коммутаторов командной строки. Для сравнения, Novell создает драйвер посредством SHGEN (NetWare 2.1x) или GENSH (NetWare 2.0a). В любом случае параметры драйвера должны соответствовать сетевому адаптеру.

Шинные разъемы и кабели для сетевого адаптера

Чтобы обеспечить совместимость между компьютером и сетью, сетевой адаптер должен взаимодействовать с архитектурой шины (ISA или PCI) компьютера, а также иметь кабельный разъем подходящего типа для подключения к сети. К примеру,

сетевой адаптер, предназначенный для работы в компьютере Apple, входящем в сеть шинной топологии, не будет работать в компьютере IBM, входящем в состав маркерного кольца. Вам следует иметь представление о различных архитектурах шин и типах кабелей и кабельных разъемов.

Архитектура шины

В системах персональных компьютеров существует четыре типа архитектур шин: ISA, EISA, MicroChannel и PCI. Каждый тип шины физически отличается от остальных, и очень важно, чтобы было соответствие между сетевым адаптером и типом шины. Сетевой адаптер нужно выбирать так, чтобы он соответствовал типу гнезда шины вашего компьютера.

Архитектура ISA

Слот ISA — это первая открытая архитектура системной шины, применявшейся в персональных компьютерах IBM, причем каждый производитель имел право воспользоваться этой архитектурой, уплатив небольшой лицензионный взнос. Так как не существовало ограничений на использование шин ISA, они воспроизводились во всех последующих компьютерах IBM. Применение стандартизованной шины не только позволило тысячам производителей выпускать совместимые ПК и устройства расширения, но и помогло обеспечить использование стандартизованных операционных систем и прикладного программного обеспечения. Существуют 8- и 16-битовая версии шины ISA, хотя во всех материнских платах, выпущенных с середины 1980-х гг., производители отказались от 8-битовой XT-версии ISA в пользу более быстрой 16-битовой AT версии.

Архитектура EISA

EISA — это 32-битовая шина, которая была разработана в 1988—89 гг. в ответ на возросшие требования к более высокой скорости и производительности периферийных устройств в связи с вводом в эксплуатацию центральных процессоров 80386 и 80486. Кроме того, было неразумно оставлять весь рынок 32-битовых шин архитектуре MCA компании Intel. Несмотря на то, что шина работает на той же тактовой частоте 8,33 МГц, 32-битовый информационный канал удваивает пропускную способность данных между материнской платой и платой расширения. В отличие от шины MCA, шина EISA гарантирует обратную совместимость с уже существующими периферийными устройствами ISA и программным обеспечением для персональных компьютеров. Шина EISA создана полностью совместимой с платами ISA и автоматически переключается между 16-битовым режимом ISA и 32-битовым режимом EISA с помощью второго ряда краевых разъемов. Таким образом, платы EISA имеют доступ ко всем сигналам плат ISA, а также ко второму ряду сигналов EISA.

Архитектура MCA

С появлением и повсеместным распространением 32-битовых микропроцессоров типа Intel 80386 и 80486, пропускной способности 16-битовой шины ISA стало недостаточно. Передача 32-битового слова по шине расширения в виде двух 16-битовых частей приводила к существенной трате времени обработки. И дело было не только в скорости передачи данных и быстродействии процессора; видео- и аудиосистемы персональных компьютеров также развивались и требовали увеличения

своей доли пропускной способности шины. К началу 1987 г. в IBM было принято решение об отказе от шины ISA и ее замене совершенно новой шинной структурой, которую назвали MCA. IBM интегрировала шину MCA в серию персональных компьютеров с разъемом PS/2, а также в рабочие станции System/6000. Шина MCA не только поддерживала 16- и 32-битовый режимы — это была первая шина для ПК, которая поддерживала управление шиной с целью повышения производительности устройств.

Архитектура PCI

К концу 1980-х гг. распространение 32-битовых центральных процессоров Pentium и операционных систем с широким применением графики показало, что шина ISA с тактовой частотой 8,33 МГц устарела. Для повышения производительности началась разработка альтернативных архитектур шин. В середине 1992 г. Intel Corporation и представительный консорциум производителей представили шину PCI с тактовой частотой 33 МГц. В то время как устаревшая видеошина VLB была разработана специально для поддержки видеосистем персонального компьютера, 188-контактная шина PCI была ориентирована на будущее центральных процессоров (и персональных компьютеров в целом), т. к. она также поддерживает периферийные устройства типа контроллеров жестких дисков, сетевых адаптеров и т. д.

Другим важным преимуществом шины PCI является возможность автоматической конфигурации для периферийных устройств без переключателей и перемычек. Такая *автоконфигурация* (суть технологии Plug-and-Play) предусматривает настройку всех адресов, запросов прерывания и распределения DMA PCI-устройства. Шина PCI поддерживает управление передачей данных по шине, что позволяет одному из периферийных устройств контролировать шину для повышения пропускной способности и выполнения высокоприоритетных задач. Архитектура PCI обеспечивает поддержку *параллелизма* — алгоритма, который обеспечивает одновременную работу процессора и устройств, контролирующих шину, и позволяет избежать простоя процессора.

Примечание

В настоящее время шинные архитектуры ISA, EISA и MCA считаются устаревшими. Теперь установка и обслуживание сетевых адаптеров производится на слотах PCI. С более старыми типами шин (как правило, с ISA) вы можете столкнуться лишь при наличии в сети персональных компьютеров устаревшей конфигурации или устаревших сетевых адаптеров.

Кабели и коннекторы

Чтобы выбрать подходящий для вашей сети сетевой адаптер, вам нужно определить тип кабельного соединения и коннекторы, используемые в сети. Помните, что каждый тип сетевого кабеля имеет свои физические характеристики, которые необходимо учитывать при выборе сетевого адаптера. Каждый сетевой адаптер совместим по крайней мере с одним типом кабеля — наиболее распространенными типами кабеля являются коаксиальный (как правило, тонкий), витая пара и оптоволоконный кабель. На некоторых сетевых адаптерах есть несколько кабельных коннекторов. К примеру, нередко на сетевом адаптере есть коннекторы для тонкого и толстого коаксиального кабелей, а также для витой пары. Если на плате несколько сетевых коннекторов, но нет встроенного детектора интерфейса, следует установить тип ка-

беля вручную, воспользовавшись имеющимися на адаптере перемычками (или специальными возможностями программного обеспечения).

При работе с толстыми коаксиальными соединениями необходимо соблюдать крайнюю осторожность. В толстом коаксиальном сетевом соединении используется кабель с 15-контактным интерфейсом AUI (Attachment Unit Interface — устройство доступа к среде передачи) для подключения 15-контактного коннектора (DB-15) на задней стороне сетевого адаптера к внешнему приемопередатчику. Внешний приемопередатчик подключается к толстому коаксиальному кабелю с помощью пронзающего ответвителя. Не перепутайте 15-контактный порт джойстика с портом AUI внешнего приемопередатчика. Они похожи, но некоторые контакты порта джойстиков проводят +5 В постоянного тока, а такое напряжение может повредить сетевое оборудование и компьютер.

При подключении сетевого адаптера следует обратить внимание еще на несколько важных моментов. Не перепутайте 25-контактные порты SCSI с параллельными портами принтера. Некоторые устаревшие устройства SCSI подключались через такие же коннекторы DB-25, как и параллельные порты принтера, но ни одно устройство не будет работать, если оно подключено не через свой коннектор. Наконец, в незащищенном соединении по витой паре применяется коннектор RJ-45. RJ-45 напоминает телефонный коннектор RJ-11, но он больше по размеру и содержит восемь проводов — в RJ-11 есть лишь четыре провода.

Сетевые адаптеры и производительность сети

Так как сетевой адаптер имеет прямое отношение к передаче данных по сети, выбор сетевого адаптера оказывает существенное влияние на производительность сети. Если сетевой адаптер работает на незначительных скоростях (например, 10 Мбит/с), то передача данных в сеть и из сети будет производиться не так быстро — в сети шинной топологии, которой никто не может пользоваться до освобождения кабеля, медленный сетевой адаптер может увеличить время ожидания для всех пользователей. Определив физические требования к сетевому адаптеру (т. е. тип шины, сетевого коннектора и сети, в которой будет установлен сетевой адаптер), необходимо рассмотреть несколько других факторов, которые влияют на возможности сетевой платы. Несмотря на то, что все сетевые адаптеры соответствуют определенным минимальным стандартам и спецификациям, в некоторых из них есть дополнительные функции, которые значительно повышают производительность сервера, клиента и сети в целом.

- Выбирайте сетевой адаптер, который поддерживает режим DMA. DMA позволяет компьютеру передавать данные из буфера сетевого адаптера прямо в ОЗУ без непосредственного участия центрального процессора. В результате процессор высвобождается для выполнения других задач, и относительная производительность компьютера повышается.
- Выбирайте сетевой адаптер, который поддерживает *разделяемую память адаптера*. Такая сетевая плата поддерживает буфер (ОЗУ), который она разделяет с компьютером, а компьютер рассматривает этот буфер как часть своего ОЗУ.
- В качестве альтернативы разделяемой памяти адаптера можно выбрать сетевой адаптер с разделяемой системной памятью. С помощью этого алгоритма встро-

енный контроллер сетевого адаптера выбирает часть системной памяти (ОЗУ) и использует его для обработки данных.

- Если вы используете сетевой адаптер с разъемом PCI, выбирайте модель с поддержкой управления шиной. Такой адаптер осуществляет временный контроль над шиной PCI компьютера и в обход центрального процессора отсылает данные напрямую в системную память. Это повышает быстродействие компьютера, т. к. высвобождает процессор для выполнения других задач, что повышает производительность сети.
- По возможности используйте сетевые адаптеры с буферами памяти ОЗУ. Зачастую скорость передачи сетевого трафика слишком высока, и обычный сетевой адаптер не успевает его обрабатывать. В этом случае микросхемы ОЗУ на сетевом адаптере выполняют функцию буфера. Когда сетевой адаптер получает больше данных, чем он может немедленно обработать, буфер ОЗУ хранит часть этих данных до тех пор, пока адаптер их не обработает. В результате производительность сетевой платы повышается.
- По возможности используйте сетевые адаптеры со встроенным процессором. Плата со встроенным процессором (который также называется микроконтроллером) значительно меньше зависит от центрального процессора при обработке данных. Это снимает дополнительную нагрузку с центрального процессора и улучшает производительность сети.

Как правило, для сервера следует выбирать лучший из всех возможных сетевых адаптеров, т. к. через сервер обычно проходит большая часть сетевого трафика. Часто на серверах используются высокопроизводительные сетевые адаптеры (например, сетевой адаптер Ethernet со скоростью 1000 Мбит/с). Для сравнения, на рабочих станциях/настольных компьютерах сети для корректной работы достаточно установить менее дорогостоящие однопортовые сетевые платы (например, Ethernet со скоростью 10/100 Мбит/с). Устаревшие адаптеры будут работать только с приложениями с низким уровнем трафика (например, обработка слов). Помните, что производительность сети шинной топологии может быть снижена из-за одного медленного сетевого адаптера. Существуют специализированные типы сетевых адаптеров, с которыми вам также следует ознакомиться.

Беспроводные сетевые адаптеры

Есть некоторые устройства, физическое соединение которых невозможно. В таких случаях появляется необходимость в альтернативе кабельному соединению. Существуют беспроводные сетевые адаптеры (типа Linksys WPC11, изображенного на рис. 10.2), которые обеспечивают поддержку основных сетевых операционных систем и часто имеют много функциональных возможностей, включая внутреннюю антенну, антенный кабель, сетевое программное обеспечение для подключения сетевого адаптера к конкретной сети, и диагностическое программное обеспечение для поиска и устранения неисправностей. Беспроводные сетевые адаптеры можно использовать как для организации полностью беспроводной локальной сети, так и для подсоединения беспроводных станций к кабельной локальной сети. Как правило, беспроводные сетевые адаптеры применяются для взаимодействия со специальным компонентом, который называется беспроводным концентратором и действует как приемопередатчик для отправления и приема беспроводных сигналов.

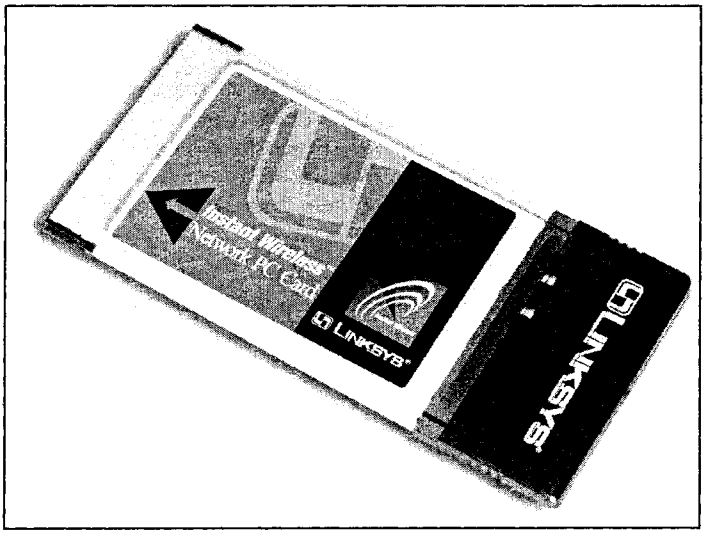


Рис. 10.2. Беспроводной сетевой адаптер Linksys WPC11 (публикуется с разрешения Linksys)

Сетевые адаптеры с оптоволоконным соединением

Скорость передачи данных постоянно растет по мере появления новых приложений с высокими требованиями по пропускной способности и потоков мультимедийных данных, которые в современных сетях стали обычным явлением. Использование сетевых адаптеров с тонким оптоволоконным соединением по сравнению с коаксиальным кабелем и витой парой позволяет осуществлять прямое подключение к высокоскоростным сетям на основе оптоволоконного кабеля. Сетевые адаптеры с оптоволоконным соединением (к примеру, SMC EtherPower II 1000) в последнее время стали экономически более эффективными по сравнению с традиционными сетевыми адаптерами на медном кабеле. Признаком оптоволоконной установки зачастую выступает указатель "S" (например, 1000BaseSX), а "T", как правило, обозначает сборку на основе медной витой пары (1000BaseTX).

Программируемое ПЗУ удаленной загрузки

В некоторых средах безопасность сети настолько важна, что на отдельных рабочих станциях даже нет дисководов для гибких дисков. Пользователи не могут копировать данные на гибкие или жесткие диски, а следовательно, не имеют возможности переносить данные со своего рабочего места. Так как компьютеры обычно загружаются с гибкого или жесткого диска, должен быть альтернативный источник с программным обеспечением, которое запускает (или загружает) компьютер и обеспечивает его соединение с сетью. В таких случаях сетевой адаптер может быть оснащен специальной микросхемой, называемой программируемым ПЗУ (ППЗУ) удаленной загрузки, которая содержит код, необходимый для загрузки компьютера и подключения пользователя к сети. Именно это позволяет рабочим станциям без дисков подсоединяться к сети при запуске. Разъем ППЗУ удаленной загрузки изображен на рис. 10.3.

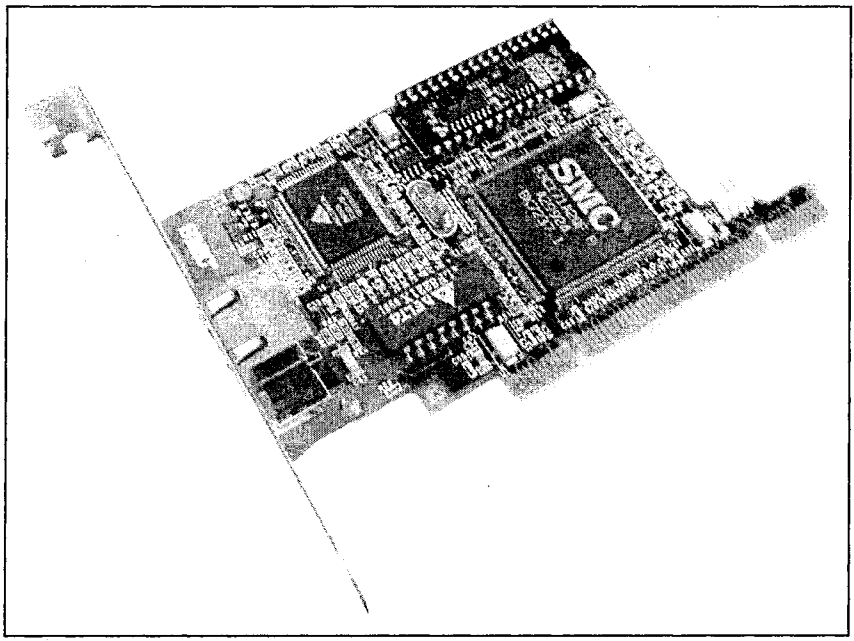


Рис. 10.3. Сетевой адаптер Ethernet SMC EtherPower II 10/100 (публикуется с разрешения SMC)

Установка сетевого адаптера

Сначала нужно установить сам сетевой адаптер. Рассмотрим установку современного PCI адаптера типа Adaptec. Процесс его установки практически не отличается от установки любого другого устройства расширения PCI PnP. Он состоит из трех основных этапов: установки сетевого адаптера, подсоединения сетевого кабеля и конфигурирования адаптера. Опытные пользователи могут пропустить этот раздел, но для многих технических специалистов он может оказаться полезным. Приведем минимальные системные требования для установки платы Adaptec и запуска ее диагностической утилиты.

- Однопортовый сетевой адаптер на шине PCI. Свободный слот PCI с управлением шиной — рекомендуется новейшая системная BIOS на основе PCI (для многопортовых сетевых адаптеров нужна PCI 2.1-совместимая шина).
- Четырехканальный (quad) или двухканальный (dual) сетевой адаптер. Системная BIOS с поддержкой микросхемы моста PCI-PCI в среде Windows NT.
- Диагностическое программное обеспечение. Требуется MS-DOS 3.3 или выше.
- Центральный процессор. Платформа Intel x86 (совместимая с IBM PC) с одним или несколькими процессорами.
- Оперативная память. 16 Мбайт ОЗУ или более.
- Программное обеспечение. Windows NT 3.51 или 4.0 для рабочей станции или сервера, Windows 95/98/2000 (или NetWare 4.x или 5.0) и выше.

Начало установки

Отключите питание компьютера и выньте из розетки шнур питания. В ходе монтажа вам нужно будет заземлить себя, прикоснувшись к любой неокрашенной поверхности корпуса компьютера. Затем сделайте следующее.

1. Откройте корпус системного блока, следуя инструкциям производителя.
2. Осторожно извлеките сетевой адаптер из антистатического контейнера. Проверьте обозначение модели на сетевом адаптере (сохраните антистатический контейнер для дальнейшего использования).
3. Убедитесь в том, что на сетевом адаптере нет видимых следов повреждения, которое могло произойти во время транспортировки. Если вы заметите повреждения, немедленно оповестите об этом вашего поставщика сетевого оборудования и службу доставки, т. к. вам придется решить вопрос о его замене.
4. После открытия корпуса найдите свободный слот расширения (в данном случае PCI). Открутите заглушку в корпусе напротив слота и снимите ее.

Примечание

Слоты PCI и сетевые адаптеры выпускаются в двух разновидностях: с напряжением 3,3 и 5 В (второй вариант более распространен). Как правило, сетевые адаптеры на базе PCI совместимы со слотами с напряжением 5 В. Некоторые модели сетевых адаптеров также поддерживают слоты с напряжением 3,3 В. Чтобы повысить производительность при использовании многопортовых сетевых адаптеров, их следует устанавливать в слоты с высоким приоритетом — например, в слот 0 на шине PCI.

5. Вставьте сетевой адаптер в слот PCI и с усилием равномерно нажмите на него до тех пор, пока все контакты шины не войдут в слот.
6. Зафиксируйте сетевой адаптер в слоте с помощью винтов, которые вы открутили при удалении заглушки на корпусе.
7. Закройте корпус.
8. Подсоедините все устройства и кабели, которые вам пришлось отключить во время установки. Не включайте питание компьютера.

Подключение кабелей

При работе с тонким коаксиальным кабелем следует подсоединить Т-коннектор к BNC-коннектору сетевого адаптера. Гнезда со штырями Т-коннекторов всех сетевых плат следует выровнять в одну линию. Вставьте Т-коннектор и поверните его по часовой стрелке, пока он не остановится (вы услышите слабый щелчок). Подсоедините кабель сети к одной стороне Т-коннектора, а оконечную нагрузку (или кабель, ведущий к следующей рабочей станции) — к другой его стороне.

Если вы работаете с витой парой, убедитесь в том, что коннектор RJ-45 на вашем кабеле смонтирован так, как нужно для стандартного адаптера 10Base-T (удивительно, как часто эти коннекторы монтируются неправильно). Совместите разъем RJ-45 на одном конце витой пары с вырезом адаптера и вставьте кабель в гнездо RJ-45 сетевого адаптера. Убедитесь в том, что другой конец кабеля подключен к сети.

Что касается толстого коаксиального кабеля (где необходим 15-контактный интерфейс AUI), найдите AUI-коннектор на сетевом адаптере и установите скользящую

защелку в открытое положение. Подключите кабель AUI или приемопередатчик к AUI-коннектору на сетевом адаптере. Чтобы зафиксировать кабель, передвиньте скользящую защелку в закрытое положение. Подключите другой конец кабеля AUI к внешнему приемопередатчику.

Сетевой адаптер, как правило, выбирает тип кабеля автоматически. Если установлен подходящий для операционной системы драйвер, он автоматически выбирает тип носителя исходя из типа кабельного соединения. Если впоследствии вы будете менять тип кабеля, то для того, чтобы новый тип кабеля был определен автоматически, нужно переустановить драйвер. Если драйвер не может определить тип кабеля (или наличие кабельного соединения), функция Auto Select Media Type (Автовыбор типа носителя) устанавливает тип коннектора, который по умолчанию предусмотрен микропрограммным обеспечением сетевого адаптера. К примеру, для сетевого адаптера 3Com 3C900-COMBO по умолчанию принимается AUI. Установку по умолчанию можно изменить, выбрав из списка вариантов другой тип носителя.

Примечание

Если при установке четырехканального или двухканального сетевого адаптера к порту не подключен кабель, на сервере при запуске может появиться сообщение об ошибке. Это нормально и не влияет на производительность.

Конфигурирование сетевого адаптера

Так как в настоящее время большинство сетевых адаптеров поддерживают стандарт Plug-and-Play, BIOS может автоматически определять доступные ресурсы сетевого адаптера на шине PCI и осуществлять его настройку. Тем не менее в некоторых системах конфигурацию сетевой платы нужно проводить самостоятельно (или проверять правильность настроек). Для этого необходимо войти в CMOS Setup, и в главном меню выбрать **Advanced Settings** (Расширенные настройки). Проверьте, активированы ли нижеперечисленные настройки (возможно, они не будут в точности совпадать с настройками вашей версии BIOS, поэтому обратитесь к руководству по эксплуатации вашей системы).

- PCI Slot Enabled. Разблокирует все слоты PCI в системе.
- Bus Mastering. Разрешает управление передачей данных по шине PCI для слота (слотов), которые используются сетевыми адаптерами.
- PCI INTA. Присваивает прерывание ISA (10, 11, 12, и т. д.) вектору прерывания A PCI.
- PCI INT Vector. Присваивает вектор прерывания A слоту (слотам) PCI, которые используются сетевым адаптером.
- PCI Bus Latency (Задержка шины PCI). Устанавливается значение в диапазоне от 40 до 80.
- Triggering. Устанавливает для слота запуск по уровню вместо запуска по фронту.

Примечание

В четырехканальных и двухканальных сетевых адаптерах, как правило, используется микросхема моста PCI-PCI материнской платы. Если BIOS вашей системы не

поддерживает микросхему моста PCI-PCI, корректную конфигурацию таких сетевых адаптеров выполнить не удастся. Свяжитесь с производителем вашего компьютера, чтобы получить новую версию BIOS, которая поддерживает микросхему моста PCI-PCI.

Установка драйверов сетевого адаптера

После установки сетевого адаптера нужно установить подходящий драйвер сетевого адаптера. В зависимости от типа вашего сетевого адаптера и сетевой операционной системы можно установить один из трех типов драйверов: стандартный драйвер, драйвер восстановления после отказа или драйвер агрегирования портов. Учтите, что установить можно драйвер лишь одного типа. Для примера, на дискетах для Adaptec Duralink64 поставляются следующие типы драйверов.

- *Стандартный* драйвер (DuraLAN Standard Driver) задействует каждый порт независимо.

Примечание

Не все версии Windows поддерживают драйверы восстановления после отказа и агрегирования портов. К примеру, Windows 9x и Novell Client32 не поддерживают драйвер восстановления после отказа Adaptec Duralink64. В таких операционных системах следует устанавливать стандартный драйвер.

- Драйвер *восстановления после отказа* (Duralink64 Failover Driver) организует группу из двух портов сетевого адаптера, один из которых выступает в роли первичного (primary), а другой — в качестве резервного порта (backup). Эти порты могут быть подключены к концентратору или коммутатору.
- Драйвер *агрегирования портов*, или Fast EtherChannel (Duralink64 Port Aggregation Driver), группирует до 12 портов и обязательно используется вместе с коммутатором. Кроме того, можно сформировать группы Fast EtherChannel (FEC) из двух или четырех портов, но для этого необходим коммутатор, который поддерживает Fast EtherChannel.

Удаление старых драйверов

Если вы заменяете или модернизируете сетевой адаптер (или устанавливаете новый драйвер), сначала нужно удалить старые драйверы сетевого адаптера — благодаря этому конфликтов между старым и новым программным обеспечением не произойдет. В этом разделе показано, как нужно удалять старые драйверы для сетевого адаптера Adaptec DuraLAN. Возможно, для вашего сетевого адаптера некоторые этапы будут отличаться от нижеприведенных, но в целом процесс должен быть примерно таким же. К примеру, если в качестве сетевой операционной системы вы используете Windows NT, то придерживайтесь следующих этапов при удалении старых драйверов сетевого адаптера:

1. Дважды щелкните на значке **My Computer** (Мой компьютер) на рабочем столе.
2. Дважды щелкните на значке **Control Panel** (Панель управления).
3. Дважды щелкните на значке **Network** (Сеть).

4. В диалоговом окне **Network** (Сеть) щелкните на значке **Adapters** (Сетевые платы).
5. В списке **Network Adapters** (Сетевые платы) выберите сетевой адаптер, который планируется удалить (например, Adaptec DuraLAN), и нажмите кнопку **Remove** (Удалить).
6. На вопрос, хотите ли вы продолжить, нажмите кнопку **Yes** (Да).
7. Повторите два предыдущих этапа до тех пор, пока все драйверы сетевого адаптера (например, Adaptec DuraLAN) не будут удалены.
8. После удаления всех драйверов нажмите кнопку **OK**.
9. Чтобы закрыть диалоговое окно **Network** (Сеть), нажмите кнопку **Close** (Закрыть).
10. Чтобы перезагрузить компьютер, нажмите кнопку **Yes** (Да).

Примечание

После перезагрузки Windows NT может появиться сообщение о том, что по крайней мере одна служба не смогла произвести запуск. После установки нового драйвера такие сообщения появляться не будут, так что просто нажмите кнопку **OK**.

Установка новых драйверов

После удаления из системы всех старых драйверов можно приступать к установке новых драйверов сетевого адаптера для вашей сетевой операционной системы. Перед этим будет не лишним посетить Web-сайт производителя вашего сетевого адаптера и проверить наличие обновлений драйверов и "заплат" (patch) для них. В этом разделе мы рассмотрим процесс установки драйверов для Adaptec DuraLAN в средах Windows NT/2000 и NetWare.

Windows NT 4.0

Если в данный момент вы устанавливаете Windows NT, то при появлении запроса о сетевом адаптере DuraLAN следует начать с шага 6. Чтобы установить драйвер DuraLAN на платформе Windows NT 4.0, сделайте следующее.

1. Загрузите операционную систему Windows NT.
2. Выберите в меню **Start** (Пуск) вкладку **Settings** (Настройки), затем щелкните на значке **Control Panel** (Панель управления).
3. В меню **Control Panel** (Панель управления) дважды щелкните на значке **Network** (Сеть).
4. В окне **Network** (Сеть) откройте вкладку **Adapters** (Сетевые платы).
5. На вкладке **Adapters** (Сетевые платы) нажмите кнопку **Add** (Добавить).
6. В окне **Select Network Adapter** (Выберите сетевую плату) нажмите кнопку **Have Disk** (Установить с диска).
7. В окне **Insert Disk** (Вставьте диск) вставьте в дисковод дискету (Duralink 64 для Windows NT) и нажмите кнопку **OK**.
8. В окне **Select OEM Option** (Выберите производителя оборудования) выберите установленную модель сетевого адаптера (DuraLAN) и нажмите кнопку **OK**.

9. В появившемся окне установки драйвера сетевого адаптера (**Adaptec DuraLAN NIC Driver Installation**) выберите драйвер и нажмите кнопку **OK**.
10. Переходите к установке стандартного драйвера, драйвера восстановления после отказа или драйвера агрегирования портов.

Windows 2000

Чтобы установить драйвер и диагностические средства на компьютере с операционной системой Windows 2000, сделайте следующее.

1. Перезагрузите компьютер и запустите операционную систему Windows 2000.
2. Войдите в систему, воспользовавшись учетной записью администратора Windows 2000. Мастер установки нового оборудования Windows 2000 обнаружит новый сетевой адаптер и запустит установку драйвера.
3. Поместите в дисковод компакт-диск с драйверами сетевого адаптера (3Com EtherLink Server CD).
4. В главном меню выберите **NIC Software** (Программное обеспечение сетевой платы).
5. В появившемся списке щелкните на значке **NIC Drivers and Diagnostics** (Драйверы и диагностическое ПО сетевой платы).
6. Следуйте указаниям мастера установки.
7. Выберите тип установки: **Typical** (Типовая) или **Custom** (Выборочная). Появится экран **Please Wait** (Подождите, пожалуйста). После завершения установки появится диалоговое окно **Update** (Обновить).
8. Нажмите кнопку **OK**; в результате появится экран **Setup Complete** (Установка завершена).
9. Чтобы завершить процесс установки, нажмите кнопку **Finish** (Завершить).
10. Нажмите кнопку **Exit** (Выход). Возможно, для активизации новых драйверов систему придется перезагрузить.

Novell NetWare

При использовании операционной системы NetWare и файлового сервера NetWare для установки и конфигурации драйверов нужно выполнить нижеперечисленные действия. Во-первых, вставьте в дисковод сервера компакт-диск с драйверами (3Com EtherLink Server CD).

1. При использовании версии NetWare 4.2 вставьте в дисковод компакт-диск с драйверами и введите следующие команды:

```
load cdrom
cd mount ecd210p980x
```

2. При использовании версии NetWare 5.0 вставьте в дисковод компакт-диск с драйверами и введите команду

```
load cdrom
```

3. Подождите, пока появится сообщение об успешном запуске компакт-диска, а затем приступайте к копированию драйвера, как показано на примере (точные инструкции по установке вы найдете в документации к вашему сетевому адаптеру).
4. В версии NetWare 4.2 используйте команду `load install`, а в NetWare 5.x — команду `load nwconfig`.
5. На экране **Configuration Options** (Параметры конфигурации) выберите **Driver** (Драйвер).
6. На экране **Driver Options** (Параметры конфигурации) выберите **Configure** (Настройка).
7. Если появится экран **Additional Driver Actions** (Другие активные драйверы), выберите **Select** (Выбрать) (в результате появится экран с перечислением всех ранее сохраненных в системе драйверов сетевого адаптера). Новый сетевой адаптер, не установленный ранее, в этом списке указан не будет.
8. Нажмите клавишу **Insert** (Вставить). Появится системное сообщение о выборе дисковода.
9. Нажмите клавишу <F3>.
10. Укажите путь к тому, на котором хранится драйвер — например, ecd210p980x:/nwserver. После этого появится экран **Select a Driver to Install** (Выберите драйвер для установки) с выделенным именем вашего драйвера (3Com EtherLink Server).
11. Нажмите клавишу <Enter>, чтобы выбрать этот драйвер.
12. При появлении запроса на подтверждение имени копируемого драйвера выберите **Yes** (Да). Программа установки копирует драйвер в соответствующий подкаталог на сервере. Затем появится экран **Configuration** (Настройка).
13. На этом этапе вы можете указать номер слота сетевого адаптера и загрузить драйвер. Номер слота указывать не нужно, если вы устанавливаете только один сетевой адаптер.
14. На экране **Configuration** (Настройка) выберите **Slot Number** (Номер слота).
15. Введите номер слота, в который будет установлен сетевой адаптер (например, 10001).
16. Для установки параметров и загрузки драйвера выберите **Save** (Сохранить). Программа установки загрузит сконфигурированный драйвер, а затем запишет команды `load` и `bind` в файл AUTOEXEC.NCF. Система выполнит присвоение номера сети.
17. Введите номер сети (или нажмите клавишу <Enter>, чтобы выбрать номер, присвоенный системой). При отсутствии ошибок программа установки спросит, хотите ли вы выбрать дополнительный сетевой драйвер.
18. Чтобы настроить еще один сетевой адаптер, выберите **Yes** (Да).
19. Для настройки остальных сетевых плат повторите весь процесс. После настройки всех сетевых адаптеров, чтобы вернуться к экрану **Installation Options** (Пара-

метры установки), нужно будет несколько раз нажать клавишу <Esc>. Теперь можете выполнить настройку групп.

20. На экране **Configuration Options** (Параметры конфигурации) выберите свойства файлов NCF (это позволит создавать или редактировать файлы запуска сервера).
21. Выберите режим редактирования файла AUTOEXEC.NCF.
22. Внесите в файл AUTOEXEC.NCF следующие изменения.
    - Добавьте команду загрузки драйверов SE и LBRSL до команд загрузки любых драйверов локальной сети — к примеру, `load se load lbrsl`.
    - Добавьте или проверьте наличие команд `load` для драйверов локальной сети в каждом разделе описания слотов.
    - Для каждой группы выравнивания нагрузки/RSL на всех сетевых адаптерах загрузите одинаковые протоколы и типы кадров.
    - Только для первичного (primary) сетевого адаптера выполните привязку протокола к каждому встречающемуся слотовому разделу.
    - Удалите из каждого вторичного (secondary) сетевого адаптера все команды привязки протоколов `bind`.
    - Для каждой группы добавьте команду `lbrsl group` — она выполнит группировку первичного и вторичного сетевого адаптера. В одной группе может быть только одна команда `lbrsl group`, и она должна регистрировать первичный и вторичный сетевой адаптеры. Поместите эту команду после драйвера.
23. Сохраните файл AUTOEXEC.NCF и вернитесь к мастеру установки.

Проверка драйверов для Windows

После установки всех драйверов необходимо проверить правильность установки драйвера Windows. В операционной системе Windows 2000 это делается следующим образом.

1. Щелкните на значке **My Computer** (Мой компьютер) правой кнопкой мыши, выберите **Properties** (Свойства) и перейдите на вкладку **Hardware** (Оборудование).
2. Нажмите кнопку **Device Manager** (Диспетчер устройств).
3. На экране **Device Manager** (Диспетчер устройств) откройте вкладку **Network Adapters** (Сетевые платы). В списке сетевых адаптеров должен быть указан ваш сетевой адаптер (рис. 10.4). Закройте это окно. Если записи о вашем сетевом адаптере нет, значит, плата была установлена неправильно. Если рядом с записью о сетевом адаптере стоит желтый восклицательный знак, возможно, установлены не те драйверы. Удалите драйвер сетевой платы и установите его заново (если возможно, проверьте наличие обновлений драйвера).
4. Если в окне **Device Manager** (Диспетчер устройств) есть записи о старом и новом сетевом адаптере, следует удалить запись о старом, а затем перезагрузить систему, чтобы никаких записей о старом сетевом адаптере не сохранилось.

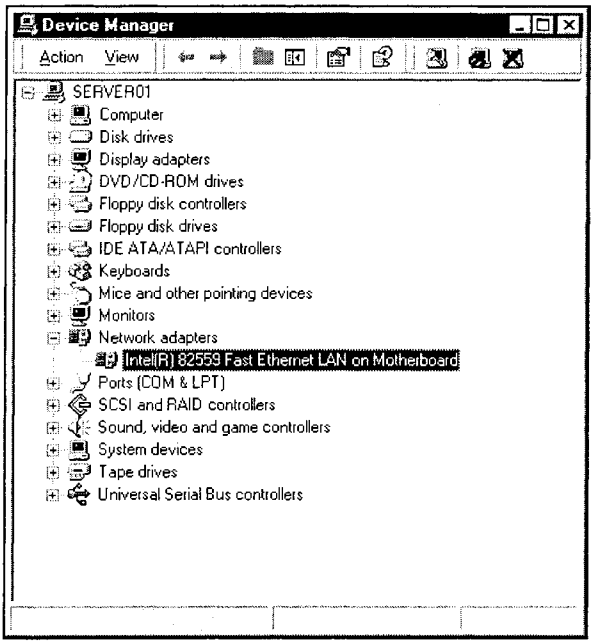


Рис. 10.4. Проверка установки сетевого адаптера в среде Windows 2000

Проверка драйверов для NetWare

Чтобы проверить правильность загрузки драйвера на сервере NetWare, выполните следующую последовательность действий.

1. В системной командной строке введите `load monitor`. В результате появится экран **NetWare Monitor**.
2. В меню **Available Options** (Допустимые параметры) выберите **LAN/WAN Drivers**. Появится меню **Available LAN Driver** (Доступные драйверы локальной сети). Если драйвер был загружен правильно, в этом меню он будет указан вместе с его типами кадров.
3. Выберите драйвер, чтобы просмотреть связанные с ним статистические данные (действующий драйвер всегда отображает отсылаемые и принимаемые пакеты).
4. Чтобы убедиться в том, что сервер выполняет передачу данных через сеть, выполните еще два шага.
5. Выполните настройку клиента NetWare в локальной сети тестируемого сервера.
6. Попробуйте установить связь с сервером. Если сделать это не получается, то связи с сервером нет. Если же связь есть, на сервере появится следующее сообщение:

```
Link integrity test for primary slot #XXXXX passed
```

Конфигурирование стандартных драйверов

Если вы установили стандартный драйвер сетевого адаптера, то сейчас нужно выполнить его настройку. Как это сделать, зависит от того, какой операционной системой вы пользуетесь: Windows NT, Windows 2000 или Novell NetWare. В этом разделе приводится последовательность действий по конфигурированию драйвера в среде Windows NT.

1. В окне **New Hardware Found** (Обнаружено новое устройство) для каждого порта сетевого адаптера назначено автоопределение и применение типа соединения по умолчанию, что всегда будет выявлять подключенный порт и устанавливать подходящие скорость и режим передачи.

Примечание

Если программа запрашивает компакт-диск с Windows NT, необходимо будет переустановить и последнюю версию Windows NT Service Pack, а затем перезапустить систему.

2. Проверьте, все ли порты сетевого адаптера указаны в окне **New Hardware Found** (Обнаружено новое устройство).
3. В окне **New NIC Port(s) Available** (Доступные порты новой сетевой платы) выберите нужный порт.
4. В списке **Connection Types** (Типы соединения) выберите тип соединения для вашей сети или используйте **Autodetect Default Connection** (Автоматическое определение соединения по умолчанию).
5. Нажмите кнопку **Apply** (Применить).
6. Повторите первые четыре шага для каждого порта.
7. Нажмите кнопку **OK**.
8. Нажмите кнопку **Close** (Закрыть) в окне **Network** (Сеть).
9. Перезагрузите систему.

Установка системы восстановления после отказа

Если на вашем сервере есть много портов или адаптеров, вы можете использовать такие возможности, как группировка (агрегирование) адаптеров, выравнивание нагрузки и т. д. На рис. 10.5 представлен образец настройки сетевого адаптера. К примеру, на сервере в среде Windows NT 4.0 можно установить драйвер восстановления после отказа. Это позволит обеспечить определенный запас избыточности в сети. Рассмотрим установку драйвера восстановления после отказа на примере.

Настройка портов

Вам придется настроить порты вашего сетевого адаптера. При настройке сетевого адаптера придерживайтесь следующей последовательности.

1. В окне **New Hardware Found** (Обнаружено новое устройство) для каждого порта сетевого адаптера задается автоопределение и применение типа соединения по умолчанию, что всегда будет выявлять соединение порта и устанавливать скорость и режим передачи.

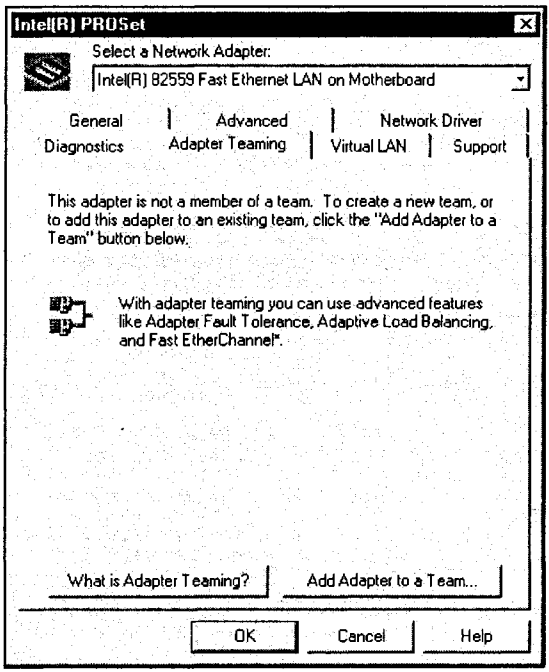


Рис. 10.5. Настройка функций сетевого адаптера на сервере в среде Windows 2000

2. Убедитесь в том, что в окне **New Hardware Found** (Обнаружено новое устройство) перечислены все порты сетевого адаптера.
3. В окне **New NIC Ports Available** (Порты новой сетевой платы) выберите нужный порт.
4. В списке **Connection Types** (Типы соединения) выберите тип соединения для вашей сети или используйте **Autodetect Default Connection** (Автоматическое определение соединения по умолчанию).
5. Нажмите кнопку **Apply** (Применить).
6. Повторите первые четыре шага для каждого порта.
7. Закончив, нажмите кнопку **OK**.

Выбор пары для восстановления после отказа

В среде Windows NT 4.0 можно создать пары для восстановления после отказа на вкладке **Configuration** (Конфигурация). Отказоустойчивая пара состоит из двух портов: первичного и резервного. Сделайте следующее.

1. В окне **Available Ports** (Доступные порты) выберите порт, который будет назначен первичным.
2. Нажмите кнопку **Add** (Добавить). Выбранный порт будет помечен как Primary Port (первичный порт) в списке **Failover Pair** (Отказоустойчивая пара).

3. Чтобы назначить резервный порт для первичного порта, выберите нужный порт в окне **Available Ports** (Доступные порты), а затем нажмите кнопку **Add** (Добавить). Этот порт будет добавлен в поле **Backup Port** (Резервный порт).
4. Нажмите кнопку **Add** (Добавить).
5. Чтобы создать еще одну такую пару, повторите первые четыре шага.

Примечание

Чтобы удалить отказоустойчивую пару, выберите порт в списке **Primary Ports** (Первичные порты) и нажмите кнопку **Remove** (Удалить). В результате оба порта будут возвращены в окно **Available Ports** (Доступные порты). Нажмите кнопку **Apply** (Применить).

6. Нажмите кнопку **OK**, и вы перейдете обратно на вкладку **Adapters** (Сетевые платы).
7. Если протокол SNMP не настроен, на экране появится сообщение об ошибке. Нажмите кнопку **OK**.
8. Введите данные протокола (при необходимости получения дополнительной информации о конфигурировании этого протокола вы можете обратиться к документации по Windows NT 4.0).
9. Закончив, извлеките дискету с драйверами из дисковода и перезагрузите систему.

Примечание

Если программа запрашивает компакт-диск с Windows NT, необходимо будет переустановить и последнюю версию Windows NT Service Pack, а затем перезапустить систему.

Мониторинг отказоустойчивых пар

Для мониторинга состояния отказоустойчивых пар вы можете воспользоваться инструментальными средствами Windows NT или специализированным программным обеспечением. Есть несколько способов выполнения этих задач.

- SNMP-менеджер. В случае восстановления после сбоя уведомления SNMP рассылаются в пункты управления сетью, а журналы регистрации ошибок обновляются с помощью журнала регистрации ошибок операционной системы. К примеру, для управления агентами SNMP выполните компиляцию файла MIB (Management Information Base — информационная база управления) a:\snmpmibs \duralink.mib на управляющей станции SNMP.
- Диалоговое окно **Event Viewer** (Просмотр событий). В Windows NT регистрация отказов портов производится с помощью локального диалогового окна **Event Viewer** (Просмотр событий).
- Поставляемое производителем программное обеспечение восстановления после отказа. Производитель может поставлять программное обеспечение (например, программа восстановления после отказа Adaptec Duralink64), которое выполняет текущий контроль трафика и степени исправности пар для восстановления после отказа.

Установка системы агрегирования портов

В среде Windows NT 4.0 или 2000 у вас есть возможность применения драйверов агрегирования портов сетевого адаптера. Это поможет распределить нагрузку по передаче данных между портами сетевого адаптера и повысить пропускную способность.

Примечание

В инструкциях, приведенных в этом разделе, предполагается, что вы работаете в операционной системе Windows NT. Если вы используете Windows 2000 или другую сетевую операционную систему, то для получения указаний по установке обратитесь к руководству по эксплуатации сетевого адаптера.

Настройка портов

Для начала необходимо настроить работу портов сетевого адаптера в режиме восстановления после отказа. Для выполнения настройки в среде Windows NT придерживайтесь следующей последовательности шагов.

1. В окне **New Hardware Found** (Обнаружено новое устройство) для каждого порта сетевого адаптера определяется автоматическое распознавание и тип соединения по умолчанию, который всегда будет выявлять соединение порта и устанавливать скорость и режим передачи.
2. Убедитесь в том, что в окне **New Hardware Found** (Обнаружено новое устройство) перечислены все порты сетевого адаптера.
3. В окне **New NIC Ports Available** (Порты новой сетевой платы) выберите нужный порт.
4. В списке **Connection Types** (Типы соединения) определите тип соединения в вашей сети или выберите **Autodetect Default Connection** (Автоматическое определение соединения по умолчанию).
5. Нажмите кнопку **Apply** (Применить).
6. Повторите первые пять шагов в отношении каждого существующего порта.
7. Закончив, нажмите кнопку **OK**.
8. Теперь, как показано в следующем разделе, можно создавать группы агрегирования портов.

Создание групп агрегирования

Теперь создаваемой группе агрегирования портов необходимо присвоить порты сетевого адаптера, чтобы создать виртуальный порт. К примеру, чтобы настроить систему агрегирования портов в операционной системе Windows NT, выполните следующую последовательность действий.

1. В поле **Group(s)** (Группа) нажмите кнопку **Create New Group** (Создать новую группу), а затем введите имя новой группы. Длина имени не должна превышать 20 символов. Если пропустить этот этап, система назначит группе имя по умолчанию (например, GroupX).
2. В поле **Link Aggregation Type** (Тип соединения) выберите подходящий тип соединения.

3. В поле **Available Ports** (Доступные порты) выберите доступный порт, который вы хотите включить в группу, и нажмите кнопку **Add** (Добавить).

Для агрегирования других портов повторите шаг 3. Помните, что для всех портов в пределах одной группы необходимо определять одинаковый тип соединения. Чтобы удалить порт из группы, сделайте следующее.

1. Выберите нужный порт в окне **Group Ports** (Порты группы) и нажмите кнопку **Remove** (Удалить).
2. После того как вы выберете все порты для удаления, нажмите кнопку **Apply** (Применить).
3. Чтобы создать другую группу, повторите пять шагов, приведенных выше.
4. Если вы хотите переименовать группу, выберите ее имя, принятое по умолчанию, в списке **Group(s)** (Группа), введите новое имя и нажмите кнопку **Apply** (Применить).
5. После настройки всех групп нажмите кнопку **OK**.
6. Если протокол SNMP на компьютере не настроен, на экране появится сообщение об ошибке, просто нажмите кнопку **OK**.
7. В окне **Network** (Сеть) нажмите кнопку **Close** (Закрыть).
8. Теперь присвойте агрегированной группе адрес TCP/IP.

Создание групп FEC

Технология Fast EtherChannel компании Cisco позволяет выполнять полное агрегирование двух или четырех портов с целью передачи и получения данных для всех протоколов. Порты, включенные в группу Fast EtherChannel, должны быть физически подсоединены к портам Fast EtherChannel коммутатора Cisco (процедура настройки портов коммутатора Cisco в режиме Fast EtherChannel приводится в документации к коммутатору Cisco). Если выбрать Fast EtherChannel на сервере, в качестве типа соединения для каждого порта будет автоматически определен TX/Full Duplex на 100 Мбит/с. Кроме того, вам нужно будет выполнить настройку портов группы Fast EtherChannel на коммутаторе Cisco. В среде Windows NT, как показано в следующем примере, их нужно настроить на работу в одном из двух режимов: Auto Negotiation (автосогласование) или Full Duplex на 100 Мбит/с.

1. В поле **Group(s)** (Группа) нажмите кнопку **Create New Group** (Создать новую группу), а затем введите имя новой группы. Длина имени не должна превышать 20 символов. Если пропустить этот этап, система назначит группе имя по умолчанию (например, GroupX).
2. В поле **Link Aggregation Type** (Тип соединения) выберите подходящий тип соединения.
3. В поле **Available Ports** (Доступные порты) выберите порт, который вы хотите включить в группу, и нажмите кнопку **Add** (Добавить).

Для добавления дополнительных портов в группу повторите шаг 3. Помните, что для всех портов одной группы необходимо определять одинаковый тип соединения. Чтобы удалить порт из группы, сделайте следующее.

1. Выберите нужный порт в окне **Group Ports** (Порты группы) и нажмите кнопку **Remove** (Удалить).

2. Закончив, нажмите кнопку **Apply** (Применить).
3. Чтобы создать другую группу, повторите три шага из *разд. "Создание групп агрегирования"*.
4. При желании переименовать группу выберите ее имя, принятое по умолчанию, в списке **Group(s)** (Группа), введите новое имя и нажмите кнопку **Apply** (Применить).
5. После настройки всех групп нажмите кнопку **OK**.
6. Если протокол SNMP не настроен, на экране появится сообщение об ошибке, просто нажмите кнопку **OK**.
7. В окне **Network** (Сеть) нажмите кнопку **Close** (Закрыть).
8. Теперь присвойте агрегированной группе FEC адрес TCP/IP.

Назначение адреса TCP/IP

После настройки агрегирования портов Windows NT пригласит вас выполнить конфигурацию протокола. IP-адреса присваиваются группам и автономным портам на вкладке **IP Address** (IP-адрес). Порты, относящиеся к одной группе, используют один и тот же IP-адрес, так что вводить его нужно лишь один раз. Чтобы назначить адрес TCP/IP, сделайте следующее.

1. На вкладке **IP Address** (IP-адрес) выберите порт сетевого адаптера (например, DuraLAN) из списка **Adapter** (Сетевые платы).
2. В поле **IP Address** (IP-адрес) введите IP-адрес.
3. В поле **Subnet Mask** (Маска подсети) введите номер маски подсети (и адрес шлюза, если необходимо) и нажмите кнопку **Apply** (Применить).
4. Повторите эти шаги для любого другого порта или группы.
5. По окончании нажмите кнопку **OK**.
6. Для сохранения изменений перезагрузите компьютер — нажмите кнопку **Yes** (Да), когда появится запрос на перезагрузку компьютера. Теперь, при необходимости, вы можете проверить состояние системы или внести изменения в группы.

Изменение групп агрегирования портов

После установки драйвера агрегирования портов и настройки групп их конфигурацию можно изменить. Ниже показано, как можно переименовать группы, а также добавить или удалить порты из существующих групп в среде Windows NT. Чтобы переименовать группу, сделайте следующее.

1. В окне агрегирования портов сетевого адаптера (т. е. в окне **Duralink64 Port Aggregation**) перейдите на вкладку **Configuration** (Конфигурация).
2. В поле **Group(s)** (Группа) выберите нужную группу, а затем введите ее новое имя.
3. Чтобы сохранить изменения, нажмите кнопку **Apply** (Применить).

Чтобы добавить или удалить порт, сделайте следующее.

1. В окне агрегирования портов сетевого адаптера (т. е. в окне **Duralink64 Port Aggregation**) перейдите на вкладку **Configuration** (Конфигурация).

2. В поле **Group(s)** (Группа) нажмите кнопку **Create New Group** (Создать новую группу), введите имя новой группы (или выберите группу, которую планируете изменить).
   - Чтобы добавить в группу новые порты, выберите нужный порт в окне **Available Adaptec Ports** (Доступные порты Adaptec) и нажмите кнопку **Add** (Добавить).
   - Чтобы удалить порты из группы, выберите нужный порт в окне **Group Ports** (Порты группы) и нажмите кнопку **Remove** (Удалить).
3. Для добавления или удаления каждого нового порта повторите предыдущий шаг.
4. Чтобы сохранить изменения, нажмите кнопку **Apply** (Применить).
5. Нажмите кнопку **OK**.
6. Если протокол SNMP не настроен, на экране появится сообщение об ошибке, просто нажмите кнопку **OK**.
7. При добавлении или удалении группы или порта на экране появится сообщение об ошибке, нажмите кнопку **OK**.
8. В окне **Network** (Сеть) нажмите кнопку **Close** (Закрыть).

Примечание

При добавлении или удалении порта IP-адрес группы или порта удаляется автоматически. Следите за назначением и удалением всех IP-адресов, чтобы использовать их впоследствии.

Проверка состояния системы

Проверить состояние группы или автономного порта можно следующим образом.

1. В меню **Start** (Пуск) переместите указатель на пункт **Settings** (Настройки) и щелкните на значке **Control Panel** (Панель управления).
2. В меню **Control Panel** (Панель управления) двойным щелчком выберите **Network** (Сеть).
3. В окне **Network** (Сеть) перейдите на вкладку **Adapters** (Сетевые платы).
4. На вкладке **Adapters** (Сетевые платы) выберите сетевой адаптер (например, Adaptec DuraLAN). В результате появится окно **Port Aggregation** (Агрегирование портов).
5. Нажмите кнопку **Properties** (Свойства).
6. Для получения информации о группе или автономном порте перейдите на вкладку **Status** (Состояние).
7. Для выхода нажмите кнопку **OK**.

Поиск и устранение неисправностей сетевого адаптера

Несмотря на то, что, как правило, большинство сетевых адаптеров устанавливаются и работают безошибочно, есть немало ситуаций, когда на сервере или рабочей стан-

ции происходят сбои. Неисправность может обнаружиться в процессе монтажа аппаратуры, при прокладке сетевого кабеля, установке драйвера или конфигурировании системы. Технический специалист должен уметь оперативно выявлять и устранять неисправности, связанные с сетевыми адаптерами. В этом разделе мы рассмотрим некоторые наиболее распространенные признаки неисправностей сетевых плат и способы их устранения, а также общие диагностические команды для платы Adaptec DuraLAN.

Применение утилиты Performance Monitor

В операционных системах Windows NT/2000 есть утилита Performance Monitor (Монитор производительности)[1], которая позволяет просматривать системный трафик, относящийся к выбранным группам и автономным портам. В этом окне каждая кривая представляет производительность группы или порта, обозначенного в нижней части экрана. Когда активность порта или группы падает, понижаются и показатели кривой. Для выбора портов и групп, которые требуется просмотреть в Windows 2000, сделайте следующее:

1. В меню **Start** (Пуск) поместите указатель на строку **Programs** (Программы), затем на строку **Administrative Tools** (Администрирование) и выберите **Performance** (Производительность). Появится диалоговое окно **Performance**, показанное на рис. 10.6.

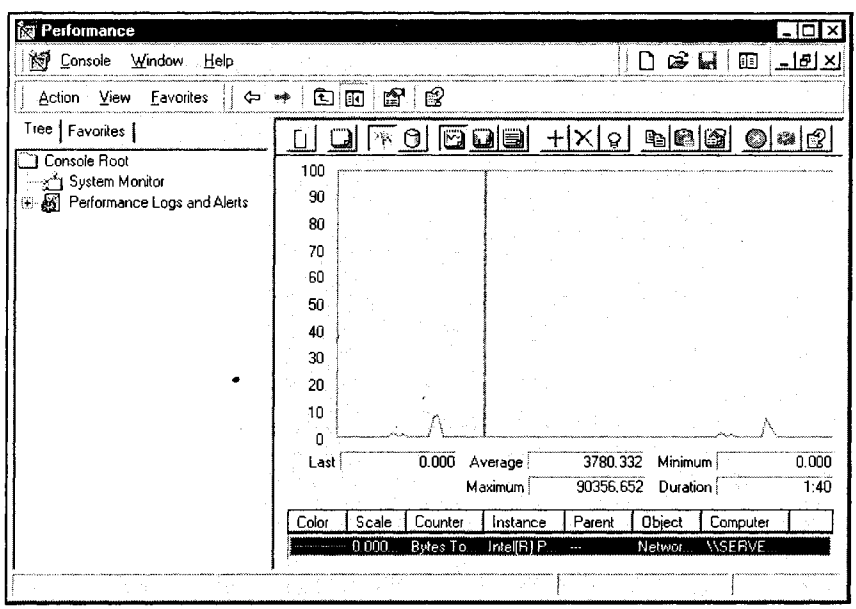


Рис. 10.6. Диалоговое окно **Performance** в операционной системе Windows 2000

[1] В Windows 2000 она называется System Monitor. — *Ред.*

2. В диалоговом окне **Performance** нажмите кнопку **Add** (Добавить), в результате появится окно **Add Counter** (Добавить счетчик).
3. Из списка в окне **Performance** выберите пункт **Network Interface** (Сетевое окружение).
4. В окне **Counters** (Счетчики) выберите элементы, мониторинг которых вы хотите выполнить (например, Bytes Total/sec), а затем выберите устройство (например, ваш сетевой адаптер). Нажмите кнопку **Add** (Добавить), чтобы начать запись.
5. Для изменения внешнего вида элементов диалогового окна **Performance** нажмите кнопку **Properties** (Свойства) (рис. 10.7) и откорректируйте внешний вид графика.
6. Для мониторинга других портов или групп (или других устройств) повторите шаги 4 и 5.
7. Завершив выполнение задачи, нажмите кнопку **Close** (Закрыть).

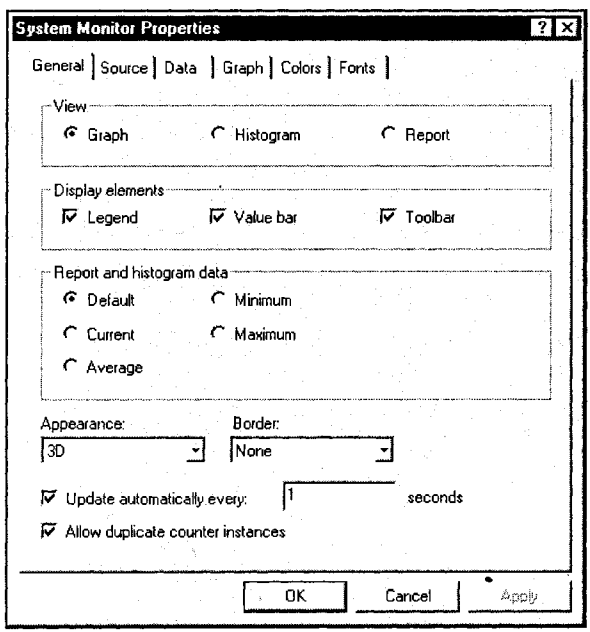


Рис. 10.7. Изменение внешнего вида графика в диалоговом окне **Properties**

Общие рекомендации по поиску и устранению неисправностей

Прежде чем рассматривать возможные неисправности сетевых адаптеров, проверьте правильность установки и настройки этих устройств. Если сетевая плата работает некорректно, убедитесь в том, что ее установка и конфигурация проводились в соответствии с руководством по эксплуатации. Ниже представлены некоторые общие рекомендации по поиску и устранению неисправностей сетевых адаптеров.

- ❒ Проверьте правильность монтажа и настройки сетевого адаптера на хосте согласно рекомендациям производителя. Кроме того, ознакомьтесь с информацией от производителя о применении сетевой платы в условиях вашей операционной системы. Это поможет обнаружить неисправности, связанные с несовместимостью устройства и ОС.
- ❒ При использовании сетевого адаптера на шине PCI убедитесь в том, что для слотов PCI разрешено управление передачей данных по шине.
- ❒ Проверьте надежность подключения сетевого кабеля к сетевому адаптеру и к остальной части сети (т. е. к сетевому концентратору). По необходимости замените кабель.
- ❒ Убедитесь в том, что тип кабеля в вашей сети отвечает требованиям сетевого адаптера (к примеру, для сетевого адаптера Gigabit нужен кабель, соответствующий стандарту IEEE 802.3z 1000BaseSX для Gigabit Ethernet).
- ❒ Убедитесь в том, что на концентраторе, коммутаторе или порте маршрутизатора установлен тот же дуплексный режим, что и на адаптере (дуплексный или полудуплексный режим).
- ❒ Проверьте правильность установки драйвера сетевого адаптера (т. е. драйвера Adaptec DuraLAN).
- ❒ Убедитесь в том, что вы используете драйверы, которые поставлялись вместе с адаптером (по возможности не используйте унифицированные драйверы и драйверы по умолчанию). Вы можете получить последние версии драйверов для вашей сетевой платы у производителя.
- ❒ Если на компьютере установлены другие сетевые адаптеры, они могут стать причиной конфликта. Если возможно, извлеките из компьютера все прочие платы и протестируйте сетевой адаптер отдельно.
- ❒ Используйте на вашем компьютере самую последнюю версию BIOS.
- ❒ Убедитесь в том, что кабель, оконечная нагрузка и коннекторы работают корректно или установите сетевой адаптер в другой слот PCI.
- ❒ Если вы производите замену существующего сетевого адаптера в среде NetWare, проверьте соответствие операторов `link` в файле NET.CFG новому сетевому адаптеру. К примеру, оператор `link` для клиента NetWare должен быть `link driver e100bodi`.
- ❒ В среде NetWare проверьте соответствие типа кадра в файле NET.CFG вашему серверу.
- ❒ При настройке сервера в среде NetWare проверьте операторы `load` и `bind`.
- ❒ В среде Windows NT проверьте загрузку драйвера и установку протоколов. Для этого обратитесь к диалоговому окну **Network Bindings** (Сетевые привязки) системы Windows NT. Если неисправность устранить не удалось, попробуйте сделать следующее.
  - Замените сетевой адаптер на другой заведомо исправный того же типа. Если новый сетевой адаптер будет нормально работать, значит, неисправен исходный сетевой адаптер, который в этом случае следует заменить.
  - Установите сетевой адаптер в другой работающий компьютер и проведите тестирование еще раз. Если на другом компьютере сетевой адаптер работает,

то неисправность связана либо с самим компьютером, либо с аппаратным конфликтом. Также следует проверить кабели и коннекторы компьютера.

PCI-совместимость

Ранние версии BIOS PCI не полностью поддерживают спецификацию PCI, и могут прекратить отвечать при попытке загрузки драйвера сетевого адаптера. В этом случае проверьте, поддерживает ли ваша версия BIOS спецификацию шины PCI Local Bus (v 2.0 или более позднего варианта), или установите последнюю версию BIOS на вашем компьютере. Некоторые системы на базе PCI не обладают возможностью автоматического конфигурирования и требуют выполнения некоторых или всех нижеперечисленных функций путем перестановки перемычек на материнской плате или изменения настроек в программе CMOS Setup.

- Убедитесь в том, что слот PCI является ведущим (bus-master), а не подчиненным (slave) слотом шины. Большинство сетевых адаптеров должно устанавливаться на ведущий слот шины PCI. На некоторых компьютерах слот PCI необходимо настроить на управление передачей данных по шине. Чтобы проверить, является ли слот PCI ведущим слотом шины, обратитесь к руководству по эксплуатации вашего компьютера и зайдите в программу CMOS Setup.
- В некоторых случаях материнская плата вашего компьютера может потребовать установки драйверов управления передачей данных по шине до перехода в режим управления шиной. Проверьте, установлено ли такое программное обеспечение, а в случае необходимости обновите его.
- На некоторых компьютерах может потребоваться отключить режим Plug-and-Play (PnP) в программе CMOS Setup в случае некорректного распределения ресурсов между сетевым адаптером и другими установленными платами. Возможно, потребуется также провести ручную настройку устройств расширения.
- На некоторых компьютерах для установленных плат ISA нужно резервировать прерывания и ячейки памяти для того, чтобы платы PCI не использовали те же настройки. Обратитесь к руководству по эксплуатации вашего компьютера и проверьте настройки CMOS Setup, относящиеся к платам ISA.
- Проверьте, настроен ли слот PCI сетевого адаптера на поддержку INTA.
- Проверьте, чтобы INTA данного слота был присвоен свободный номер прерывания IRQ.
- Проверьте параметры программы CMOS Setup для слота PCI, на котором установлен сетевой адаптер. Этот слот должен быть настроен на прерывания с запуском по уровню, а не по фронту. Пример типичного набора параметров PCI приведен ниже:
  - PCI Slot # (номер гнезда, в котором установлен сетевой адаптер);
  - Master: Enabled;
  - Slave: Enabled;
  - Latency Timer: 40 (в диапазоне от 20 до 255);
  - Interrupt Type: Level-Triggered;
  - Interrupt Number: (выберите любой не конфликтующий с другой установленной платой номер из тех, что предлагают CMOS Setup).

Применение средств диагностики сетевых адаптеров

Сбои в сети динамично работающей компании могут привести к огромным материальным убыткам, поэтому производители сетевых адаптеров разработали встроенные средства диагностики, которые должны ускорять процесс поиска и устранения неисправностей. Эти средства позволяют тестировать основные функции сетевого адаптера и проверять ее способность к взаимодействию с другими платами в сети, поэтому при любом поиске неисправностей стоит использовать диагностические функции сетевого адаптера. Есть два основных способа тестирования: локальный и удаленный.

Локальное тестирование

Локальные тесты помогают проверить основные функции сетевого адаптера. Чтобы подвергнуть сетевой адаптер испытаниям, выберите **Run Loopback Tests** (Запустить тесты для кольцевой проверки) и **Run Internal Tests** (Запустить внутренние тесты). В окне результатов тестирования выбранные тесты должны показывать состояние **Ready** (Готовность). Чтобы запустить тесты, нажмите кнопку **Run Local Tests** (Запустить локальное тестирование). Ход каждого теста отображается в строке состояния **Test Progress** (Прохождение теста). После завершения тестов для вывода их результатов нажмите кнопку **View Test Results** (Просмотр результатов теста). Как правило, если тест для кольцевой проверки и внутренний тест не пройдены, это означает, что сетевой адаптер вышел из строя (или был неправильно установлен).

Удаленное тестирование

Удаленные тесты (они также называются тестами на отправку и получение) проверяют правильность подсоединения сетевого кабеля, при котором сетевой адаптер может передавать и получать данные. Для проведения этого теста требуется наличие двух компьютеров с совместимыми сетевыми адаптерами. При этом один из компьютеров должен работать в режиме отсылки, создавая и отсылая контрольные сообщения. Другой компьютер работает в режиме получения, принимая тестовые сообщения и пересылая их обратно отправителю. Чтобы выполнить этот тест, нажмите кнопку **Send** (Отправка) на одном компьютере и кнопку **Receive** (Прием) на другом. С результатами теста вы можете ознакомиться, нажав кнопку **View Test Results** (Просмотр результатов теста). Если локальные тесты выполнены, а удаленные заканчиваются неудачей, можете быть уверены, что неисправность связана с кабельным соединением, связью или межсетевыми устройствами (концентраторами, коммутаторами или маршрутизаторами), расположенными между двумя станциями. Кроме того, вполне возможно, что одна из двух станций неправильно настроена (к примеру, использует неверный протокол).

Диагностическое программное обеспечение сетевых адаптеров

Многие сетевые адаптеры поставляются вместе с многофункциональными диагностическими программами (DOS), которыми можно пользоваться для проверки производительности сетевых адаптеров. В этом разделе рассматриваются диагностические средства, поставляющиеся с сетевым адаптером Adaptec DuraLAN. Хотя диагностическое программное обеспечение вашего сетевого адаптера может отличаться от рассматриваемого, этот раздел поможет вам ознакомиться с некоторыми наиболее распространенными диагностическими командами.

Запуск диагностической утилиты

Убедитесь в том, что HIMEM.SYS и EMM386.EXE в данный момент находятся в файле CONFIG.SYS, и что в нем присутствует запись `files=30`. Либо добавьте в начало файла CONFIG.SYS следующие строки и выполните нижеперечисленные действия.

```
device=c:\dos\himem.sys
device=c:\dos\emm386.exe /noems
files=30
```

Примечание

Если эти DOS-программы расположены не в каталоге c:\dos, укажите другой путь.

1. Создайте на жестком диске каталог для размещения диагностических средств.
2. Скопируйте все файлы из исходного диагностического каталога в новый каталог на жестком диске.
3. В командной строке DOS введите `go_diags` и нажмите клавишу <Enter>.

Примечание

Протестировать сетевой адаптер DuraLAN проще всего с помощью функции самотестирования.

Назначение основных команд

После запуска диагностической программы вы можете использовать команды, представленные в табл. 10.2 для тестирования сетевого адаптера Adaptec DuraLAN. Помните, что диагностические средства, поставляемые в комплекте с вашим сетевым адаптером, могут быть другими, данный список может выступать в качестве удобного примера и руководства.

Примечание

Для проведения такого тестирования требуется концентратор, коммутатор или кабель с заглушкой (loopback cable). Кроме того, если кабель не подсоединен, следует выполнить автосогласование установок по умолчанию, приравняв их к 10 Мбит/с.

Таблица 10.2. *Типичные команды диагностики сетевого адаптера*[1]

Команда	Назначение	Значение параметров	Объяснение параметров
`Address_filter`	Тестирование функций фильтрации пакетов в Ethernet		

[1] Эти команды предназначены для тестирования сетевой платы Adaptec DuraLAN, но команды для вашей платы, возможно, подобны им.

Таблица 10.2 (продолжение)

Команда	Назначение	Значение параметров	Объяснение параметров
`Autonegotiate <speed>`	Тестирование скорости, на которой плата проводит согласование. Есть пять установок для этого теста	0	Тестирование полного автосогласования (самая высокая скорость)
		10	Тестирование на скорости 10 Мбит/с в полудуплексном режиме
		20	Тестирование на скорости 10 Мбит/с в дуплексном режиме
		100	Тестирование на скорости 100 Мбит/с в полудуплексном режиме
		200	Тестирование на скорости 100 Мбит/с в дуплексном режиме
`Checksum`	Тестирование вычисления контрольной суммы TCP/IP		
`Display`	Отображение значений всех регистров микросхем сетевого адаптера		
`Echoer #/sender #`	Этот тест полезен при проверке сети и передачи данных между агентом echoer и отправителем		
`Eeprom`	Тестирование содержимого последовательной памяти EEPROM сетевого адаптера и его отображение на экране		
`Exit`	Выход из диагностической утилиты		
`External_10`	Для выполнения этого теста требуется кабель с заглушкой (loopback cable). Это кольцевая проверка на скорости 10 Мбит/с		
`External_100`	Для выполнения этого теста требуется кабель с заглушкой (loopback cable). Это кольцевая проверка на скорости 100 Мбит/с		

Таблица 10.2 (продолжение)

Команда	Назначение	Значение параметров	Объяснение параметров
hbi_dma	Проверка передач DMA на сетевой адаптер и из него		
hbi_slave	Тестирование подчиненных обращений (slave accesses), последовательной памяти EEPROM и обращений регистра к микросхеме		
Internal_10_mac	Внутренняя кольцевая проверка на скорости 10 Мбит/с на микросхеме		
Internal_10_phy	Кольцевая проверка с физического устройства на скорости 10 Мбит/с		
Internal_100_mac	Внутренняя кольцевая проверка на скорости 100 Мбит/с на микросхеме		
Internal_100_phy	Внутренняя кольцевая проверка с физического устройства на скорости 100 Мбит/с		
Io	Установка подчиненного обращения в режим I/O (ввода/вывода)		
Loop	Последовательное многократное выполнение тестов		
Mac	Тестирование регистров и различных функций контроллера Ethernet		
Mem (по умолчанию)	Установка подчиненного обращения (slave access) в режим Memory (память)		
Mod (данные смещения mac)	Эта функция позволяет вносить изменения в регистры контроллера Ethernet		
Pause	Тестирование функций контроллера потока микросхемы		
Port X	Определение порта, который вы хотите протестировать		
Power-management	Тестирование функций контроллера Ethernet, связанных с функцией выключения питания		

Таблица 10.2 (окончание)

Команда	Назначение	Значение параметров	Объяснение параметров
`Selftest`	Проверка разнообразных функций сетевого адаптера. Этот тест следует запускать в первую очередь, т. к. он позволяет выявить самые распространенные неисправности сетевых адаптеров		
`Statistics`	Проверка функций микросхемы, связанных со сбором статистических данных		
`Timer`	Тестирование времени задержки прерывания контроллера Ethernet		

Создание загрузочного/регистрационного диска

При возникновении неисправностей, связанных с сетевым адаптером или его доступом к сети, вам может потребоваться загрузочный/регистрационный диск, который позволит загрузить систему в реальном режиме (DOS) и получить доступ к сети. Следующая последовательность действий показывает типичный процесс создания загрузочного/регистрационного диска Windows NT 4.0 для сетевого адаптера локальной сети Intel PRO/100+ (вероятно, для вашего сетевого адаптера потребуются другие файлы, но в целом эта процедура будет одинаковой в среде Windows NT 4.0 для различных сетевых адаптеров). Для этого вам потребуется диск с последней версией драйверов для вашего сетевого адаптера и сервер Windows NT 4.0 с каталогами клиентов (или установочный компакт-диск Windows NT 4.0).

1. Создайте загрузочный диск DOS на компьютере с MS-DOS 6.2x или более поздней версии.
2. Поместите этот диск в дисковод сервера Windows NT 4.0.
3. Выберите в меню **Start** (Пуск) строку **Programs** (Программы), затем строку **Administrative Tools (Common)** (Администрирование) и **Network Client Administrator** (Администратор клиента сети).
4. Пометьте флажок **Make Network Installation Start** (Начать установку сети) и нажмите кнопку **Continue** (Продолжить).
5. Если вы пользуетесь настройками по умолчанию, выберите настройку **Use Existing Shared Directory** (Использовать существующий общий каталог). После этого нажмите кнопку **OK**.
6. Выберите Network Client v3.0 for MS-DOS and Windows в окне **Network Client** (Клиент сети).
7. Выберите ваш сетевой адаптер (например, Intel EtherExpress 16 или 16TP) в списке адаптеров **Network Adapter Card** (Сетевые платы). Нажмите кнопку **OK**.

8. Введите имя компьютера, который вы будете загружать. Введите имя пользователя, под которым вы собираетесь регистрироваться. Введите домен. Укажите сетевой протокол. Нажмите кнопку **OK**.
9. Убедитесь в том, что диск находится в дисководе, и нажмите кнопку **OK** еще раз. После создания диска нажмите **OK** и выйдите из окна **Network Client Administrator** (Администратор клиента сети). При появлении сообщения об управлении памятью нажмите кнопку **OK**.
10. После создания диска вам нужно будет отредактировать три записанных на нем текстовых файла. Для редактирования A:\AUTOEXEC.BAT вы можете воспользоваться любым текстовым редактором. Удалите последние две строки, содержание которых приводится ниже, и сохраните файл.

```
echo Running Setup...
z:\msclient\netsetup\setup.exe /$
```

11. Теперь приступайте к редактированию файла A:\NET\SYSTEM.INI. Перейдите к его разделу, отмеченному как [network drivers] (сетевые драйверы). Вы увидите следующую строку:

```
netcard=exp16.dos
```

12. Замените имя драйвера, расположенное после знака равенства, на имя файла .DOS (NDIS), который находится на диске с драйверами для вашего сетевого адаптера. К примеру, если вы используете сетевой адаптер Intel PRO/100+, содержание этой строки должно быть следующим:

```
netcard=e100b.dos
Save the file.
```

13. Отредактируйте файл A:\NET\PROTOCOL.INI. Перейдите к его разделу, помеченному как [ms$ee16]. В нем есть следующая строка:

```
drivername=EXP16$
```

14. Замените имя драйвера, расположенное после знака равенства, на имя файла .DOS (NDIS). К примеру, если вы используете сетевой адаптер Intel PRO/100+, содержание этой строки должно быть следующим:

```
drivername=e100b$
```

15. Сохраните файл.
16. Скопируйте драйвер NDIS (обычно им является файл с расширением .dos) с диска с драйверами сетевого адаптера в каталог A:\NET на загрузочном диске.
17. Теперь вы сможете загрузить этот диск и с его помощью зарегистрироваться на сервере Windows NT 4.0.

Симптомы неисправностей

Если после ознакомления с приведенными выше общими рекомендациями и решениями вы все еще испытываете трудности, можете обратиться к целому набору решений для специфических признаков неисправности сетевых плат. В этой части главы рассматриваются наиболее часто встречающиеся симптомы неисправностей.

Симптом 10.1. Сетевой адаптер конфликтует с установленным на шине PCI адаптером SCSI

Вероятно, имеет место конфликт прерываний (или другой конфликт, связанный с ресурсами) между двумя устройствами. Нужно настроить сетевой адаптер и адаптер SCSI на применение разных прерываний с помощью BIOS (CMOS Setup), утилиты конфигурации системы (SCU, System Configuration Utility) или утилиты конфигурации EISA (ECU, EISA Configuration Utility), предоставляемой производителем системы. Если адаптер SCSI не совместим со стандартом Plug-and-Play, то лучше заменить его адаптером, поддерживающим PnP (на шине PCI), причем настройка такого адаптера и управление им автоматически выполняется самой системой.

Симптом 10.2. Сетевой адаптер успешно прошел диагностические тесты, но установить сетевое соединение не удается

Другими словами, сетевой адаптер прошел локальное диагностическое тестирование, но не прошел удаленную диагностику. Зачастую это может быть вызвано неисправностью сетевых соединений или конфигурацией сети. Начните с проверки сетевого кабеля и надежности его подключения (а при необходимости — и его оконечной нагрузки). Если вы работаете в среде NetWare, проверьте, указан ли в файле NET.CFG правильный тип кадров. Наконец, проверьте установки дуплексного режима и убедитесь в том, что настройка дуплексного режима (т. е. полудуплексный или дуплексный режим) на сетевом адаптере соответствует настройкам на концентраторе, коммутаторе или маршрутизаторе.

Симптом 10.3. При загрузке драйверов компьютер зависает

В большинстве случаев такой тип неисправности означает, что настройка сетевого адаптера на хосте выполнена неверно — как правило, из-за того, что не была проведена корректировка настроек шины PCI с помощью CMOS Setup. Возможно, вы обнаружите, что настройки прерываний PCI ошибочны. Даже если эти настройки приемлемы для сетевого адаптера, попробуйте установить другое подходящее распределение прерываний PCI. Если в вашей системе загружается модуль EMM386, убедитесь в том, что его версия не ниже 4.49 (именно эта версия поставляется с MS-DOS 6.22 и последующими вариантами этой системы).

Симптом 10.4. Драйвер сетевого адаптера не загружается или не опознает плату NIC

Обычно это связано с конфигурацией системы, а именно с настройками шины PCI. В первую очередь заново проверьте установку сетевого адаптера. Проверьте соответствие настроек BIOS (с помощью CMOS Setup) рекомендуемым настройкам для вашего сетевого адаптера. Иногда функция управления передачей данных по шине PCI отключена по умолчанию. Если это так, ее нужно активировать.

Симптом 10.5. При установке драйверов сетевого адаптера процедура Setup сообщает о том, что адаптер "Не разрешен BIOS" ("Not enabled by BIOS")

Программа установки драйвера не может обнаружить сетевой адаптер. Практически во всех случаях это говорит о том, что из-за неверной настройки (с помощью CMOS Setup) BIOS не может обнаружить сетевой адаптер на шине PCI. В разделе об установке сетевого адаптера обратите внимание на советы по настройке BIOS или озна-

комьтесь с рекомендациями по настройке BIOS для вашего сетевого адаптера в инструкции по эксплуатации сетевого адаптера.

Симптом 10.6. Вы постоянно сталкиваетесь с проблемами при назначении прерывания IRQ 15 сетевому адаптеру

Это встречается в среде Novell NetWare и почти во всех случаях связано с неисправностью аппаратных ресурсов, вызванных конфликтующими прерываниями. Либо отключите IRQ 15, либо присвойте сетевому адаптеру другое прерывание.

Симптом 10.7. Система зависает при загрузке

Часто такое происходит после установки сетевого адаптера. В первую очередь, проверьте установку сетевого адаптера в слоте PCI; кроме того, тщательно проверьте проводку внутренних кабелей системы. Возможно, вам также потребуется обновить BIOS, обратитесь к производителю компьютера. Если неисправность сохраняется, можно предположить наличие аппаратного конфликта между сетевым адаптером и другим устройством в компьютере. Обратитесь к Диспетчеру устройств (**Device Manager**) и измените настройки конфликтующих устройств.

Симптом 10.8. При выполнении автосогласования с помощью диагностической утилиты сетевого адаптера светодиод этой платы не светится

Скорее всего, вы обнаружите, что перед тестированием сетевого адаптера вы забыли подсоединить подходящий кабель с заглушкой (loopback cable). Пользуйтесь подходящим кабелем от производителя сетевого адаптера (или изготовьте кабель с заглушкой самостоятельно, по инструкции, приведенной в руководстве по эксплуатации сетевого адаптера).

Симптом 10.9. Светодиод связи (LNK) сетевого адаптера не светится

Сетевой адаптер не подключен к сети. Есть множество причин этой неисправности. Попробуйте выполнить следующее:

- проверьте драйверы сетевого адаптера и установите самые последние версии драйверов;
- проверьте все сетевые соединения на сетевом адаптере и концентраторе;
- переключитесь на другой порт концентратора (возможно, тот порт, который вы использовали, неисправен);
- проверьте, чтобы настройка дуплексного режима на адаптере (т. е. полудуплексный или дуплексный режим) соответствовала аналогичной настройке на концентраторе;
- убедитесь в том, что между адаптером и концентратором проложен кабель нужного типа — для некоторых концентраторов необходим перекрестный кабель, в то время как другие требуют наличия кабеля прямого соединения.

Симптом 10.10. Светодиод активности (ACT) сетевого адаптера не светится

Во-первых, может быть, что в данный момент в сети нет трафика. Попробуйте обратиться к серверу и посмотрите, начнет ли при этом светиться светодиод ACT. Если сетевой адаптер не откликается, проверьте, установлены ли у вас последние версии

сетевых драйверов. Если неисправность устранить не удается, значит, сетевой адаптер не передает и не принимает данные. Практически всегда это означает, что сетевой адаптер (или порт сетевого адаптера) неисправен: установите другой сетевой адаптер или поменяйте порт сетевого адаптера.

Симптом 10.11. Сетевой адаптер прекратил работать после установки на компьютер другой платы этого типа

Практически во всех случаях это связано с аппаратным конфликтом между двумя сетевыми адаптерами. Проверьте ресурсы, выделенные каждому сетевому адаптеру, и убедитесь в том, что они не используют одни и те же ресурсы (IRQ, DMA, I/O, ОЗУ или ПЗУ). Попробуйте переустановить сетевые адаптеры. Проверьте, поддерживают ли BIOS, операционная система и сетевые адаптеры "совместное использование прерываний" (для плат PCI). Если BIOS, операционная система или сетевой адаптер не поддерживают "совместное использование прерываний", возможно, этот элемент системы придется заменить, чтобы обеспечить полную поддержку дополнительных сетевых адаптеров. К примеру, возможно, вы используете старую систему, BIOS материнской платы которой не обеспечивает полную поддержку PCI и PnP, или у вас устаревшая модель сетевого адаптера или же операционная система OS/2, которая не поддерживает совместное использование прерываний PCI. Помимо этого проверьте сетевые кабели и убедитесь в том, что каждый порт сетевого адаптера соединен с сетевым кабелем.

Симптом 10.12. В среде Windows 2000 не обнаруживается BNC-соединение

При использовании сетевого адаптера в режиме "автоматического обнаружения" распознавание BNC-соединения не происходит. Как правило, сетевые адаптеры подключаются с помощью BNC-, AUI- или коннекторов витой пары, а программные драйверы для большинства адаптеров могут автоматически распознавать тип применяемого коннектора. Впрочем, в некоторых случаях эти драйверы распознают только коннекторы витой пары и могут оказаться неспособными к распознаванию соединений с помощью BNC или коаксиального кабеля. Это может произойти, если используемый коннектор неправильно определяется системой Windows 2000. Чтобы избежать такой ситуации, настройте адаптер на применение BNC-коннектора вместо функции автоматического распознавания. Эта настройка, как правило, располагается в свойствах сетевого адаптера в Диспетчере устройств (Device Manager).

Симптом 10.13. Сетевой адаптер сначала работал, а потом прекратил работу без видимых причин

Когда сетевой адаптер прекращает работать, в первую очередь следует попытаться запустить программу его диагностики. Если этой программе не удается обратиться к сетевому адаптеру или обнаружить его, попробуйте переустановить сетевую плату или установите ее в другой слот. Кроме того, возможно, файлы с драйвером сетевого адаптера повреждены или удалены. Удалите старые драйверы и установите последние версии драйверов. Если программа диагностики смогла обратиться к сетевому адаптеру и сообщила о том, что он неисправен, его следует заменить на аналогичную модель. Если сетевой адаптер отвечает и успешно проходит диагностическое тестирование, то возможно, неисправность на хосте связана с аппаратным или программным обеспечением, и ее нужно локализовать. Проверьте все остальные устройства системы и вспомните, не проводилась ли перед возникновением неисправ-

ности установка нового программного обеспечения (кроме того, следует проверить, нет ли в сети вирусов).

Симптом 10.14. Вы сталкиваетесь с неполадками при использовании сетевого адаптера Xircom CE3 в среде Windows 2000

При использовании сетевого адаптера Xircom CE3 вы рискуете столкнуться с множеством неисправностей. Во время передачи файла большого объема связь в сети может быть прервана (ее можно восстановить путем переустановки сетевого адаптера). Если установить сетевой адаптер, но не подключить к нему сетевой кабель, то центральный процессор будет испытывать максимальные перегрузки, в результате чего произойдет полный отказ системы. В других случаях создается впечатление, что связь с сетью установлена, хотя кабель при этом не подключен. Такие неисправности вызваны исключительно аппаратным обеспечением и возникают при использовании сетевого адаптера Xircom CE3 0340C (или более ранней версии). Проверьте версию микропрограммного обеспечения сетевого адаптера (в большинстве случаев она указана на наклейке с серийным номером на плате Xircom). Если у вас более старая версия этого сетевого адаптера, необходимо получить обновленное микропрограммное обеспечение от производителя Xircom или заменить плату.

Симптом 10.15. Вы получаете сообщение типа "Конфигурация адаптера не была сохранена. Для определения текущих настроек проверьте конфигурацию"

Почти во всех случаях это сообщение означает, что сетевой адаптер обнаружил неисправность при конфигурировании программного обеспечения, а внесенные изменения сохранены не были. Проверьте текущую конфигурацию программного обеспечения и убедитесь в том, что сброса настроек не происходило. Чтобы изменить настройки сетевого адаптера, воспользуйтесь утилитой конфигурации (на дискете с драйверами) для сетевого адаптера. Или установите плату на другом компьютере и запустите утилиту конфигурирования программного обеспечения.

Симптом 10.16. Связь между сетевым адаптером и эхо-сервером (echo server) установить не удалось

Сетевой адаптер (например, EtherLink 16) не может обмениваться пакетами с работающим эхо-сервером. Вполне возможно, что эхо-сервер функционирует некорректно. Проверьте, чтобы компьютер, настроенный в сети как эхо-сервер, нормально работал и не сообщал об ошибках. Проверьте кабельные соединения сетевого адаптера и адаптера сетевого эхо-сервера.

Симптом 10.17. Появляется ошибка, указывающая на сбой адресного программируемого ПЗУ (address PROM)

Это означает, что сетевой адаптер не может считать данные, хранящиеся в его адресной памяти PROM, в результате чего внутренняя диагностика сетевого адаптера не выполняется. Либо неисправна микросхема ППЗУ сетевого адаптера, либо адаптер не может получить к ней доступ. Возможно, микросхема плохо закреплена. Извлеките сетевую плату из компьютера и проверьте установку модуля ППЗУ, затем переустановите сетевой адаптер в компьютер. Если неисправность устранить не удалось, вероятно, поврежден сетевой адаптер. Замените его.

Симптом 10.18. Появляется сообщение о сбое теста прерываний

Либо уровень прерывания сетевого адаптера в компьютере настроен неправильно (например, вместо запуска по уровню установлен запуск по фронту), либо ненадежно установлен сам адаптер. Пользуясь утилитой конфигурирования (на дискете с драйверами), выполните реконфигурацию уровня прерывания сетевого адаптера. Если изменение уровня прерывания не приведет к желаемому результату, переустановите сетевой адаптер или установите новый.

Симптом 10.19. Вы наблюдаете ошибку типа "Сбой при тестировании микросхемы сетевого сопроцессора"

Микросхема сетевого сопроцессора сетевого адаптера не прошла диагностическое тестирование. Ошибка связана либо с микросхемой сетевого сопроцессора, либо со способностью платы обращаться к ней. Тщательно проверьте установку и настройку сетевого адаптера. Если неисправность устранить не удалось, то микросхема (и сетевой адаптер), скорее всего, повреждена и ее придется заменить.

Симптом 10.20. Появляется сообщение о сбое при прохождении теста ОЗУ NIC

Встроенная память (буфер) сетевого адаптера во время диагностического тестирования дала сбой. Возможно, настройка базового адреса ОЗУ сетевого адаптера конфликтует с другими устройствами. Кроме того, есть вероятность неисправности, связанной с ОЗУ (или со способностью сетевого адаптера обращаться к нему). Проверьте правильность конфигурации сетевого адаптера, выберите подходящий базовый адрес его ОЗУ и проверьте сетевую плату еще раз. Если плата сконфигурирована правильно, удалите ее и выполните повторную установку. Если сетевой адаптер неисправен, замените его.

Симптом 10.21. Вы наблюдаете ошибку типа "Сбой теста простой передачи (simple transmit test)"

Сетевой адаптер не может выполнить передачу небольших пакетов данных приемопередатчику, и диагностическое тестирование окончилось неудачей. В этом случае причина заключается в неисправности сетевого соединения. Проверьте, чтобы сетевой адаптер был подключен к сети или на нем стояла заглушка. Помните, что при использовании заглушки значение программной опции "Transceiver Type" (тип приемопередатчика) должно быть установлено на ONBOARD. Чтобы проверить или (при необходимости) изменить настройки этой опции, вы можете воспользоваться утилитой конфигурирования (на дискете с драйверами).

Симптом 10.22. Вы наблюдаете ошибку типа "Невозможно обнаружить эхо-сервер"

Сетевой адаптер не может обнаружить в сети эхо-сервер. Убедитесь в том, что один из работающих компьютеров, подключенных к сети, настроен как эхо-сервер, причем он не передает сообщения об ошибках. В большинстве случаев источником появления этой ошибки является проводка сетевых кабелей, поэтому проверьте кабельные соединения сетевого адаптера и адаптера на эхо-сервере. Если неисправность устранить не удалось, скорее всего, виноват эхо-сервер, попробуйте проверить сетевой адаптер на другой рабочей станции с другим сервером.

Симптом 10.23. Вы наблюдаете ошибку типа "Ваша система выполняет кэширование в верхней области памяти (high memory) — вы должны отключить кэширование в базовой области адресов ОЗУ 64 Кбайт"

В большинстве случаев эта неисправность появляется из-за конфликта ОЗУ. Если в верхней области памяти вашей системы выполняется кэширование доступа к ОЗУ, оно, вероятно, конфликтует с установленным значением размера ОЗУ адаптера. Убедитесь в том, что размер ОЗУ, равный 64 Кбайт, применяется только с базовыми адресами ОЗУ F00000h или выше (F20000h, F40000h, F60000h, F80000h). Либо отключите кэширование ОЗУ, либо установите некэшируемую область памяти.

Симптом 10.24. Появляется ошибка вида "Размер ОЗУ слишком велик для базового адреса ОЗУ 0d8000. Определите ОЗУ в размере 16 или 32 Кбайт"

Базовый адрес ОЗУ слишком велик. Вероятно, вам придется уменьшить размер буфера до 16 или 32 Кбайт по базовому адресу ОЗУ 0D8000h. Если установить больший размер ОЗУ (например, 48 или 64 Кбайт), эта настройка автоматически уменьшает его до 32 Кбайт, т. к. это максимальный размер буфера ОЗУ для базового адреса 0D8000h. Вы должны либо согласиться с размером ОЗУ, определяемым автоматически (32 Кбайт), либо выбрать более низкий базовый адрес ОЗУ, чтобы установить размер ОЗУ больше 32 Кбайт.

Симптом 10.25. Появляется ошибка вида "Для базового адреса ОЗУ F00000 или выше размер ОЗУ должен составлять 64 Кбайт"

Если базовый адрес ОЗУ приравнен к 0F00000 или выше (например, F20000h, F40000h, F60000h или F80000h), размер буфера ОЗУ должен составлять 64 Кбайт. Если базовый адрес ОЗУ приравнивается к F00000h или ниже, размер ОЗУ должен находиться в диапазоне от 16 до 64 Кбайт. Такие сообщения об ошибке система создает в том случае, если базовый адрес ОЗУ и настройки размера ОЗУ несовместимы. Необходимо либо отключить в системе кэширование ОЗУ, либо откорректировать некэшируемую область памяти.

Симптом 10.26. Появляется ошибка вида "Все каналы DMA не функционируют — нет возможности обнаружить другой канал"

DMA-каналы сетевого адаптера (т. е. каналы 1, 2 и 3) не прошли диагностическое тестирование. Проверьте правильность установки и настройки сетевого адаптера. Убедитесь в том, что в программе диагностического тестирования применяется соответствующее значение DMA-канала. Если все установки верны, то возможно, сетевой адаптер неисправен и требует замены.

Симптом 10.27. Появляется ошибка о сбое тестирования ASIC

Микросхема сетевого адаптера ASIC (специализированная интегральная схема, Application-Specific Integrated Circuit) не прошла диагностическое тестирование. Возможно, микросхема ASIC (или схема, применяемая для обращения к этой микросхеме) не функционирует. Проверьте правильность установки сетевого адаптера и микросхемы ASIC в гнезде. Если неисправность устранить не удалось, вероятно, сетевой адаптер неисправен и требует замены.

Симптом 10.28. Появляется ошибка "DMA-канал <x> поврежден — попробуйте использовать DMA-канал <y>"

Почти во всех случаях эта неисправность имеет отношение к конфигурации системы. DMA-канал <x> сетевого адаптера не прошел диагностическое тестирование, но при этом DMA-канал <y> оказался пригодным. Возможно, DMA-канал <x> (текущая настройка) применяется другой установленной в системе платой или устройством. Попробуйте установить в качестве DMA-канала платы DMA-канал <y>.

Симптом 10.29. Обнаруживается, что рабочие станции не могут подключиться к серверу NetWare

Проверьте, чтобы рабочая станция и сервер пользовались одним и тем же типом кадра. Добавьте в файл STARTUP.NCF сервера NetWare следующие две строки:

```
set minimum packet receive buffers=512
set maximum packet receive buffers=1024
```

Для сервера восстановления после отказа и сервера агрегирования NetWare убедитесь в том, что на каждой рабочей станции `IPX RETRY COUNT=255`.

Симптом 10.30. Во время установки драйвера NetWare появляются сообщения об ошибках

Вероятно, требуется обновление NetWare. Установите NetWare Service Pack 6 (IWSP6) или более позднюю версию, выберите спецификацию ODI 3.31, а затем установите драйвер сетевого адаптера. Зайдите на сайт Novell для получения обновлений (**www.novell.com**).

Симптом 10.31. Сервер NetWare возвращает ошибку "Обнаружена ошибка конфигурации маршрутизатора"

Практически во всех случаях появление такого сообщения обусловлено непоследовательностью в схеме сетевой нумерации. В каждом сегменте сети IPX для каждого типа кадра должен быть назначен уникальный внешний сетевой номер IPX. Этот сетевой номер должен оставаться неизменным для всех устройств (серверов, маршрутизаторов и т. д.), подключенных к этому сегменту и применяющих данный тип кадра. Не забывайте, что сегмент определяется как любой совместно используемый сетевой канал передачи информации, типа линии коаксиального кабеля, концентратора (нескольких концентраторов) или сочетания устройств, соединенных повторителем или коммутатором 2-го уровня.

Эта ошибка чаще всего происходит, когда один IPX привязан к двум различным сетевым адаптерам с одним типом кадра и в одном сегменте, но с разными внешними сетевыми номерами IPX. Внешние сетевые номера IPX присваиваются во время привязки IPX к логической плате; они должны быть уникальными для каждого сегмента (в отличие от внутреннего сетевого номера IPX, который назначается при запуске сервера и должен быть уникальным для каждого сервера). К примеру, предположим, что на сервере NetWare в сети на базе витой пары вы пользуетесь двумя PCI-адаптерами Intel EtherExpress PRO/10+, а в файле AUTOEXEC.NCF содержатся следующие данные:

```
LOAD E100B SLOT=13 FRAME=ETHERNET_802.2 NAME=CARD1
LOAD E100B SLOT=14 FRAME=ETHERNET_802.2 NAME=CARD2
BIND IPX TO CARD1 NET=1
BIND IPX TO CARD2 NET=2
```

Если каждый из двух сетевых адаптеров подключен к отдельному концентратору, их работа должна быть безошибочной. Впрочем, если соединить эти два концентратора с помощью витой пары (объединив их в единый "сегмент"), компьютер в ответ создаст сообщение об ошибке. Проверьте, нет ли в ваших сетевых соединениях петель, объединяющих разные сегменты. Проверьте конфигурацию всех устройств (серверов, маршрутизаторов, сетевых принтеров и т. д.), подключенных к возможно неисправному сегменту, и убедитесь в том, что их сетевой номер остается одним и тем же для данного типа кадра. Если неисправность устранить не удалось, посмотрите, нет ли в сети неисправного или неправильно функционирующего маршрутизатора.

Симптом 10.32. Сервер NetWare создает сообщение: "Буферы приема недостаточны. Установите максимальный размер буфера приема пакетов в файле STARTUP.NCF равным 1536"

Эта ошибка часто встречается при использовании сетевых адаптеров Intel в сочетании с драйверами локальной сети EtherExpress; как правило, она связана с неверной командной строкой в файле STARTUP.NCF. Проверьте, нет ли в этом файле такой командной строки

```
SET MAXIMUM PHYSICAL RECEIVE PACKET SIZE=2048
```

Этот параметр определяет объем памяти, который ваш сервер выделяет каждому буферу пакетов, но абсолютно не влияет на размер самих пакетов.

Симптом 10.33. Сервер NetWare сообщает, что "Загрузчик не может найти общедоступный символ *<имя символа>*"

Если сообщение об этой ошибке появляется во время загрузки драйвера сетевого адаптера, то, вероятно, оно указывает использование старого модуля NLM, что касается файлов MSM.NLM, NBI.NLM и ETHERTSM.NLM для адаптеров Ethernet или TOKENTSM.NLM — для адаптеров маркерного кольца. Установите на сервере NetWare новейшие средства поддержки сетевого режима. Кроме того, важно использовать на сервере последние версии заплат и служебных пакетов.

Симптом 10.34. Сервер NetWare сообщает, что "NetWare не поддерживает обращения к BIOS в защищенном режиме. В отсутствие заплаты загрузчика драйверы PCI могут дать сбой"

Эта ошибка может появиться при загрузке драйвера 3.3x ODI. Причина ее кроется либо в неверном применении последней заплаты (заплат), либо в использовании старых версий модулей NLM. Проверьте, есть ли на сервере NetWare модули NLM последней версии 3.3x и последние заплаты. Если самые последние заплаты уже установлены, убедитесь в правильности применения заплаты загрузчика с помощью утилиты LSWAP и в соответствии с инструкциями Novell.

Дополнительные ресурсы

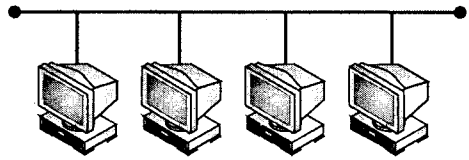
Adaptec: **www.adaptec.com**.

D-Link: **www.dlink.com**.

Linksys: **www.linksys.com**.

Netgear: **www.netgear.com**.

SMC: **www.smc.com**.



ГЛАВА 11

RAID-адаптеры и устранение неисправностей

Несмотря на то, что сети предназначены для обработки больших объемов ценных данных, их вряд ли можно признать безотказными. Сбои аппаратного обеспечения и несовместимость между программами, несомненно, способны помешать функционированию сети. Подобные помехи могут подвергнуть опасности передачу данных и защищенные операции и привести к многочисленным сбоям, которые будут препятствовать вашей повседневной деятельности. Применение метода отказоустойчивости — это попытка преодолеть сбои в работе сети. Одним из наиболее распространенных методов отказоустойчивости является RAID (Redundant Array of Independent Disks — избыточный массив независимых дисков)[1]. Технология RAID позволяет задействовать множество физических дисков и создать множество логических томов, которые могут воспроизводить диски или распределять данные между несколькими физическими дисками в целях повышения производительности. В этой главе будут рассмотрены важнейшие принципы систем RAID, изложены основные положения установки и конфигурирования RAID и представлены общие проблемы поиска и устранения неисправностей.

Примечание

Помните, что применение технологии RAID ограничено дисками IDE и SCSI — в зависимости от выбранного RAID-контроллера. На небольших бизнес-серверах в целях экономии зачастую используется IDE RAID, а на профессиональных, как правило, — SCSI RAID.

Введение в RAID

Массив дисков создается из группы (двух или более) физических дисков, которые воспринимаются системой как единый диск. Преимущество массива состоит в повышенной производительности и отказоустойчивости данных. Повышение производительности осуществляется путем разделения рабочей нагрузки по передаче данных одновременно между несколькими физическими дисками. Отказоустойчивость достигается с помощью операции по резервированию данных, благодаря которой при

[1] Обычно вместо слова Independent используется Inexpensive, т. е. недорогой. — *Ред.*

отказе (или сбое сектора) одного (или нескольких) дисков копию утраченных данных можно найти на других дисках. Для получения наилучших результатов формировать массивы дисков следует из идентичных дисков. Согласованная производительность (matched performance) дисков позволяет добиться более эффективной работы массива как единого диска. Отдельные диски в массиве называются ее участниками. Каждый участник массива дисков хранит в своем зарезервированном секторе идентифицирующую его конфигурационную информацию.

Логические диски

Логический диск — это пространство памяти, распределенное между множеством физических дисков массива (за исключением оперативных резервов). Подобное разделение пространства памяти обеспечивает некоторые значительные преимущества. К примеру, в таком случае возможен доступ к данным сразу на всех физических дисках, в результате чего заметно повышается производительность хранения и извлечения данных. Отказоустойчивые уровни RAID можно использовать для защиты данных от аппаратных сбоев. Наконец, массив может состоять из нескольких логических дисков, каждый из которых при этом охватывает множество физических дисков (для достижения максимальной эффективности использования пространства все физические диски в каждом массиве должны иметь одинаковые размеры).

Адаптер дискового массива (DAA)

Это общее обозначение *RAID-контроллера* — устройства (DAA, Disk Array Adapter), поддерживающего дисковый массив. Большинство RAID-контроллеров используют SCSI-интерфейс типа Adaptec SCSI RAID 3410S (рис. 11.1), но компания Promise Technologies предлагает FastTrack100 с поддержкой функций RAID для жестких дисков UDMA/66 и UDMA/100. Почти во всех случаях контроллер содержит систему BIOS, которая полностью поддерживает операции диска (SCSI или UDMA/100), и предусматривает возможность настройки (типа CMOS Setup), которая позволяет выполнять конфигурацию множества функций RAID-контроллера.

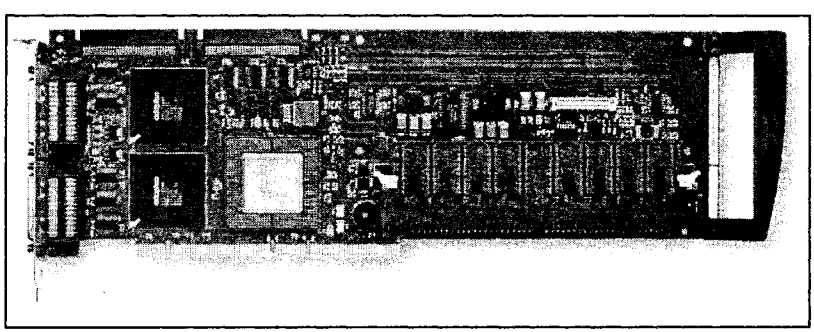


Рис. 11.1. RAID-контроллер Adaptec SCSI RAID 3410S (с разрешения Adaptec)

Типы адаптеров

Как правило, применяются два метода реализации RAID-контроллера: на базе хоста и SCSI-to-SCSI. Оба этих метода обеспечивают приемлемый уровень работы устрой-

ства, но он достигается посредством некоторых компромиссов, о которых вам следует знать.

Адаптер на базе хоста

Интеллект RAID-устройства на базе хоста (host-based) сосредоточен на плате адаптера, установленной на сетевом сервере. Так как при этом службы RAID реализованы аппаратно, RAID на основе хоста обеспечивает наилучшую производительность. К примеру, на сервере Gateway 7400 адаптер AMI MegaRAID Express Plus является частью файлового сервера, поэтому он может напрямую передавать данные по шине PCI компьютера со скоростью до 132 Мбит/с. Впрочем, будучи аппаратными устройствами, адаптеры на базе хоста должны предусматривать подходяшие драйверы для каждой операционной системы. Возможная скорость последовательной передачи данных определяется следующими факторами:

- поддерживаемая скорость передачи данных по шине PCI материнской платы;
- поддерживаемая скорость передачи данных по мосту PCI-PCI i960RP;
- поддерживаемая скорость передачи данных по SCSI-контроллеру;
- поддерживаемая скорость передачи данных в устройствах SCSI;
- количество каналов SCSI;
- количество дисков SCSI.

Адаптер на базе SCSI-to-SCSI

Интеллект RAID-контроллера на базе SCSI-to-SCSI сосредоточен в самом контроллере. Этот контроллер использует простой хост-адаптер SCSI, установленный на сетевом сервере. Это означает, что скорость передачи данных ограничивается пропускной способностью канала SCSI. К примеру, RAID-система SCSI-to-SCSI с двумя широкими каналами SCSI, которые работают на скорости до 80 Мбит/с, сжимает данные до одного широкого канала SCSI (40 Мбит/с), ведущего обратно на хост. Впрочем, реализация RAID SCSI-to-SCSI позволяет подсистеме жесткого диска применять лишь один идентификатор SCSI, а это дает возможность подключать множество подсистем дисков к одному контроллеру SCSI.

Адаптер на базе программной реализации (software-based)

Третий, редко используемый тип реализации RAID основывается на программном обеспечении. Таким дисковым массивом управляет не аппаратное, а программное обеспечение сервера. Это наименее удачный вариант RAID-контроллера, т. к. он увеличивает нагрузку на центральный процессор системы и требует подходящего для данной операционной системы управляющего программного обеспечения. Кроме того, функционирование RAID может прерваться в результате отказа системы, что приведет к искажению данных. В большинстве случаев, если это возможно, откажитесь от применения систем RAID на базе программной реализации.

Зарезервированный сектор (reserved sector)

Важнейшая информация хранится в специальной области каждого участника дискового массива, и эта область называется *зарезервированным сектором*. Этот сектор содержит данные конфигурации массива, связанные как с данным диском, так и

другими участниками дискового массива. Если данные, хранящиеся на одном из участников массива, подвергаются искажению или теряются, их автоматическое восстановление выполняется с использованием резервной конфигурационной информации, получаемой от других участников. Как правило, для каждого участника дискового массива не предусмотрено конкретное местоположение. Следовательно, диски можно размещать на различных коннекторах или платах RAID-контроллеров в пределах системы, при этом не выполняя реконфигурацию или восстановление массива.

Организация чередующегося диска

При организации *чередующегося диска* (disk striping) данные записываются на нескольких дисках вместо одного. Это подразумевает разделение пространства памяти каждого диска на слои, размер которых колеблется от 2 до 128 Кбайт. Слои многократно и последовательно чередуются. Общее пространство памяти состоит из слоев каждого диска. К примеру, в четырехдисковой системе, в которой организуется только чередующийся диск (как в RAID 0-го уровня), сегмент 1 записывается на диск 1, сегмент 2 — на диск 2, сегмент 3 — на диск 3 и т. д. Организация чередующегося диска повышает эффективность хранения, т. к. доступ к множеству дисков производится одновременно. Впрочем, это не предусматривает резервирование данных.

Размером слоя является длина чередующихся сегментов данных, которые RAID-контроллер записывает на множество дисков. RAID-контроллеры типа AMI MegaRAID Express Plus поддерживают слои размером в 2, 4, 8, 16, 32, 64 или 128 Кбайт. Под *шириной слоя* подразумевается количество дисков, задействованных в массиве с реализацией чередования. К примеру, в четырехдисковом массиве с чередованием ширина слоя составляет 4.

Организация составного диска

Организация составного диска (disk spanning, — "стягивание" дисков) позволяет нескольким дискам функционировать как один большой диск. Метод стягивания позволяет преодолеть недостаток дискового пространства и упрощает управление сохранением данных, используя существующие ресурсы или добавляя сравнительно недорогие. К примеру, четыре диска емкостью 400 Мбайт каждый можно объединить, и операционная система будет рассматривать их как один диск емкостью 1600 Мбайт. Стягивание само по себе не повышает надежность и производительность — оно лишь увеличивает возможности сохранения данных. Иногда стягивание называют JBOD (простой массив дисков, Just a Bunch Of Disks). Стянутые логические диски должны быть смежными и иметь одинаковый размер слоя. Ниже приводится несколько примеров реализации стягивания в типичных настройках RAID.

- Выполните конфигурацию массива RAID 10 путем стягивания двух смежных логических дисков RAID 1. Логические диски RAID 1 должны иметь одинаковый размер слоя.
- Выполните конфигурацию массива RAID 30 путем стягивания двух смежных логических дисков RAID 3. Логические диски RAID 3 должны иметь одинаковый размер слоя.

- Выполните конфигурацию массива RAID 50 путем стягивания двух смежных логических дисков RAID 5. Логические диски RAID 5 должны иметь одинаковый размер слоя.

Примечание

Стягивание двух смежных логических дисков RAID 0 не приводит к формированию нового уровня RAID и не обеспечивает отказоустойчивости. Тем не менее эта операция увеличивает размер логического тома и повышает производительность за счет удваивания числа шпинделей.

Зеркальное копирование дисков

При *зеркальном копировании* (disk mirroring) (применяемом в RAID 1) данные, записанные на один диск, одновременно сохраняются на другом диске. Если один из этих дисков выходит из строя, функционирование системы (и восстановление неисправного диска) обеспечивается содержимым второго диска. Основным преимуществом зеркального копирования дисков является 100%-ное резервирование данных. Так как содержимое первого диска полностью повторяется на втором, отказ одного из этих дисков не приводит к негативным последствиям. Оба диска всегда содержат одни и те же данные и в роли рабочего диска может выступать любой из них. Зеркальное копирование дисков обеспечивает 100%-ное резервирование, но эта методика является дорогостоящей, т. к. каждый диск в системе должен быть дублирован. К примеру, чтобы дублировать диск емкостью 10 Гбайт, вам потребуется второй диск аналогичной емкости.

Контроль по четности

Контроль по четности — это вид резервирования, при котором из двух или более порождающих наборов данных (parent data set) создается набор "данных резервирования". Впоследствии эти данные резервирования могут быть при необходимости использованы для восстановления одного из порождающих наборов данных. Данные четности, в отличие от зеркального копирования, не обеспечивают полного дублирования порождающих наборов данных. В технологии RAID этот метод применяется к целым дискам (или к слоям всех дисков массива). Есть два типа контроля по четности.

- Выделенный контроль по четности (dedicated parity). Информация о четности данных на двух или нескольких дисках хранится на дополнительном диске.
- Распределенный контроль по четности (distributed parity). Информация о четности данных распределяется по всем дискам в системе.

Четность обеспечивает резервирование на случай сбоя одного диска без полного дублирования содержимого всех дисков, но генерирование четности может замедлить процесс записи (и снизить эффективность массива). К примеру, если из строя выйдет один из дисков, его содержимое может быть восстановлено с помощью четности и данных на оставшихся дисках. В RAID 3 специализированный контроль по четности сочетается с чередованием дисков — диск четности в RAID 3 является последним логическим диском в наборе RAID. В RAID 5-го уровня чередование дисков сочетается с распределенным контролем по четности.

Горячие резервы (hot spares)

Горячим резервом называется дополнительный (неиспользуемый) диск, являющийся частью дисковой подсистемы. Как правило, он находится в режиме обхода, т. е. он готов к работе в случае выхода из строя другого диска. Горячие резервы позволяют заменять или восстанавливать неисправные диски, не прибегая к отключению системы или вмешательству со стороны пользователя. Многие RAID-контроллеры (такие как AMI MegaRAID Express Plus) предусматривают автоматическое и прозрачное восстановление с помощью дисков горячих резервов, обеспечивая предельную отказоустойчивость и отсутствие простоя. Назначение физических дисков в качестве горячих резервов производится с помощью управляющего программного обеспечения RAID. При необходимости RAID-контроллер назначает горячий резерв, емкость которого должна быть наиболее близка или равна емкости неисправного диска, который предполагается заменить. Впрочем, горячие резервы применяются только в массивах с резервированием (таких как RAID 1, 3, 5, 10, 30 и 50). Как правило, горячий резерв, подключенный к определенному RAID-контроллеру, можно использовать для восстановления лишь того диска, который подсоединен к тому же контроллеру.

Восстановление диска

RAID-контроллер может восстановить диск путем воссоздания данных, которые хранились на этом диске до того, как он вышел из строя. Резервное восстановление (теплый резерв) применяется в системе с зеркальным копированием (RAID 1). Если диск выходит из строя, незамедлительно активируется диск, идентичный неисправному. В роли исходного диска выступает диск, являющийся первичным источником данных. В системах RAID 1, 3, 5, 10, 30 или 50 для восстановления дисков может использоваться горячий резерв. Если горячий резерв недоступен, неисправный диск следует заменить новым, чтобы можно было восстановить данные на неисправном диске. Если горячий резерв активирован, то при сбое диска его восстановление начинается автоматически. Если в процессе восстановления система прекращает работу, RAID-контроллер автоматически перезапускает ее и возобновляет восстановление.

Примечание

Возобновление возможно лишь в массивах с резервированием данных — таких как RAID 1, 3, 5, 10, 30 и 50.

RAID-контроллер восстанавливает неисправные диски автоматически и незаметно, причем скорость восстановления определяется пользователем.

Скоростью восстановления называется часть мощности (циклов) центрального процессора, выделенная на восстановление неисправных дисков. При 100%-ной скорости восстановления система занимается только восстановлением вышедшего из строя диска. Многие RAID-контроллеры предусматривают диапазон скорости восстановления от 0 до 100%. Если скорость восстановления равна 0%, это означает, что восстановление производится лишь тогда, когда система не занята ничем другим

(простаивает). При скорости восстановления 100% процесс восстановления имеет высший приоритет в системе.

Уровни RAID

Методики типа расслоения, зеркального копирования и стягивания способствуют повышению пропускной способности данных, увеличению емкости и достижению резервирования данных. В большинстве случаев они применяются в разных сочетаниях, что еще больше расширяет возможности их применения. Некоторое представление об этих методиках вы получили ранее, а теперь самое время ознакомиться с уровнями RAID более подробно. В табл. 11.1 приводится сравнение основных уровней RAID.

Примечание

Не забывайте, что все диски-участники созданного дискового массива, в основном, воспринимаются центральной системой как единый логический диск Тем не менее массив можно разбить на несколько логических дисков.

Таблица 11.1. *Сравнение уровней RAID*

Уровень	Описание и применение	Преимущества	Недостатки	Максимальное количество дисков	Отказоустойчивость
0	Данные разделяются на блоки и распределяются последовательно (чистое чередование). Применяется для обычных данных, требующих высокой производительности	Высокая пропускная способность при передаче крупных файлов	Отсутствие отказоустойчивости. При сбое любого диска все данные будут потеряны	От 1 до 32	Нет
1	Данные дублируются на другом диске (зеркальное копирование). Применяется в отказоустойчивых системах с интенсивным считыванием	100%-ное резервирование данных	Удваивает дисковое пространство. При восстановлении данных общая производительность снижена	2, 4, 6 или 8	Да
3	Чередование дисков со специализированным диском четности. Применяется для неинтерактивных приложений, последовательно обрабатывающих крупные файлы	Резервирование достигается минимальными затратами	Хуже, чем RAID 1	От 3 до 8	Да

Таблица 11.1 (окончание)

Уровень	Описание и применение	Преимущества	Недостатки	Максимальное количество дисков	Отказоустойчивость
5	Чередование дисков и четности на всех дисках. Применяется при больших объемах считывания, но незначительных объемах записи, например, для обработки транзакций	Резервирование достигается минимальными затратами	Хуже, чем RAID 1	От 3 до 8	Да
10	Чередование данных и зеркальное копирование дисков	Интенсивная передача данных, полное резервирование	Более сложный	4, 6 или 8	Да
30	Чередование дисков со специализированным диском четности	Интенсивная передача данных, резервирование	Более сложный	От 6 до 32	Да
50	Чередование дисков и данные четности на всех дисках	Интенсивная передача данных, резервирование	Более сложный	От 6 до 32	Да

RAID 0 (только чередование)

RAID 0 предусматривает чередование на всех дисках (которых может быть от 1 до 32) в подсистеме RAID. RAID 0 обеспечивает наилучшую производительность по сравнению с другими уровнями RAID, но не поддерживает резервирование данных — отказ любого расслоенного диска приводит к искажению всего дискового массива. RAID 0 разбивает данные на небольшие блоки, а затем записывает по блоку на каждый диск массива. Размер каждого блока определяется параметром размера слоя (который устанавливается во время создания набора RAID). RAID 0 обеспечивает высокую пропускную способность. Разбивая крупный файл на более мелкие блоки, RAID-контроллер может использовать несколько дисков для увеличения скорости считывания и записи файла. В RAID 0 не предусмотрены вычисления, связанные с четностью, а следовательно, операции записи не усложняются. Поэтому RAID 0 идеален для приложений, которым необходима высокая пропускная способность, но не требуется отказоустойчивость.

RAID 1 (только зеркальное копирование)

При использовании этого метода дублируемые данные записываются на два диска, а операции считывания выполняются параллельно (что повышает их эффективность). RAID 1 характеризуется отказоустойчивостью, т. к. данные дублируются, а диски из дублирующей пары устанавливаются на разных коннекторах. RAID-контроллер вы-

полняет операции считывания с помощью методов обработки данных, которые распределяют рабочую нагрузку эффективнее, чем при использовании одного диска. При получении запроса на считывание контроллер выбирает диск, расположенный ближе всего к запрашиваемым данным, а затем ищет незанятый диск, который будет выполнять следующий доступ для чтения.

Если один из дублируемых дисков получает механическое повреждение (например, повреждение шпинделя) или не отвечает, оставшийся в паре диск продолжает работу (это и есть отказоустойчивость). Если на одном диске появляется физическая ошибка сектора, диск с дублированными данными также продолжит работу. При следующей перезагрузке программная утилита RAID отобразит ошибку в массиве и порекомендует заменить неисправный диск. При этом пользователь может продолжить работу на компьютере, но лучше всего заменить поврежденный диск как можно скорее. Обычно RAID 1 поддерживает 2, 4, 6 или 8 дисков.

Благодаря резервированию емкость дискового массива составляет половину от общей емкости всех входящих в него дисков. К примеру, два диска емкостью 1 Гбайт каждый, общая емкость которых составляет 2 Гбайт, вместе имеют лишь 1 Гбайт полезной памяти. Если в массив входят диски разной емкости, то на диске большей емкости часть ее может остаться неиспользованной. В целях повышения производительности в конфигурациях, состоящих более чем из двух дисков, данные по ним расслаиваются (это также называется RAID 1+0 или RAID 10).

Примечание

Если из строя выйдут оба диска, участвующих в зеркальном копировании, том также выйдет из строя и возможна потеря данных.

RAID 0+1 (чередование/зеркальное копирование)

Это сочетание типов массивов, описанных выше, повышает производительность за счет параллельного считывания и записи данных и защиты данных с помощью резервирования. В данном случае установить нужно не менее четырех дисков. В дисковом массиве, состоящем из четырех дисков, две пары дисков расслаиваются, причем каждая из них выполняет зеркальное копирование данных на другую пару расслоенных дисков. Емкость такого массива аналогична емкости массива с зеркальным копированием, где половина общей емкости выделяется под резервирование.

RAID 1+0 или "10" (чередование/зеркальное копирование)

Это еще одно сочетание зеркального копирования (RAID 1) и расслоения (RAID 0). Как и в случае с RAID 0+1, такое сочетание повышает производительность за счет параллельного считывания и записи данных и их защиты путем резервирования. Необходимо наличие как минимум четырех дисков. Но в дисковом массиве, состоящем из четырех дисков, расслоению подвергается лишь одна пара дисков, а другая пара выполняет зеркальное копирование данных. Это обеспечивает отказоустойчивость типа RAID 1, а посредством расслоения этих элементов RAID 1 достигаются высокие скорости ввода/вывода. Конфигурация этого типа наиболее часто используется на серверах баз данных, где крайне важны высокая производительность и отказоустойчивость. Не следует путать RAID 0+1 с RAID 1+0.

RAID 2 (чередование с кодом ECC)

При записи блока данных производится разбивка и распределение данных по всем дискам *(см. разд. "RAID 0")*, а также проверка данных на наличие ошибок. Проверка и исправление ошибок требует больше дискового пространства, чем контроль по четности, но код ECC лучше защищает данные, чем контроль по четности.

RAID 3 (чередование с контролем по четности)

RAID 3 поддерживает чередование дисков и полное резервирование данных с помощью специализированного диска четности. При использовании RAID 3 размер слоя должен составлять 64 Кбайт. RAID 3 обрабатывает данные на уровне блоков (в отличие от RAID 5, где обработка происходит на байтовом уровне), поэтому использование RAID 3 идеально для сетей, в которых часто обрабатываются очень крупные файлы, типа графических изображений. Впрочем, дополнительный ввод/вывод, необходимый для контроля по четности, во время случайных операций ввода/вывода может стать причиной сбоя. RAID 3 разбивает данные на мелкие блоки, вычисляет их четность, а затем записывает их на все диски массива, кроме одного. Данные четности, созданные во время операций записи, сохраняются на последнем диске массива (это называется специализированным контролем по четности). Размер каждого блока определяется параметром размера слоя, который устанавливается во время создания набора RAID.

Если один из дисков выходит из строя, массив RAID 3 продолжает работать в "неполном режиме". Если неисправный диск — это диск с данными, операции записи продолжатся в нормальном режиме, но запись на поврежденный диск осуществляться не будет. Операции считывания восстанавливают данные на неисправном диске путем проверки оставшихся данных слоя и контроля по четности для этого слоя. Если поврежденный диск — это диск четности, операции записи будут проводиться в нормальном режиме, но сохранение данных четности осуществляться не будет. При операциях считывания данные будут по-прежнему считываться с дисков. RAID 3 поддерживает от трех до восьми дисков.

На практике вы, возможно, обнаружите, что использование RAID 5 более предпочтительно, чем RAID 3, даже в отношении приложений с последовательными операциями считывания и записи, т. к. большинство RAID-контроллеров имеют очень мощные алгоритмы кэширования. Преимущества RAID 3 исчезают при наличии множества небольших операций ввода/вывода, произвольно и широко распределенных по дискам логического диска. В таких приложениях фиксированный диск четности RAID 3 становится узким местом. К примеру, хост пытается выполнить две небольших операции записи, в которых задействуются два различных слоя и разные диски. В идеале, обе операции должны выполняться одновременно. Но в RAID 3 это невозможно, т. к. доступ к фиксированному диску четности операции должны получать поочередно. По этой причине в подобных ситуациях предпочтение RAID 5 очевидно.

RAID 3+0 или "30"

RAID 30 — это сочетание RAID 0 и RAID 3, которое обеспечивает высокие скорости передачи данных и их надежность. Лучше всего RAID 30 реализуется на двух дисковых массивах RAID 3, когда данные по ним расслоены. RAID 30 разбивает

данные на небольшие блоки, а затем расслаивает их по каждому набору RAID 3. RAID 3 разбивает данные на еще более мелкие блоки, вычисляет их четность, а затем записывает блоки данных на все диски массива, кроме одного. Данные четности, созданные во время операций записи, сохраняются на последнем диске массива RAID 3. Размер каждого блока определяется параметром размера слоя, который устанавливается во время создания набора RAID.

RAID 30 следует применять для последовательно записываемых и считываемых данных, операций допечатной подготовки, а также операции видео по требованию, которая требует повышенной отказоустойчивости и емкости выше средней. Этот уровень RAID обеспечивает надежность данных и высокие скорости их передачи, он выдерживает повреждение от одного до четырех дисков, при этом сохраняя целостность данных (если все вышедшие из строя диски расположены в разных массивах RAID 3). К сожалению, реализация RAID 30 обходится дорого, т. к. этот уровень требует в 2—4 раза больше дисков, чем RAID 3, и поддерживает от 6 до 32 дисков.

RAID 4 (защита данных)

Защита данных (RAID 4) обеспечивает надежность данных при использовании небольшой емкости памяти логического диска. Отдельный назначенный диск содержит данные четности. Если диск выходит из строя, для восстановления его данных контроллер использует данные на диске четности, а также данные на остальных дисках. Это позволяет системе продолжать работу при незначительной потере производительности до тех пор, пока вы не замените поврежденный диск. Защита данных требует наличия как минимум трех дисков (двух дисков с данными и одного диска четности) в одном массиве, а максимальное количество дисков определяется возможностями сервера. К примеру, в массиве, содержащем три физических диска, защита данных использует только 33% общей емкости логического диска для достижения отказоустойчивости. Для сравнения, в 18-дисковой конфигурации (17 дисков с данными и один диск четности) для этого выделяется лишь 6% общей емкости.

Примечание

Учитывая надежность современных технологий жестких дисков, вероятность неисправности дискового массива повышается с увеличением количества дисков в массиве.

RAID 5 (чередование с контролем по четности)

RAID 5 предусматривает чередование дисков на байтовом уровне, а также контроль по четности, причем данные четности фиксируются на нескольких дисках (это также называется распределенным контролем по четности, а иногда — распределенной защитой данных). RAID 5 лучше всего подходит для сетей, в которых одновременно происходит множество небольших транзакций ввода/вывода. RAID 5 решает проблему узких мест при выполнении случайных операций ввода/вывода. Так как каждый диск содержит как данные, так и информацию четности, одновременно может происходить несколько операций записи. Кроме того, мощные алгоритмы кэширования и поддержка аппаратного обеспечения обуславливают необычайно высокую производительность RAID 5 в различных средах. Как правило, на уровне RAID 5 применяется от трех до восьми дисков.

RAID 5 обеспечивает высокую пропускную способность (особенно в отношении крупных файлов), поэтому мы рекомендуем использовать этот уровень для приложений, обрабатывающих транзакции — операции считывания и записи выполняются при этом независимо на каждом диске. Если диск выходит из строя, для воссоздания недостающей информации RAID-контроллер использует диск четности. RAID 5 также является хорошим решением для офиса или интерактивной службы, где требуется отказоустойчивость, а также для любого приложения с высокой интенсивностью запросов на считывание и низкой интенсивностью запросов на запись. Однако в процессе восстановления диска производительность падает. Если в среде одновременно выполняется несколько процессов, то высокой производительности в этом случае добиться не удается, т. к. падение производительности при восстановлении дисков не компенсируется одновременным выполнением нескольких процессов.

RAID 5+0 или "50"

RAID 50 сочетает функции RAID 0 и RAID 5. Этот уровень поддерживает контроль по четности и чередование на множестве дисков. RAID 50 лучше всего реализуется на двух дисковых массивах RAID 5 с чередованием данных на обоих массивах. RAID 50 разбивает данные на небольшие блоки, а затем расслаивает их по каждому набору RAID 5. RAID 5 разбивает данные на еще меньшие блоки, вычисляет их четность, а затем записывает на каждый диск массива блоки данных и информацию о четности. Размер каждого блока определяется параметром размера слоя, который устанавливается в ходе создания набора RAID.

Лучше всего использовать RAID 50, если требуется высокая надежность данных, скорость запросов, уровень передачи данных и емкость выше средней. RAID 50 способен выдержать отказ от одного до четырех дисков, при этом сохраняя целостность данных (при условии, что все поврежденные диски располагаются в разных массивах RAID 5). Впрочем, применение RAID 50 сопряжено с высокими расходами, т. к. для реализации этого уровня требуется в 2—4 раза больше дисков, чем для RAID 5.

Ускоритель массива (Array accelerator)

В современном мире быстрой передачи данных и высокоскоростных жестких дисков обращение к диску и перемещение данных может занимать миллисекунды. Для современных компьютеров это слишком долго, не говоря уже об интенсивно загруженных сетях. В некоторых RAID-контроллерах (типа Compaq SmartArray 4250ES) предусмотрена функция ускорителя массива, которая может кэшировать операции записи и считывания в массиве RAID. Кэширование повышает "явную" производительность команд считывания и записи и уменьшает приостановки системы, которые зачастую случаются при ожидании окончания доступа к диску.

Ускоритель массива RAID позволяет RAID-контроллеру записывать данные в его кэш-память (ОЗУ), а не напрямую на диски. Сервер обращается к кэш-памяти RAID-контроллера в 100 раз быстрее, чем к диску. После того как данные записаны в кэш ускорителя массива, RAID-контроллер перепишет эти данные в дисковый массив позже, когда у него не будет других задач. Кроме того, RAID-контроллер использует ускоритель массива для повышения производительности во время считывания с диска, когда он упреждает запросы на считывание. Ожидаемые данные передаются ускорителю массива и ожидают своего запроса на считывание. Когда

RAID-контроллер получает запрос на считывание кэшированных данных, он может незамедлительно переместить их в системную память (ОЗУ) со скоростью шины PCI.

Так как ускоритель массива использует ОЗУ как кэш, содержимое ОЗУ необходимо защитить на случай, если произойдет отключение питания системы. Резервное питание от аккумулятора и память ECC гарантируют надежность кэша. Это дает техническим специалистам по обслуживанию серверов некоторые замечательные преимущества. Методика ECC может исправлять однобитовые ошибки, так что потерянные биты можно восстановить в реальном времени и без вмешательства в работу системы. Запасные аккумуляторы способны сохранять данные в ускорителе массива в течение нескольких дней. Когда энергоснабжение системы восстанавливается, в процессе инициализации сохраненные данные записываются на диски. Аккумуляторы, как правило, заряжаются путем непрерывной подзарядки малым током, когда электропитание системы исправно. Если кэшированные данные хранились в ускорителе массива, а затем произошло отключение электропитания, вы должны восстановить электропитание ускорителя до того, как аккумуляторы разрядятся; в противном случае все данные будут потеряны. Так как модуль ускорителя массива часто является съемным, плату ускорителя можно переставить с одного совместимого RAID-контроллера на другой. Это очень полезный прием, если RAID-контроллер выйдет из строя до того, как кэшированные данные ускорителя можно будет записать на диск.

Примечание

Если вы будете устанавливать RAID-контроллер с ускорителем массива, питание которого обеспечивается аккумулятором, вполне возможно, что при установке контроллера аккумулятор будет разряжен. На полную зарядку аккумуляторов и обеспечение поддержки ускорителя массива системе может потребоваться до 36 часов. При низком заряде аккумулятора во время загрузки RAID-контроллер сообщит об ошибке, а ускоритель массива будет заблокирован вплоть до полной зарядки аккумуляторов.

Изменение емкости массива

Емкость массива можно изменить путем ее расширения или наращивания. Между этими понятиями есть тонкие различия, которые вам следует понимать. *Наращивание емкости* (capacity expansion) подразумевает увеличение размера массива путем добавления физических дисков и создания дополнительных логических дисков. А *расширение емкости* (capacity extension) означает увеличение размера массива с помощью добавления физических дисков и расширения существующих логических дисков без создания новых логических дисков. В любом случае на сервер необходимо установить дополнительные жесткие диски. Емкость можно регулировать с помощью конфигурационной утилиты RAID-контроллера. RAID-контроллер выполняет перераспределение данных с исходного логического диска на логический диск, который охватывает все физические диски массива (включая добавленные диски). Затем оставшееся пространство применяется для увеличения размера логического диска (расширение) или создания дополнительных логических дисков, которые будут также распространяться на физические диски (наращивание). Логический диск измененного размера (расширенный диск) находится в более крупном дисковом массиве. При добавлении новых логических дисков (наращивании) они впоследст-

вии включаются в более крупный дисковый массив. Изменение емкости существующего логического диска может производиться автономно путем резервирования всех данных, реконфигурирования массива и, наконец, восстановления данных. Для изменения емкости диска в онлайновом режиме (при работающем сервере) ваша операционная система обязательно должна поддерживать увеличение размера логического диска.

Примечание

Конфигурационная утилита RAID-контроллера, как правило, позволяет увеличивать размер существующих логических дисков в условиях любой операционной системы. Тем не менее лишь Windows NT 4.0 и OS/2 позволяют изменять размер сегмента на расширенном логическом диске с помощью средств сторонних разработчиков, например, Partition Magic 3.0 или более поздней версии этого продукта (**www.powerquest.com**).

Пример

Рассмотрим один пример. Предположим, что в вашем дисковом массиве 14 дисков, а вы хотите нарастить его до 18. Просто установите в свободные отсеки четыре подходящих диска. Запустите утилиту конфигурации RAID-контроллера. Во время ее работы RAID-контроллер перераспределяет данные в равном количестве на все диски; при этом используется тот же самый метод отказоустойчивости (уровень RAID), что и в исходной конфигурации. Первый логический диск остается первым, но теперь вместо 14 дисков он вмещает 18. Кроме того, утилита конфигурации выявляет на каждом диске неиспользуемое пространство (т. к. каждый диск теперь содержит 14/18 тех данных, которые на нем были до увеличения общей емкости) и по вашему желанию помогает превратить это неиспользованное дисковое пространство во второй логический диск. У этого нового логического диска тоже есть отказоустойчивость, распределенная по неиспользованному пространству всех дисков. Когда этот процесс завершается, оба логических диска (один содержит исходные данные, а второй не содержит ничего) можно превратить в единый массив, емкость которого будет превышать емкость исходного массива.

При изменении размера дискового массива необходимо иметь в виду несколько важных моментов. Во-первых, размер всех логических дисков в массиве не обязательно должен быть одинаковым; более того, конфигурация отказоустойчивости дисков (уровни RAID) также может быть разной. Каждый логический диск рассматривается как автономный объект (независимо от того, сколько физических дисков он задействует) и может быть настроен так, как вам нужно. Кроме того, помните, что все физические диски в массиве должны иметь одинаковую емкость. Так как каждый диск содержит равную часть одного или нескольких логических дисков, общий размер всех частей должен соответствовать размеру наименьшего диска. Вы, конечно, можете установить диски большей емкости, но их дополнительное пространство будет невозможно использовать. Наконец, при наращивании массива, который изначально состоит из двух или нескольких логических дисков, перераспределение данных осуществляется сначала на одном из них, а затем на другом. Любой новый логический диск становится доступным после завершения наращивания емкости. В средах Windows NT и NetWare новый логический диск впоследствии можно присоединить к существующему логическому тому.

В некоторых случаях RAID-контроллер и его утилита настройки позволяют изменять емкость памяти в оперативном режиме без отключения сервера при использовании операционной системы Windows NT или NetWare (за исключением NetWare 3.11) в сочетании с диском с горячим подключением. Диски с горячим подключением необходимы для внесения оперативных изменений памяти, потому что обычные диски (без горячего подключения) требуют отключения сервера перед их извлечением или установкой. Для использования дисков с горячим подключением ваш сервер (например, Compaq ProLiant или Gateway 7400) должен поддерживать эти устройства.

Применение жестких дисков большей емкости

Дополнительное пространство памяти в рамках отказоустойчивой конфигурации можно получить путем систематической замены существующих дисков дисками большей емкости без увеличения их количества. При поочередной замене дисков данные на новом диске воссоздаются на основе резервной информации на оставшихся дисках. После восстановления одного нового диска можно производить замену следующего. После замены и восстановления всех дисков можно использовать дополнительную емкость каждого диска. Для этого нужно увеличить (расширить дисковый массив) существующий логический диск или добавить новый логический диск (нарастить дисковый массив). Утилита настройки RAID-контроллера автоматически определяет неиспользуемое пространство и помогает вам выполнить процедуры, необходимые для его применения.

Функции аварийного управления контроллером

В зависимости от уровня RAID ваш сервер может поддерживать ускоренный доступ к данным и отказоустойчивость (а часто обе эти функции одновременно). Дело в том, что обычно допускается лишь возникновение неисправностей жестких дисков, а RAID-контроллер как источник системных сбоев не рассматривается. Сегодня RAID-контроллеры обладают уровнем интеллекта и возможностями, которые позволяют выявить и исправить ошибки в дисковом массиве, а также на самом контроллере. В этом разделе рассматриваются некоторые функции аварийного управления, присутствующие в большинстве RAID-контроллеров SCSI и поддерживаемые сетевыми операционными системами.

Резервные контроллеры

Часто при настройке RAID слабым звеном являются контроллеры. Поэтому современные серверы поддерживают использование резервного контроллера. Один контроллер является первичным, а другой работает в активном режиме ожидания. При выходе из строя первичного контроллера активный резервный контроллер немедленно берет на себя управление дисковым массивом, при этом не происходит ни потери данных, ни сбоя в работе сервера. К примеру, RAID-контроллеры SCSI Compaq SmartArray 4250ES поддерживают такой режим, если они установлены на серверах с 64-битовой шиной PCI и расширенными коннекторами SCSI. Шины SCSI проводятся к обоим расширенным коннекторам SCSI, поэтому каждый из двух контроллеров получает возможность производить операции считывания и записи в дисковом массиве. Другой канал SCSI проводится между двумя коннекторами, в результате чего организуется линия между контроллерами, по которой они отслеживают состояние друг друга и поддерживают целостность кэшей. Контроллеры обме-

ниваются друг с другом данными о своем состоянии. Если один из контроллеров выходит из строя (что маловероятно), другой контроллер оповещает об этом операционную систему. Если первичный контроллер не отвечает, управление дисковым массивом переходит к вторичному контроллеру. Если не отвечает вторичный контроллер, первичный контроллер просто оповестит операционную систему о невозможности дальнейшего резервирования.

Автоматический мониторинг надежности

Автоматический мониторинг надежности (ARM, Automatic Reliability Monitoring) — это фоновый процесс, который ищет поврежденные секторы на жестких дисках, входящих в отказоустойчивые логические диски. Автоматический мониторинг надежности проверяет согласованность данных четности на дисках с защитой данных или распределенной защитой данных. Этот стандартный процесс гарантирует успешное восстановление данных в случае выхода из строя диска. Он работает только на уровнях RAID 1, 4 и 5.

Динамическое исправление сектора

Естественно, возраст и степень использования влияют на целостность секторов диска. RAID-контроллер, поддерживающий динамическое исправление сектора (DSR, Dynamic Sector Repairing) по требованию, способен автоматически восстанавливать любые поврежденные секторы, выявляемые либо в ходе нормальной эксплуатации, либо во время автоматического мониторинга надежности.

Отслеживание параметров диска

Отслеживание параметров диска (или отслеживание производительности диска) позволяет осуществлять мониторинг различных параметров диска и его функциональных тестов. Параметры мониторинга для RAID-контроллеров типа Compaq Smart Array 4250ES включают "ошибки чтения/записи/поиска", "время разгона", "неисправности кабеля" и функциональные тесты типа "время поиска дорожки". Отслеживание параметров диска позволяет RAID-контроллеру выявлять неисправности диска и прогнозировать его выход из строя.

Временное восстановление данных

Если в отказоустойчивой конфигурации RAID 1 (или выше) диск выходит из строя, система продолжает работать в режиме *временного восстановления данных*. К примеру, если логический диск сформирован на основе RAID 5 с использованием четырех физических дисков, и один из них выходит из строя, то система продолжает обрабатывать запросы ввода/вывода, но на более низком уровне производительности. Чтобы восстановить производительность и полную отказоустойчивость данного логического диска, необходимо как можно скорее заменить неисправный диск.

Автоматическое восстановление данных

После замены неисправного диска процесс *автоматического восстановления данных* восстановит все утраченные данные и запишет их на новый диск. Эта функция обеспечивает быстрый возврат к рабочей производительности без приостановки нормальной работы системы. Как правило, для восстановления 1 Гбайт данных тре-

буется примерно 15 минут. Но фактическое время, необходимое для восстановления, зависит от приоритета восстановления по отношению к тому объему операций ввода/вывода, который выполняется во время восстановления, а также от скорости диска и количества дисков в массиве (RAID 4 и RAID 5). К примеру, в конфигурациях RAID 4 и RAID 5 время восстановления может составлять от 10 минут на 1 Гбайт данных для трех дисков до 20 минут на 1 Гбайт для 18 дисков (при использовании жестких дисков SCSI Ultra Wide емкостью 9 Гбайт).

Примечание

Чтобы активизировать функции восстановления, в утилите настройки RAID-контроллера необходимо определить уровень RAID 5, 4 или 1.

Диски с горячим подключением

Установка и извлечение дисков с горячим подключением может производиться без отключения электропитания системы. Это значительно увеличивает скорость технического обслуживания, т. к. систему не нужно выключать, открывать, обслуживать, а затем снова подключать к источнику питания. Данная функция работает независимо от сетевой операционной системы и требует применения RAID-контроллера и корпуса сервера с поддержкой дисков с горячим подключением.

Примечание

Ни в коем случае не отключайте сервер с возможностью горячего подключения во время извлечения или установки съемных сменных дисков. Если при включенном питании сервера отключить запоминающую подсистему, RAID-контроллер отметит все диски как "неисправные", что может привести к потере данных без возможности их восстановления при включении запоминающей системы.

Дублирование контроллеров

Некоторые операционные системы поддерживают *дублирование контроллеров* — функцию обеспечения отказоустойчивости, для применения которой необходимо наличие двух RAID-контроллеров. При дублировании каждый из двух контроллеров имеет собственные диски, на которых содержатся идентичные данные. В случае отказа одного RAID-контроллера (что маловероятно) оставшиеся диски и второй RAID-контроллер продолжат обслуживание запросов.

Примечание

Так как оба RAID-контроллера подключаются к одинаковым шинам SCSI, дублирование контроллеров является функцией операционной системы, поддержка которой обеспечивается не всеми моделями RAID-контроллеров. Например, RAID-контроллер Compaq SmartArray 4250ES не поддерживает дублирование контроллеров.

Программное зеркальное копирование диска

Некоторые операционные системы поддерживают программное зеркальное копирование диска как функцию обеспечения отказоустойчивости. Программное зеркальное копирование диска аналогично аппаратному зеркальному копированию диска (RAID 1), их различие состоит в том, что в первом случае операционная система

копирует не физические, а логические диски. Программное зеркальное копирование имеет один недостаток — операционная система рассматривает каждый логический диск как отдельный физический диск. Если вы осуществляете зеркальное копирование логических дисков в одном массиве и при этом физический диск выйдет из строя, то оба логических диска также выйдут из строя, и извлечь данные вам не удастся. Если вы хотите воспользоваться зеркальным копированием диска, создайте по меньшей мере две массива уровня RAID 0, чтобы обеспечить максимальную емкость памяти. При настройке зеркального копирования диска с помощью операционной системы копировать следует те логические диски, которые находятся в разных массивах.

Установка и настройка RAID-контроллера

Для того чтобы воспользоваться возможностями RAID-контроллера, сначала его нужно установить на сервере. В этой части главы рассматривается общий процесс установки и настройки платы RAID-контроллера SCSI на сервере с поддержкой горячего подключения по шине PCI и без него. При установке второго RAID-контроллера (например, AMI MegRAID Express Plus или Compaq SmartArray 4250ES) в целях его резервирования необходимо убедиться в том, что на обоих контроллерах установлена последняя версия микропрограммного обеспечения, а в системе установлена последняя версия BIOS. Версии микропрограммного обеспечения на обоих контроллерах должны совпадать. Перед установкой выполните перечисленные ниже действия.

Примечание

Если ваш RAID-контроллер рассчитан на 64-битовые слоты PCI с расширенными коннекторами SCSI, установку нужно проводить только в эти слоты. Если установить контроллер в слоты без коннекторов этого типа, система будет работать некорректно.

1. Всегда начинайте с резервирования данных любого жесткого диска, который планируется переместить на новый контроллер.
2. Обновите существующее микропрограммное обеспечение контроллера и BIOS.
3. Снимите заглушки на коннекторы шин PCI и SCSI (например, 64-битовой шины PCI с расширенными SCSI-коннекторами).
4. При необходимости установите на сервер дополнительные отсеки для дисков.
5. Подсоедините 68-контактные Wide SCSI кабели устанавливаемого RAID-контроллера SCSI к соответствующим отсекам дисков.
6. Подключите к дискам порты (порт 1 SCSI к отсеку диска 1, порт 2 — к отсеку диска 2 и т. д.)
7. Установите диски в отсеки.

Если ваш сервер поддерживает горячее подключение, то для установки RAID-контроллера отключать питание сервера не потребуется.

1. Откройте и разблокируйте панель доступа горячего подключения.
2. С помощью кнопки отключения питания горячего разъема PCI (или специальной программы) отключите питание слота. В процессе отключения электропитания зеленый светодиод будет мигать, а после полного отключения он погаснет.

3. Сверху нажмите на рычаг, открывающий слот расширения, и поверните его. Проверьте, правильно ли вы выбрали слот расширения.
4. Установите плату RAID-контроллера в слот расширения в соответствии с направляющими.
5. Вставьте плату RAID-контроллера так, чтобы она находилась непосредственно над слотом.
6. Зафиксируйте плату RAID-контроллера, опустив рычаги.
7. Закрепите плату с помощью рычага на слоте. Убедитесь в том, что рычаг зафиксирован в закрытом положении.
8. С помощью программы горячего подключения PCI (или нажав кнопку отключения питания горячего разъема PCI на соответствующем слоте PCI) возобновите подачу электропитания к слоту.
9. Проверьте состояние слота по сигналу светодиода: мигающий зеленый означает переход к нормальному электропитанию, а постоянно горящий зеленый — установление нормального режима электропитания.
10. Закройте и заблокируйте панели доступа горячего подключения на сервере.
11. Чтобы настроить RAID-контроллер, запустите утилиты настройки сервера и RAID-контроллера.

Примечание

Убедитесь в том, что в операционной системе установлены необходимые драйверы горячего подключения. Иначе при извлечении или установке контроллера работа системы будет приостановлена

Если ваш сервер не поддерживает режим горячего подключения, то перед установкой RAID-контроллера вам придется отключить питание системы (и подождать, пока внутренние устройства охладятся).

1. Сделайте копию данных с жестких дисков, которые предполагается переместить на новый контроллер.
2. Отключите электропитание сервера и отсоедините шнуры питания.
3. Снимите заглушки с коннекторов шин PCI и SCSI (т. е. 64-битовой шины PCI с расширенными SCSI-коннекторами).
4. Установите плату RAID-контроллера в слот расширения в соответствии с направляющими.
5. Вставьте плату RAID-контроллера так, чтобы она находилась непосредственно над слотом.
6. Зафиксируйте плату RAID-контроллера, опустив рычаги.
7. Закрепите плату с помощью рычага на слоте. Убедитесь в том, что рычаг зафиксирован в закрытом положении.
8. Закройте и заблокируйте панели доступа горячего подключения на сервере.
9. Включите электропитание сервера.
10. Чтобы настроить RAID-контроллер, запустите утилиты настройки сервера и RAID-контроллера.

Настройка сервера

После установки RAID-контроллера на сервере необходимо запустить утилиту настройки сервера. Утилита настройки системы позволяет выполнить настройку аппаратного обеспечения, установленного на сервере или подключенного к нему. Эта утилита обнаруживает каждое аппаратное устройство и настраивает сервер на взаимодействие с ним. С ее помощью можно:

- автоматически настраивать платы PCI;
- определять настройки переключателей и перемычек устройства;
- устранять конфликты использования ресурсов памяти, адресов портов и прерываний;
- управлять установкой модулей памяти, обновлений процессора и запоминающих систем большой емкости (типа жестких дисков, накопителей на магнитной ленте и дисководов гибких дисков);
- устанавливать и хранить такие функции, как установка даты и времени;
- хранить информацию о настройках в энергонезависимой памяти;
- принимать участие в установке сетевой операционной системы;
- принимать участие в работе серверных диагностических средств.

На серверах, входящих в линейку Compaq ProLinea, утилиту настройки системы можно запускать непосредственно с компакт-диска с драйверами/программным обеспечением, поставляемого вместе с сервером или устройствами Compaq (например, RAID-контроллером Smart Array 4250ES). Возможно, у вас уже есть версия этой утилиты, хранящаяся в системном разделе загрузочного диска, но лучше всего использовать ее последнюю версию. Если на вашем сервере нет дисковода для компакт-дисков, с которого можно осуществлять загрузку, создайте дискеты с утилитой настройки с помощью входящего в комплект компакт-диска.

Примечание

Нижеследующие инструкции предназначены для серверной системы Compaq ProLinea; поэтому для получения конкретных инструкций для вашего сервера обратитесь к его документации.

Запуск утилиты

Чтобы настроить сервер на работу с новым RAID-контроллером, необходимо запустить утилиту настройки системы сервера или установочное программное обеспечение вашего RAID-контроллера. Как правило, процесс настройки должен происходить следующим образом:

1. Вставьте загрузочный компакт-диск или дискету 1 с утилитой в соответствующий дисковод сервера.
2. Перезагрузите сервер. Во время загрузки появится несколько сообщений. По меньшей мере, одно из них сообщит о том, что на одном из факультативных слотов обнаружено новое устройство (т. е. RAID-контроллер).
3. Нажмите клавишу (клавиши), необходимую для продолжения загрузки, и запустите утилиту настройки системы.

4. При наличии варианта автоконфигурации выберите **Yes** (Да), и сервер загрузит файлы настроек для всех обнаруженных устройств.
5. На экране **Configuration Complete** (Конфигурирование выполнено) выберите **Review or Modify Hardware Settings** (Просмотр и изменение настроек оборудования).
6. На экране **Steps In Configuring Your Computer** (Шаги по конфигурированию вашего компьютера) выберите **View or Edit Details** (Просмотр или редактирование деталей).
7. Выберите из списка на экране факультативный слот, на котором установлен RAID-контроллер, и измените настройки в соответствии с данными инструкциями.

Настройка последовательности контроллеров

Выберите очередность опознавания нового RAID-контроллера. Всем контроллерам жестких дисков (включая интегрированный SCSI-контроллер на материнской плате, если он предусмотрен) должен быть присвоен уникальный порядковый номер от 1 до 15. Первым контроллером является контроллер первичного диска, который содержит загрузочный диск. Сервер загружается с первого диска этого контроллера. Остальным контроллерам присваиваются номера от 2 до 15.

При установке нового RAID-контроллера вы должны определить, какой контроллер будет управлять загрузочным диском: новый RAID-контроллер, другой SMART-контроллер или встроенный SCSI-контроллер материнской платы. Если новый RAID-контроллер будет первичным контроллером, присвойте ему первый номер. Если вы хотите присвоить встроенному SCSI-контроллеру порядковый номер, отличный от второго, установите номер этого контроллера вручную. При установке нового RAID-контроллера в систему, в которой уже есть контроллер массива, вы можете либо поместить новый контроллер в конец списка номеров контроллеров, либо изменить порядок номеров контроллеров. При изменении порядка номеров изменятся и буквенные обозначения всех дисков в системе. Если вы хотите избежать переименования дисков, поместите новый контроллер в конец списка контроллеров.

Примечание

Если в системе уже есть RAID-контроллеры, то не создавайте ни на одном из дисков, устанавливаемых вместе с новым RAID-контроллером, первичный сегмент.

Сохранение и выход

После настройки сервера на работу с новым RAID-контроллером необходимо сохранить изменения и выйти из программы настройки.

1. Проверьте и отредактируйте свойства всех остальных контроллеров массивов на экране **View or Edit Details**.
2. По окончании редактирования закройте этот экран.
3. На экране **Steps in Configuring Your Computer** (Шаги по конфигурированию вашего компьютера) выберите **Save and Exit** (Сохранить и выйти).

4. На экране **Save and Exit** выберите **Save the Configuration** (Сохранить конфигурацию) и перезагрузите компьютер.
5. На экране **Reboot** (Перезагрузка) нажмите клавишу <Enter>.
6. Извлеките компакт-диск или дискету с утилитой и убедитесь в том, что сервер загрузился в нормальном режиме без ошибок POST — на этом настройка сервера завершена.

Настройка RAID-контроллера

После настройки нового RAID-контроллера с помощью утилиты настройки сервера необходимо запустить утилиту настройки RAID-контроллера, чтобы настроить сам RAID-контроллер. Утилита настройки поддерживает широкий выбор элементов управления дисковым массивом, включая добавление дисков, выбор уровня RAID, создание новых массивов, расширение и наращивание емкости, изменение размеров слоев и других важных параметров RAID.

Примечание

В некоторых операционных системах перед запуском утилиты настройки нужно перевести сеть в автономный режим. К примеру, на серверах с Windows NT и последними версиями Novell Netware утилита настройки контроллера Compaq SmartArray 4250ES не требует перевода сети в автономный режим, а в других операционных системах применение этой утилиты возможно только в автономном режиме.

Запуск утилиты настройки в режиме онлайн

При использовании сетевой операционной системы, поддерживающей утилиту настройки RAID-контроллера в режиме онлайн (например, Windows NT), вы можете устанавливать и запускать ее во время соединения с сетью. При установке Software Support Diskette для Windows NT (NT SSD) дискета приглашает вас вставить диск с утилитой настройки, с которого ее можно будет установить. Значок программы создается автоматически. Запустите утилиту настройки с помощью этого значка. Чтобы запустить утилиту настройки с диска RAID-контроллера, вставьте его в дисковод и включите питание сервера. При появлении меню выберите пункт **Configuration Utility**. После завершения настройки извлеките диск и перезагрузите сервер.

Применение мастера настройки

Если ваш RAID-контроллер поддерживает использование мастера настройки, то процесс проверки и оптимизации дискового массива производится почти автоматически. При запуске утилиты настройки RAID-контроллера программа проверяет установки контроллера и его дисковых массивов. Если массивы не настроены или их настройка не является оптимальной, мастер поможет вам произвести настройку. Это средство оказывается особенно полезным при настройке новых RAID-контроллеров. RAID-контроллер с мастером настройки (например, SmartArray 4250ES) способен выявить следующее.

- Ненастроенный контроллер. Когда утилита настройки обнаруживает ненастроенный контроллер, мастер помогает вам выполнить его настройку.

- Неиспользуемые физические диски. Когда утилита настройки обнаруживает неиспользуемые физические диски, мастер обеспечивает простой способ добавления этих дисков к массиву. К примеру, благодаря способности SmartArray 4250ES наращивать емкость утилита настройки добавляет новые физические диски к существующему массиву без уничтожения данных на существующих логических дисках.
- Неиспользуемое пространство дискового массива. Если утилита настройки обнаруживает наличие в массиве неиспользуемого пространства, мастер поможет вам настроить это пространство на один или несколько логических дисков.

Ручная настройка

Вместо того чтобы использовать мастер настройки для активации дискового массива, вы можете вручную настроить контроллер и дисковый массив с помощью утилиты настройки RAID-контроллера. Рассмотрим, как при использовании RAID-контроллера SmartArray 4250ES создавать новые массивы, наращивать существующие, расширять логические диски, изменять размеры слоев и уровни RAID.

Создание нового массива

Чтобы создать новый дисковый массив, необходимо выбрать RAID-контроллер, который будет им управлять, сгруппировать диски (одинакового размера), а затем на основе физического массива создать логические диски. Предположим, что к вашему RAID-контроллеру SCSI подключено четыре диска емкостью 4,3 Гбайт и два диска емкостью 9,1 Гбайт. Вероятно, вы захотите создать два массива. Массив A будет состоять из трех дисков емкостью 4,3 Гбайт (четвертый диск емкостью 4,3 Гбайт будет выполнять роль резерва), а в массиве B будет два диска емкостью 9,1 Гбайт. Методом обеспечения отказоустойчивости всех логических дисков в массиве A станет RAID 5 (распределенная защита данных), а в массиве B — RAID 1 (зеркальное копирование диска). Рассмотрим этапы ручной настройки такой схемы.

1. Запустите утилиту настройки RAID-контроллера. На экране **Main Configuration** (Главная конфигурация) выберите **Controller Selection** (Выбор контроллера).
2. Выберите один из перечисленных контроллеров. Если на сервере установлен один RAID-контроллер, в списке должен быть только один контроллер.
3. Нажмите кнопку **Controller Settings** (Установки контроллера); в результате появится экран **Controller Settings** (рис. 11.2).
4. Выберите операционную систему.
5. Нажмите кнопку **Create Array** (Создать массив); в результате появится экран **Create Drive Array** (Создать дисковый массив) (рис. 11.3).
6. Из перечисленных дисков выберите три, из которых планируется создать массив A (например, идентификаторы SCSI 0, 1 и 2). Не забывайте, что группировать следует физические диски одинаковой емкости — при объединении дисков разных размеров емкость более крупных из них не используется полностью.
7. Нажмите кнопку **Assign Drive(s) to Array** (Отнести дисковод к массиву).
8. Выберите последний диск емкостью 4,3 Гбайт (ID 3) и нажмите кнопку **Assign Spare to Array** (Назначить резерв в массив). Помните, что один и тот же резерв-

ный диск можно выделить для нескольких массивов, но емкость резервных дисков должна быть равной или превышать емкость дисков, входящих в дисковый массив.

9. Чтобы вернуться к экрану **Main Configuration**, нажмите кнопку **Done** (Выполнено).

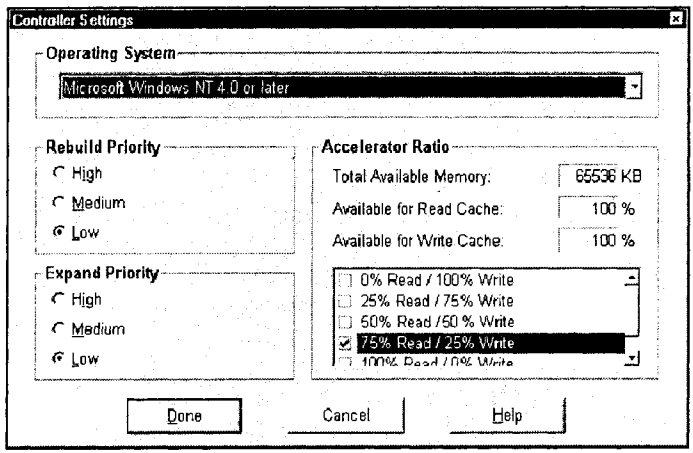


Рис. 11.2. Стандартное диалоговое окно **RAID Controller Settings**

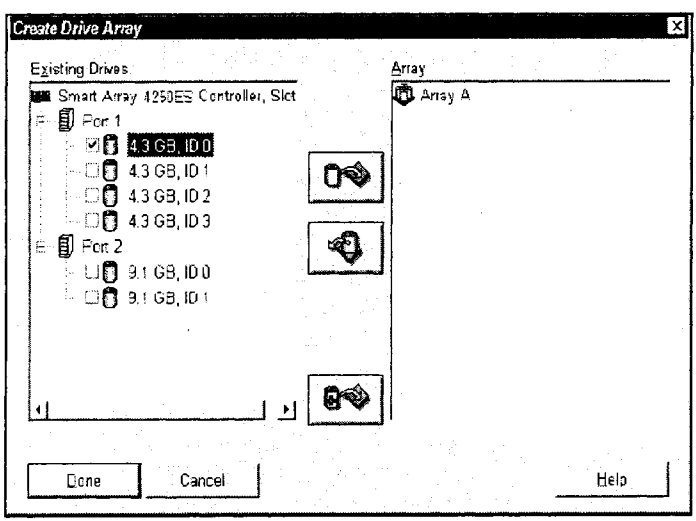


Рис. 11.3. Создание дискового массива RAID

10. Еще раз выберите контроллер, а затем, чтобы создать массив B, нажмите кнопку **Create Array** (Создать массив).
11. Включите в новый массив оба диска емкостью 9,1 Гбайт и нажмите кнопку **Done** (Выполнено).

12. Выберите массив A (или значок **Unused Space** (Неиспользуемое пространство), относящийся к массиву A) в **Logical Configuration View** (Просмотр логической конфигурации).
13. Нажмите кнопку **Create Logical Drive** (Создать логический диск). Появится диалоговое окно **Create Logical Drive** (рис. 11.4).

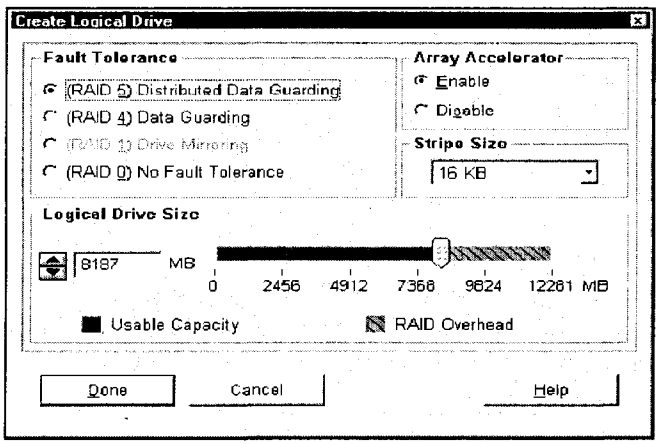


Рис. 11.4. Создание логического диска RAID

14. Выберите уровень RAID. В нашем примере следует нажать кнопку выбора **Distributed Data Guarding (RAID 5)** (Распределенная защита данных).
15. Если ваш контроллер поддерживает ускоритель массива, нажмите кнопку **Array Accelerator Enable** (Разрешить применение ускорителя массива).
16. Определите размер слоя. Вы можете либо оставить значение по умолчанию для выбранного уровня RAID, либо задать другое значение.
17. Определите размер логического диска. В области **Logical Drive Size** доступная емкость диска представлена графически. Если вы хотите создать из доступной емкости единый логический диск, примите значения по умолчанию.
18. Нажмите кнопку **Done** (Выполнено).
19. Выберите массив B (или значок **Unused Space**, относящийся к массиву B) в **Logical Configuration View**.
20. Чтобы создать логический диск в массиве B, повторите вышеприведенные этапы, но на этот раз выберите отказоустойчивость RAID 1.
21. На этом базовая настройка дискового массива завершена.

Наращивание емкости

Под *наращиванием емкости* подразумевается добавление памяти (дисков) к предварительно настроенному массиву. Если существующий массив почти заполнен данными, вы можете нарастить его емкость, не нарушая содержащиеся в нем данные. При запуске утилиты настройки RAID-контроллера она проверяет аппаратную составляющую диска и его настройку. Если утилита настройки обнаружит неиспольз-

зуемый физический диск, то мастер настройки поможет вам добавить этот диск, или вы можете выполнить наращивание емкости вручную.

1. Установите новый физический диск (диски). Группировать следует физические диски одного размера, т. к. если вы объедините диски разной емкости, то емкость дисков большего размера не будет использоваться полностью.
2. Добавьте новые физические диски к имеющемуся массиву. Существующие логические диски автоматически задействуют все физические диски (включая только что добавленные).
3. Создайте новый логический диск для использования дополнительного пространства нового массива.

Рассмотрим конфигурацию, похожую на предыдущую: три диска емкостью 4,3 Гбайт каждый в массиве A (без резервного диска) и два диска по 9,1 Гбайт в массиве B. Если позже будет добавлен четвертый диск емкостью 4,3 Гбайт, то можно выполнить наращивание массива A за счет этого диска.

1. Выберите массив A и нажмите кнопку **Expand** (Нарастить).
2. Выберите свободный диск емкостью 4,3 Гбайт и нажмите кнопку **Assign Drive(s) to Array** (Отнести дисковод к массиву).
3. Нажмите кнопку **Next** (Дальше) в нижней части экрана.
4. Нажмите кнопку **Create Logical Drive** (Создать логический диск) (рис. 11.5).
5. Установите отказоустойчивость, активируйте ускоритель массива, определите размер слоя и задайте размер логического диска 2.
6. Нажмите кнопку **Done** (Выполнено).
7. Вернитесь в главное окно и в строке меню выберите **Controller** и **Save Configuration**, что позволит сохранить новые настройки логического диска 2 и запустить процесс наращивания емкости.

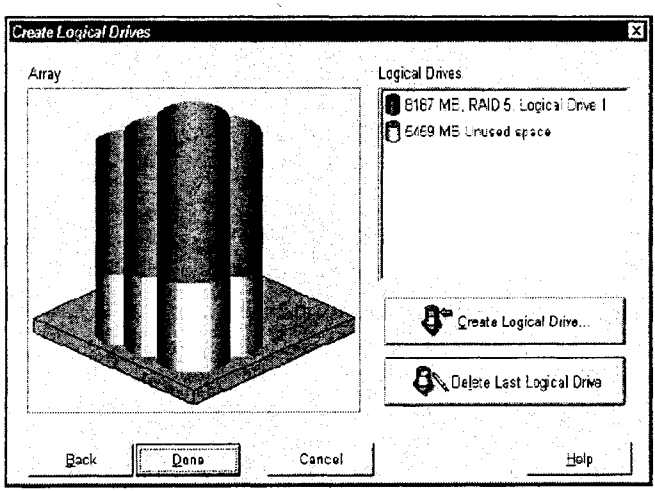


Рис. 11.5. Наращивание емкости массива RAID без изменения его данных

Примечание

В случае отключения электропитания данные о наращивании емкости временно сохраняются в памяти ускорителя массива. Чтобы не допустить потери данных на логическом диске, не стоит заменять RAID-контроллеры или платы ускорителей массива в ходе процесса наращивания емкости.

Расширение емкости

Расширение логических дисков позволяет увеличивать их размер, не трогая находящиеся на них данные. Помните, что не все операционные системы поддерживают расширение логических дисков. Если существующий логический диск заполнен данными, то при наличии в массиве свободного пространства логический диск можно расширить. Если свободного пространства нет, то вы можете добавить в массив диски, а затем расширить логический диск.

1. Щелкните на значке логического диска, который вы хотите расширить.
2. Выберите меню **Drive** (Диск).
3. Выберите **Extend Logical Drive** (Расширить логический диск).
4. На экране **Extend Logical Drive** отображается текущая емкость и служебные данные RAID данного логического диска (рис. 11.6).

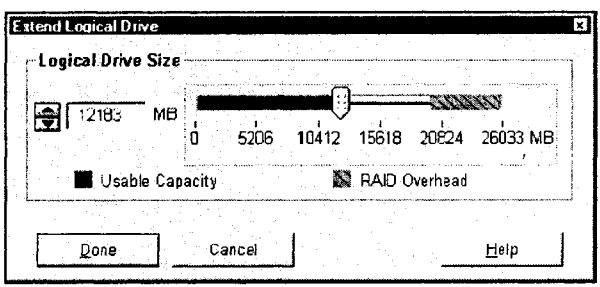


Рис. 11.6. Расширение емкости логического диска при наличии свободного физического пространства

5. Перемещая ползунок, измените (увеличьте) размер логического диска. На этом экране невозможно уменьшить размер логического диска.
6. Нажмите кнопку **Done** (Выполнено).
7. Чтобы сохранить логический диск, войдите в меню **Controller** и выберите пункт **Save Configuration** (Сохранить конфигурацию).
8. Емкость логического диска будет изменена с сохранением всех данных.
9. Активизируйте расширенное пространство логического диска, создав на нем новый раздел или увеличив размер существующих разделов расширенного логического диска.

Изменение уровня RAID и размера слоя

Для изменения уровня отказоустойчивости настроенного логического диска вы можете воспользоваться диалоговым окном **RAID Level** (Уровень RAID), а для измене-

ния текущего размера слоя логического диска — диалоговым окном **Stripe Size Migration**. Оба процесса могут проходить в режиме онлайн и при этом не приводить к потере данных.

1. Выберите логический диск в **Logical Configuration View**.
2. Выберите меню **Drive**.
3. Нажмите кнопку выбора **Migrate RAID/Stripe Size**.
4. Выберите новый уровень RAID (например, нажмите кнопку **RAID 5 Distributed Data Guarding**).
5. Размер слоя для выбранного уровня RAID можно либо изменить, либо оставить значение по умолчанию. К примеру, можно задать размер слоя, равный 16 Кбайт.
6. Нажмите кнопку **Done**.

Перестановка модуля ускорителя массива

В состав многих современных RAID-контроллеров входит крупный кэш-модуль под названием ускоритель массива (к примеру, контроллер SmartArray 4250ES имеет съемный ускоритель массива емкостью 64 Мбайт, а AMI MegaRAID Express Plus поддерживает до 128 Мбайт встроенной памяти ОЗУ). Ускоритель массива обеспечивает промежуточное хранение данных между системой и дисковым массивом, чтобы в случае отключения электропитания и повреждения диска эти данные не были повреждены. Как правило, ускоритель массива представляет собой съемную плату, так что при необходимости его можно без труда заменить. Учитывая отказоустойчивую природу большинства RAID-контроллеров, перед включением RAID-контроллера нужно обязательно подключить модуль ускорителя массива. Ускоритель массива выполняет несколько особых функций.

- Он ускоряет сохранение данных, временно кэшируя их на высокой скорости внутренней шины и перенося их на диски с более низкой скоростью записи.
- Он имеет собственные аккумуляторы, которые позволяют сохранять данные в отсутствие внешнего питания — даже в том случае, если ускоритель массива удален с RAID-контроллера.
- Его память поддерживает обнаружение и исправление ошибок; благодаря этому надежность данных повышается.
- В конфигурации с одним RAID-контроллером модуль ускорителя массива можно переместить на другой совместимый RAID-контроллер, чтобы завершить передачу данных в случае выхода из строя первого RAID-контроллера.
- В конфигурации с резервированием RAID-контроллера обычно не нужно перемещать ускоритель массива в случае отказа одного из контроллеров — данные, предназначенные для записи, автоматически синхронизируются между обоими RAID-контроллерами.

Извлечение ускорителя

Так как ускоритель массива обычно реализуется в виде платы, он закрепляется на RAID-контроллере с помощью многочисленных винтов. Для того чтобы извлечь ускоритель с RAID-контроллера SmartArray 4250ES, проделайте нижеприведенные шаги.

1. Для снятия двух винтов с верхней части платы ускорителя следует воспользоваться отверткой Torx T-10.
2. Переверните плату RAID-контроллера и выкрутите пять винтов, которые фиксируют на ней кронштейн жесткости.
3. Снимите кронштейн жесткости.
4. Выкрутите из кронштейна платы ускорителя последний винт.
5. Снимите кронштейн платы ускорителя.
6. Чтобы снять модуль ускорителя массива с RAID-контроллера, переверните плату и поверните защелку на 90°.
7. Аккуратно поднимите плату ускорителя (взявшись за ее верхнюю часть), чтобы отделить ее от сигнальных коннекторов на RAID-контроллере.
8. Чтобы установить плату ускорителя на RAID-контроллер, выполните перечисленные действия в обратном порядке.

Установка драйверов операционной системы

После установки и настройки RAID-контроллера нужно установить драйверы для операционной системы. В этой части главы даны инструкции по установке драйверов для контроллеров (типа Compaq SmartArray 4250ES) в среде Windows 2000/NT, Novell NetWare и Linux. Прежде чем устанавливать драйверы операционной системы, следует (при необходимости) обновить систему BIOS на сервере и настроить дисковые массивы с помощью утилиты настройки RAID-контроллера.

Примечание

Эти последовательности действий следует рассматривать как примеры. Подробные инструкции по установке можно получить в документации к RAID-контроллеру.

Windows 2000

Большинство современных RAID-контроллеров поддерживают драйверы для Windows 2000 (т. е. для сервера на базе Windows 2000). К примеру, для работы AMI MegaRAID в среде Windows 2000 поставляется драйвер мини-порта. Чтобы установить утилиты и драйверы AMI MegaRAID на компьютере с Windows 2000, сделайте следующее.

1. После установки RAID-контроллера загрузите Windows 2000. На экране появится мастер **Found New Hardware Wizard** (Мастер обнаружения нового устройства).
2. Нажмите кнопку **Cancel** (Отмена) для всех новых устройств (не позволяйте мастеру проводить автоматическое распознавание контроллера).
3. Нажмите кнопку **Start** (Пуск), выберите **Settings** (Настройки), а затем **Control Panel** (Панель управления).
4. Двойным щелчком выберите значок **Add/Remove Hardware** (Установка и удаление оборудования). На экране появится мастер установки оборудования **Add/Remove Hardware Wizard**. Нажмите кнопку **Next** (Дальше).

5. Затем появится экран **Choose a Hardware Task** (Выбор задачи). Выберите для нужного устройства **Add/Troubleshoot** (Добавить/Найти неисправности), и нажмите кнопку **Next** (Дальше).
6. Появится экран **Choose a Hardware Device** (Выбор устройства). Выберите PCI-устройство, которое в перечне устройств отмечено восклицательным знаком (!). Оно должно быть первым в списке устройств. Нажмите кнопку **Next** (Дальше).
7. После завершения работы с мастером установки оборудования **Add/Remove Hardware Wizard** нажмите кнопку **Finish** (Готово).
8. Нажмите кнопку **Next** (Дальше). В результате откроется диалоговое окно **Welcome to the Upgrade Device Driver Wizard** (Добро пожаловать в Мастер установки обновления драйверов устройств), затем нажмите кнопку **Next** (Дальше).
9. Появится экран **Install Hardware Device Drivers** (Установка драйверов оборудования). Обязательно укажите все доступные драйверы.
10. Вставьте в дисковод диск с RAID-драйвером.
11. Появится экран **Hardware Type** (Тип оборудования). Выберите из списка SCSI- и RAID-контроллеры и нажмите кнопку **Next** (Дальше).
12. Появится экран **Select a Device Driver** (Выбор драйвера устройства). На экране появится запрос на указание драйвера, который вы хотите установить для данного устройства. Выберите производителя и модель вашего устройства и нажмите кнопку **Next** (Дальше).
13. На экране появится список всех контроллеров данного класса устройств. Укажите модель вашего контроллера и нажмите клавишу <Enter>.
14. Появится экран **Start Device Driver Installation** (Начало установки драйвера устройства). Чтобы начать установку драйвера для выбранного устройства, нажмите кнопку **Next** (Дальше).
15. По окончании установки драйверов всех SCSI-контроллеров, чтобы закончить работу с мастером, нажмите кнопку **Finish** (Готово). На этом процесс установки драйверов завершается.

Windows NT 4.0

Чтобы установить на сервере драйвер RAID-контроллера для Windows NT, вам понадобится диск с драйверами, чистые дискеты, а также доступ к серверу или рабочей станции с загрузочным компакт-диском (чаще всего, это компьютер, на который производится установка RAID-контроллера). Чтобы получить доступ к драйверу на диске, сначала нужно создать дискеты SSD (Support Software Diskettes — дискеты с сопровождающим программным обеспечением) для Windows NT. На этих дискетах будут записаны последняя версия операционной системы, драйверы и сопроводительная документация к контроллеру. Чтобы создать такие дискеты, сделайте следующее:

1. Загрузите сервер с компакт-диска контроллера.
2. На экране **System Utilities** (Системные утилиты) выберите **Create Support Software** (Создать ПО поддержки).

3. На экране **Diskette Builder** (Создание дискеты) выберите **Create Support Server Diskettes from CD** (Создать дискеты поддержки сервера с CD).
4. В списке выберите **Support Software for Windows NT** (ПО поддержки для Windows NT).
5. Чтобы создать дискеты SSD, следуйте инструкциям на экране.

Установка RAID-контроллера в среде Windows NT

Установить драйвер RAID-контроллера можно в ходе установки Windows NT 4.0 с помощью файлов с дискет SSD для Windows NT:

1. Запустите процесс установки Windows NT.
2. Программа установки автоматически распознает запоминающие устройства. Если программа просит вас указать дополнительные запоминающие устройства, нажмите клавишу <S>.
3. Выберите пункт списка **Other (Requires Disk Provided by Manufacturer)** и нажмите клавишу <Enter>.
4. Вставьте в дисковод дискету SSD Windows NT 4.0 #1 и нажмите клавишу <Enter>.
5. Из списка контроллеров выберите RAID-контроллер (например, Compaq Integrated Smart Array 42XX контроллер для Windows NT 4.0) и нажмите клавишу <Enter>.
6. Нажмите клавишу <Enter> еще раз и продолжайте установку Windows NT 4.0.
7. При появлении соответствующего запроса вставьте дискету SSD Windows NT еще раз, и программа установки скопирует драйверы в систему.

Обновление драйвера RAID-контроллера

Как правило, обновление драйвера RAID-контроллера проходит в два этапа: сначала удаляется старый драйвер, а затем устанавливается новый. Программа SSD Setup операционной системы Windows NT позволяет пропустить этапы удаления/установки драйверов и обновить драйвер следующим образом.

1. Запустите Windows NT и войдите в систему, воспользовавшись учетной записью с привилегиями администратора.
2. Вставьте в дисковод дискету SSD Windows NT (дискету #1).
3. Чтобы запустить программу установки, введите a:\setup (где a: является именем диска).
4. Выберите **Custom Setup** (Выборочная установка).
5. Выберите ваш RAID-контроллер (например, Compaq Integrated Smart Array 42XX Controller) и нажмите кнопку **Update** (Обновить).
6. Программа установки выполнит обновление драйвера в вашей системе с дискет SSD Windows NT.
7. Выберите **Close** и выйдите из программы установки.
8. Извлеките из дисковода дискету SSD, закройте Windows NT и перезагрузите систему, чтобы загрузить новый драйвер.

Установка RAID-контроллера после установки Windows NT

Если вам нужно установить RAID-контроллер после завершения установки Windows NT, вы можете воспользоваться утилитой установки с дискет SSD Windows NT. Эта утилита распознает аппаратные средства, физически установленные в системе, и предложит драйверы устройств, которые следует установить или обновить.

1. Запустите Windows NT в системе, в которой вы хотите установить драйверы, и зарегистрируйтесь, воспользовавшись учетной записью с привилегиями администратора.
2. Вставьте в дисковод дискету#1 SSD Windows NT.
3. Откройте **Program Manager** и выберите **File**, а затем **Run**.
4. Введите `a:\setup` и нажмите клавишу <Enter>.
5. Выберите **Custom**.
6. Выберите RAID-контроллер (например, Compaq Integrated Smart Array 42XX Controllers). Если его драйвер в вашей системе уже установлен, программа установки сообщит, можно ли его обновить. Если можно, нажмите кнопку **Update**. Если же драйвер ранее не устанавливался, нажмите кнопку **Install** и по запросу утилиты вставьте в дисковод необходимые дискеты.
7. После этого вы можете либо установить с помощью утилиты установки другие компоненты, либо, если все задачи выполнены, нажать кнопку **Close**. Программа установки сообщит вам о необходимости перезагрузки системы для активации установленного/обновленного драйвера.

Удаление драйвера

Возможно, перед установкой нового контроллера или разрешением конфликтов устройств вам потребуется удалить драйвер RAID-контроллера. В системе Windows NT все операции с драйверами устройств проводятся только через **Control Panel** (Панель управления).

Примечание

Если система загружается с устройства, подключенного к RAID-контроллеру, то драйвер RAID-контроллера удалять не следует. В этом случае на экране появится диалоговое окно с сообщением о том, что выбранный контроллер используется как загрузочное устройство и его удаление может привести к тому, что система не загрузится.

1. Запустите Windows NT и войдите в систему, воспользовавшись учетной записью с привилегиями администратора.
2. В Панели управления **Control Panel** запустите утилиту SCSI Adapter.
3. Откройте вкладку **Drivers**.
4. Выберите контроллер (например, Compaq Integrated Smart Array 42XX Controllers) и нажмите кнопку **Remove**.
5. После удаления драйвера нажмите кнопку **OK**. Чтобы удаление вступило в силу, необходимо перезагрузить систему.

Установка программных средств резервирования

Если ваша операционная система поддерживает программные средства резервирования, их можно установить следующим образом (вариант для Windows NT).

1. В системе, в которой планируется установить программные средства резервирования, запустите Windows NT и зарегистрируйтесь, воспользовавшись учетной записью с привилегиями администратора.
2. Вставьте в дисковод дискету SSD Windows NT (обычно это дискета #7).
3. В **Program Manager** выберите **File**, а затем **Run**.
4. Введите `a:\setup` и нажмите клавишу <Enter>.
5. Выберите программу резервирования для RAID-контроллера. Если вы уже устанавливали такую программу в системе, утилита установки сообщит, можно ли ее обновить. Если да, нажмите кнопку **Update** (Обновить). Если это программное обеспечение не установлено, нажмите кнопку **Install** (Установить).
6. После этого вы можете либо установить с помощью утилиты установки другие компоненты, либо, если все задачи выполнены, нажать кнопку **Close**. Программа установки сообщит вам о необходимости перезагрузки системы для активации только что установленного программного обеспечения.

Удаление программных средств резервирования

Если на вашем сервере установлены программные средства резервирования RAID-контроллера, и вы хотите их удалить, это можно сделать следующим образом.

1. В системе, в которой установлены программные средства резервирования, запустите Windows NT и зарегистрируйтесь, воспользовавшись учетной записью с привилегиями администратора.
2. Вставьте в дисковод дискету #1 SSD Windows NT.
3. В **Program Manager** выберите **File**, а затем **Run**.
4. Введите `a:\setup` и нажмите клавишу <Enter>.
5. Выберите программный компонент резервирования RAID-контроллера и нажмите кнопку **Remove**.
6. После этого вы можете либо установить/удалить с помощью утилиты установки другие компоненты, либо, если все задачи выполнены, нажать кнопку **Close**. Утилита установки сообщит вам о необходимости перезагрузить систему для активации только что установленного программного обеспечения.

Novell NetWare 5.0

Чтобы установить на сервере драйвер RAID-контроллера для NetWare, вам потребуется диск с драйверами контроллера, чистые дискеты, а также доступ к серверу или рабочей станции с загрузочным компакт-диском (чаще всего это система, в которой происходит установка RAID-контроллера). Прежде чем обратиться к драйверу на компакт-диске, нужно создать дискеты Novell SSD. На этих дискетах будут храниться последняя версия программы операционной системы, драйверы и сопроводи-

тельная документация к контроллеру. Чтобы создать такие дискеты, сделайте следующее.

Примечание

Прежде чем проводить установку драйверов устройства, установите и загрузите последнюю версию Support Pack или заплату к операционной системе. Комплекты заплат и Support Pack для Novell можно загрузить непосредственно с Web-сайта этой компании.

1. Загрузите сервер с компакт-диска контроллера.
2. На экране **System Utilities** выберите **Create Support Software**.
3. На экране **Diskette Builder** выберите **Create Support Server Diskettes from CD**.
4. Из списка выберите **Support Software for Novell NetWare**.
5. Чтобы создать дискеты SSD Novell, следуйте инструкциям на экране.

Установка драйвера

Компакт-диск с драйвером автоматически распознает только что установленный контроллер, затем копирует необходимые драйверы и обновляет файл STARTUP.NCF на сервере. Процесс установки или обновления драйверов устройств в среде NetWare довольно прост. Чтобы установить драйвер RAID-контроллера на сервере NetWare v3.20, v4.2 или v5.0, скопируйте необходимые файлы с дискеты SSD Novell (обычно они расположены на дискете #3) в загрузочный каталог сервера (а при желании — и в каталог SYS:SYSTEM). После завершения процесса установки драйвера вам следует обратиться к документации по установке NetWare для получения информации об установке и сборке томов, связанных с новой дисковой подсистемой.

NetWare и зеркальное копирование дисков

NetWare рассматривает каждый логический диск массива как отдельный физический диск. Если вы скопируете логические диски в одном массиве, а затем физический диск выйдет из строя, то из строя выйдут и оба логических диска из пары и ваши данные будут потеряны. Во избежание этого следует копировать логические диски, находящиеся в разных массивах. Для просмотра настроек контроллера воспользуйтесь утилитой настройки RAID-контроллера для NetWare (файл CPQONLIN.NLM) с дискеты SSD #1 Novell. Зафиксируйте логические диски (и массивы, в которых они расположены). При настройке зеркального копирования дисков в среде NetWare выбирайте логические диски одинакового размера, расположенные в разных массивах.

Примечание

Не используйте зеркальное копирование дисков в среде NetWare, если у вас нет хотя бы двух различных дисковых массивов.

Устранение неисправностей дисков в среде NetWare

Несмотря на то, что диски выходят из строя достаточно редко, большое значение имеет защита важных данных. Лучший способ обеспечить восстановление после

выхода диска из строя — это настроить в вашей системе дисков какую-либо форму отказоустойчивости. При наличии методик обеспечения отказоустойчивости контроллер также получает возможность выполнять фоновый анализ поверхности жестких дисков и проверять их на наличие поврежденных секторов (перемещая данные в другие области носителя). Эта возможность повышает надежность и доступность ваших данных. В любом случае, вам следует использовать методы резервирования данных, чтобы защитить данные в случае масштабного сбоя. При обнаружении неисправного диска придерживайтесь следующих общих правил.

1. Определите, какой физический диск вышел из строя и отметьте его тип и емкость.
2. Обратите внимание, какой раздел и том неисправны. Эта информация содержится в сообщении об ошибке на консоли сервера. Кроме того, она фиксируется в файле с журналом регистрации ошибок на сервере, который можно просмотреть с помощью утилиты SYSCON или NWADMIN.
3. Проверьте, есть ли у вас недавно сделанная резервная копия данных с неисправного диска. Если диск входит в отказоустойчивый том с зеркальным отображением или в аппаратный отказоустойчивый том, то потерянные данные, вероятно, можно будет восстановить без помощи резервной копии; впрочем, это не умаляет роли резервных копий как важного средства защиты данных.
4. Найдите замену неисправному диску; тип и емкость нового диска должны быть аналогичны неисправному.

Ниже приводятся инструкции по замене диска применительно к конфигурации вашего сервера. Помните, что NetWare не выполняет зеркальное копирование информации на разделах DOS — поддержку дублированных разделов DOS предусматривают только аппаратные методы обеспечения отказоустойчивости. Если у вас есть дублированный диск, содержащий раздел DOS, то для восстановления информации из раздела DOS нужно будет обратиться к другому источнику. Если на диске, который вышел из строя, был раздел DOS, NetWare не сможет обратиться к той информации, которая была в этом разделе. К примеру, среди файлов в разделе DOS есть STARTUP.NCF и драйверы дисководов для Novell. Чтобы предупредить попытки NetWare считать или записать на неисправное устройство, выполните с консоли следующую команду:

```
REMOVE DOS
```

Если ваш сервер не настроен на аппаратное обеспечение отказоустойчивости, а на неисправном диске был раздел DOS, который использовался для загрузки сервера, то после отключения питания сервера вы не сможете его включить. Запланируйте текущий ремонт на ближайшее время и сделайте следующее:

1. Отключите питание сервера.
2. Замените неисправный физический диск.
3. Перезапустите систему с дискеты с утилитой настройки сервера.
4. Выберите вариант установки системного раздела (**Install a System Partition**) на загрузочное устройство DOS.
5. Выйдите из утилиты настройки сервера.

6. Найдите загрузочную дискету DOS, на которой содержатся программы DOS FDISK и FORMAT.
7. С помощью программы FDISK создайте на новом диске первичный раздел DOS, размер которого должен составлять как минимум 60 Мбайт.
8. Сделайте созданный раздел DOS активным.
9. С помощью команды FORMAT отформатируйте раздел DOS; в результате в нем должны появиться файлы, необходимые для того, чтобы он выполнял функцию загрузочного раздела (например, `FORMAT C: /S`).
10. Если у вас есть резервная копия раздела DOS, воспользуйтесь ей для выполнения предыдущего пункта. В противном случае, возьмите дискеты для сервера NetWare и скопируйте в каталог NetWare раздела DOS файлы SERVER.EXE, INSTALL.NLM, VREPAIR.NLM, MONITOR.NLM, CLIB.NLM и STREAMS.NLM.
11. Скопируйте необходимые драйверы дисков, драйверы локальной сети и служебные файлы .NLM, которые должны быть в разделе DOS, с дискеты SSD Novell.
12. Скопируйте в раздел DOS всю прочую необходимую информацию и перезапустите систему. Теперь можно загрузить сервер NetWare (возможно, вам придется создать файл STARTUP.NCF).

Если вы не настроили отказоустойчивость для дисков, подключенных к RAID-контроллеру, но при этом настроили зеркальное копирование или дублирование контроллеров для NetWare, то для восстановления данных после выхода диска из строя необходимо выполнить следующие действия:

1. Определите, какой неисправный физический диск привел к выходу из строя устройства NetWare. Запишите номер и имя устройства неисправного логического диска, например:

   ```
   NWPA: [V503-A2-D1:0] Compaq SMART-2 Slot 8 Disk 2 NFT
   ```

2. Сообщения о неисправностях фиксируются на консоли сервера и в файле с журналом регистрации ошибок на сервере, который можно просмотреть с помощью утилиты SYSCON или NWADMIN. Позже, при создании нового раздела, эта информация вам понадобится.
3. Загрузите файл INSTALL.NLM и откройте меню **Disk Options Mirroring**. Выберите дублированный логический раздел, на который повлиял выход диска из строя. Зафиксируйте номер устройства и номер раздела действующего логического диска в группе зеркального копирования. Эта информация впоследствии потребуется для того, чтобы выполнить повторное зеркальное копирование восстановленного логического диска.
4. Удалите недоступное (возможно, работающее не синхронно) устройство из группы **Mirror Partition** (Зеркальный раздел) — это устройство недоступно из-за неисправности диска.
5. Запомните место отсека, в котором находился вышедший из строя физический диск — новый диск должен быть установлен в тот же отсек.
6. Если неисправный диск обладает возможностью горячего подключения, отключать питание сервера не потребуется. В противном случае вам придется заплани-

ровать время простоя сервера, отключить его от сети и отключить питание устройства.

7. Вставьте новый физический диск в отсек, в котором находился неисправный диск. Емкость нового диска должна быть равна емкости диска, вышедшего из строя. Проверьте крепления всех кабельных коннекторов.
8. Подключите новое устройство. Для выбора этого устройства воспользуйтесь опцией **Disk Information** (Информация о диске) в файле MONITOR.NLM. В некоторых версиях NetWare при выборе этой опции активация устройства происходит автоматически. В других версиях активацию устройства нужно производить вручную, заменив его рабочее состояние на "активное". Если активация неисправного логического диска прошла успешно, драйвер отсылает на консоль соответствующее уведомление.
9. Чтобы определить количество блоков Hot Fix Redirection, установленных для данного раздела (т. е. просмотреть данные о зеркально скопированном, а не о вышедшем из строя диске), воспользуйтесь опцией **Change Hot Fix** в файле INSTALL.NLM.
10. Для удаления и создания раздела на восстановленном логическом диске воспользуйтесь утилитой INSTALL.NLM.

Примечание

Хотя таблица разделов логического диска, вероятно, верна, данные на этом логическом диске недействительны. Некоторые данные могут оказаться действительными, потому что неисправный физический диск являлся всего лишь частью логического диска. Но в этой точке в данных логического диска появляется "дыра". Удалите все устаревшие или недействительные данные, а затем создайте на логическом диске новый раздел.

11. В меню **Disk Options** (Параметры диска) утилиты INSTALL.NLM выберите опции **Modify Disk Partitions** (Изменить разделы диска) и **Hot Fix** ("Горячая" фиксация).
12. В меню **Available Disk Drives** (Доступные дисководы) утилиты INSTALL.NLM выберите восстановленный логический диск, который ранее был неисправен (информация об этом устройстве была зафиксирована во время выполнения 1-го шага).
13. Выберите опцию **Delete Partition** (Удалить раздел). Утилита INSTALL.NLM, возможно, выведет несколько сообщений об ошибке. Так как вы собираетесь удалить данный раздел, не нужно обновлять какую-либо информацию Volume Definition Table. Продолжайте, пока раздел не будет удален.
14. Если утилита INSTALL.NLM сообщит о невозможности удаления раздела из-за того, что он заблокирован другим процессом, выгрузите все процессы NLM, которые заблокировали раздел. После создания раздела и данных тома модули NLM нужно будет перезагрузить.
15. Создайте раздел на том же логическом диске.
16. Вернитесь в меню **Disk Options Mirroring** и выберите номер ранее дублированного раздела NetWare 386 (его нужно было записать во время выполнения 2-го шага).

17. Чтобы вывести список разделов, которые можно повторно зеркально копировать, нажмите клавишу <Insert>. Выберите раздел, ассоциированный с восстановленным устройством (указанный в шаге 1). В результате NetWare проведет повторную синхронизацию дублированных разделов. Сообщение на консоли укажет на успешное завершение этапа повторной синхронизации.

Если на вашем сервере не был настроен ни один метод обеспечения отказоустойчивости, вам придется восстанавливать данные с резервного носителя. Это делается следующим образом.

1. Определите, какой неисправный физический диск привел к выходу из строя устройства NetWare. Запишите номер и имя неисправного логического диска, например:

```
NWPA: [V503-A2-D1:0] Compaq SMART-2 Slot 8 Disk 2 NFT
```

Примечание

Сообщения о неисправностях фиксируются на консоли сервера и в файле с журналом регистрации ошибок на сервере, который можно просмотреть с помощью утилиты SYSCON или NWADMIN. Эта информация потребуется вам позже, при создании раздела.

2. Снимите неисправный диск.
3. Вставьте новый диск в отсек, в котором был неисправный диск. Емкость нового диска должна быть равна емкости диска, вышедшего из строя.
4. Подключите новое устройство. Для выбора этого устройства воспользуйтесь опцией **Disk Information** в файле MONITOR.NLM. В некоторых версиях NetWare при выборе этой опции активация устройства происходит автоматически. В других версиях активируйте устройство вручную, заменив его рабочее состояние на "активное". Если реактивация неисправного логического диска прошла успешно, драйвер отсылает на консоль соответствующее уведомление.
5. Если вы хотите определить количество блоков Hot Fix Redirection, установленных для данного раздела, воспользуйтесь опцией **Change Hot Fix** утилиты INSTALL.NLM.

Примечание

Хотя таблица разделов логического диска, возможно, верна, данные на этом логическом диске недействительны. Возможно, некоторые данные окажутся действительными, потому что неисправный физический диск являлся всего лишь частью логического диска. Но в этой точке в данных логического диска появляется "дыра". Удалите все устаревшие или недействительные данные, а затем создайте на логическом диске новый раздел.

6. Возвратитесь к меню **Disk Options** утилиты INSTALL.NLM, и выберите опции **Modify Disk Partitions** и **Hot Fix**. В результате драйвер должен реактивировать неисправный логический диск. В случае успешного выполнения реактивации неисправного логического диска драйвер отсылает на консоль соответствующее уведомление.

7. В меню **Available Disk Drives** утилиты INSTALL.NLM выберите восстановленный логический диск, который ранее неисправен (информация об этом устройстве была зафиксирована во время выполнения 1-го шага).
8. Выберите опцию **Delete Partition**. Утилита INSTALL.NLM, возможно, выведет несколько сообщений об ошибке. Удалите том, связанный с этим разделом. Так как вы собираетесь удалить этот раздел, не обновляйте информацию Volume Definition Table. Продолжайте, пока раздел не будет удален.
9. Если утилита INSTALL.NLM сообщит о невозможности удаления раздела из-за того, что он заблокирован другим процессом, выгрузите все блокирующие раздел процессы NLM. После создания раздела и данных тома эти модули нужно будет перезагрузить.
10. Создайте раздел на том же логическом диске.
11. Создайте том.
12. Найдите носитель с последней резервной копией данных и восстановите данные в этот том сервера.

Linux

Учитывая рост популярности операционных систем Linux, вам, возможно, придется устанавливать или обновлять драйверы RAID на сервере, работающем на основе этой операционной системы. Чтобы установить драйверы контроллера AMI MegaRAID вместе с системой Red Hat Linux 6.2, выполните следующую процедуру.

1. Загрузите компакт-диск с Disk 1.
2. В загрузочной командной строке на экране **Welcome** введите `expert` и нажмите клавишу <Enter>.
3. Скопируйте образ драйвера для Linux с диска с драйверами RAID на дискету, а затем вставьте ее в дисковод.
4. Выберите **English** как язык по умолчанию и нажмите кнопку **OK**.
5. Выберите тип системной клавиатуры **US** и нажмите кнопку **OK**.
6. Выберите **Local CD-ROM** в качестве типа носителя, содержащего пакеты, предназначенные для установки, и нажмите кнопку **OK**.
7. Чтобы добавить устройства SCSI, выберите **Add Device** и нажмите **OK**.
8. Выберите **SCSI** и нажмите кнопку **OK**.
9. Выберите из списка **AMI MegaRAID Adapter Driver**. В результате будет загружен драйвер для устройства SCSI. Нажмите кнопку **OK**.
10. На экране **Mouse Configuration** выберите ваш тип мыши и нажмите кнопку **OK**.
11. При появлении экрана **GUI Welcome** нажмите кнопку **Next**.
12. При появлении экрана **Install Options** выберите **Custom** и нажмите кнопку **OK**.
13. Проведите инициализацию дисков. Для создания разделов следует выбрать **Add** на экране **Partitions**.
14. Введите левую косую черту (/), чтобы обозначить точку сборки.

15. Перейдите к **Size (MB)**, введите размер массива и нажмите клавишу <Enter>. Введенное значение должно быть не меньше 1,515 Мбайт; в противном случае установка будет невозможна. Обратите внимание, что выделенным типом раздела (**Partition Type**) является **Linux Native**. Это значит, что вы выбираете пространство на жестком диске.
16. Для создания еще одного раздела нажмите кнопку **Add** на экране **Partitions**.
17. Выберите в качестве типа раздела (**Partition Type**) **Linux Swap**.
18. Перейдите к **Size (MB)**. Введите 125 и нажмите кнопку **OK**.
19. На следующем экране также нажмите кнопку **OK**.
20. Появится экран **LILO Configuration**. Снимите флажок **Create Book disk** и нажмите кнопку **OK**. Что делать в данном случае, решает пользователь — создание загрузочного диска не является обязательным условием для продолжения установки.
21. При появлении экрана **Time Zone Select** выберите часовой пояс, в котором находится ваша система и нажмите кнопку **OK**.
22. Появится экран **Account Configuration**. Выберите и введите корневой пароль, затем подтвердите его. Нажмите кнопку **Next**. Этот пароль необходимо запомнить, чтобы после завершения инсталляции с его помощью вы смогли зарегистрироваться в системе.
23. На экране **Authentication Configuration** нажмите кнопку **Next**.
24. Появится экран **Select Package Group**. Выберите **Everything** и нажмите кнопку **Next**.
25. При появлении экрана **X-Configuration** выберите установленные в системе монитор и видеокарту и нажмите кнопку **Next**.
26. Для начала установки Linux 6.2 нажмите кнопку **Next**.
27. Для завершения установки нажмите кнопку **Exit**.
28. Теперь произойдет перезагрузка системы.

Изменение настроек контроллера

После установки и ввода в действие RAID-контроллера вам, возможно, понадобится изменить его настройки. Прежде чем пытаться вносить какие-либо изменения в существующую установку RAID, следует внимательно ознакомиться с мерами предосторожности и требованиями, связанными с конкретными RAID-контроллером и корпусом сервера. Вот несколько замечаний, которые нужно учесть с самого начала.

- Каждый канал RAID может поддерживать большое количество дисков (до 14), но контроллер ограничен количеством физических дисков, поддерживаемых сервером.
- Проверьте допустимые сочетания дисков. Некоторые RAID-контроллеры позволяют использовать Wide Ultra2 SCSI, Wide Ultra SCSI-3 или комбинации этих типов на серверах и в запоминающих системах, поддерживающих диски с горячим подключением. Впрочем, это замечание справедливо по отношению не ко всем сочетаниям контроллера/сервера.

- Диски могут не требовать терминирования. К примеру, серверы Compaq и структура их внутренних кабелей обеспечивают терминирование шины SCSI.
- Проверьте допустимые размеры дисков. Ваш RAID-контроллер может быть ограничен в размерах и интерфейсах используемых дисков.
- При группировке дисков в одном массиве их емкость должна быть одинаковой, что обеспечивает максимальную эффективность хранения данных.
- Проверьте наличие "зарезервированных идентификаторов". К примеру, внешние диски (без возможности горячего подключения), подключенные к некоторым RAID-контроллерам (например, Compaq SmartArray 4250ES) не должны устанавливаться с идентификатором 6 и 7 (т. е. SCSI ID6), т. к. идентификаторы 6 и 7 SCSI предназначены для резервирования контроллеров.

Точная настройка отказоустойчивости

Возможно, вам понадобится внести изменения в уровень отказоустойчивости (RAID), применяемый в массиве. Такая необходимость может возникнуть при добавлении или снятии дисков с сервера или при модификациях сети. К примеру, в ранних реализациях сети приоритет эффективного хранения данных может быть выше приоритета обеспечения отказоустойчивости, но необходимость защиты ценных данных, возможно, заставит вас выбрать другой уровень отказоустойчивости RAID. Вот, как можно это сделать.

1. Выберите новый уровень RAID. Первой задачей является определение нужного уровня *(см. разд. "Уровни RAID" ранее в этой главе)*.
2. Сделайте копию данных дискового массива. Как правило, переход от одного уровня RAID к другому с помощью утилиты настройки RAID-контроллера осуществляется без потери данных. Если это невозможно (утилита настройки должна сообщить вам об этом), вам нужно будет сначала создать резервные копии данных, а затем изменить уровень RAID.
3. Выполните настройку массива. Чтобы изменить настойку дискового массива, назначив для него новый метод обеспечения отказоустойчивости, запустите утилиту настройки RAID-контроллера. Если сообщение об ошибке указывает на необходимость увеличения количества секторов, вы должны удалить старый том и настроить его в качестве нового тома с новым методом обеспечения отказоустойчивости, который вы выбрали.
4. Восстановите данные. Скопируйте защищенные данные обратно на те же логические диски (если это необходимо). Ваша система автоматически перераспределит данные, основываясь на новой схеме обеспечения отказоустойчивости.

Точная настройка размера слоя

Возможно, вам придется изменить размер слоя в массиве. Такая необходимость может возникнуть при добавлении или снятии дисков с сервера или при модификациях сети. Ниже приведены основные принципы выполнения этой задачи:

1. Выберите новый размер слоя. Определите желаемый размер слоя для вашего массива и уровня RAID *(см. разд. "Организация чередующегося диска" ранее в этой главе)*.

2. Сделайте копию данных дискового массива. Как правило, переход от одного размера слоя к другому с помощью утилиты настройки RAID-контроллера осуществляется без потери данных. Если это невозможно (утилита настройки должна сообщить вам об этом), вы должны сначала создать резервные копии данных, а затем изменить размер слоя.
3. Выполните настройку размера слоя. Чтобы изменить настройку дискового массива, назначив для него новый размер слоя, запустите утилиту конфигурации RAID-контроллера. Если сообщение об ошибке указывает на необходимость увеличить количество секторов, вы должны удалить старый том и настроить его в качестве нового тома с новым размером слоя, который вы выбрали.
4. Восстановите данные. Скопируйте защищенные данные обратно на те же логические диски (если это необходимо). Ваша система автоматически перераспределит данные, основываясь на новой схеме чередования.

Перемещение дисков в пределах массива

Перемещение дисков (применение иных назначений идентификаторов) возможно на любом отдельно взятом RAID-контроллере. Это позволяет в любой момент заменять и перераспределять диски после организации массива. Для перемещения дисков необходимо отключить питание сервера (и всех системных компонентов); в результате перемещения к одному контроллеру не должно быть подключено более 32 логических дисков (томов); кроме того, массив должен сохранить свои первоначальные настройки и в нем не должно быть активных резервных дисков. Также на RAID-контроллере должно быть установлено новейшее микропрограммное обеспечение. Выполнив все перечисленные условия, сделайте следующее.

Примечание

Всякий раз, когда вы перемещаете диски или вносите изменения в настройки RAID, следует проводить полное резервирование всех данных.

1. Отключите питание системы.
2. Переместите диски так, как запланировано.
3. Возобновите подачу электропитания в систему.
4. Запустите утилиту настройки RAID-контроллера, чтобы просмотреть и проверить настройки новых дисков.

Сообщение об ошибке (сообщение POST 1724) должно указывать на изменение положения дисков и обновление настроек. При появлении сообщения об ошибке "настройка не выполнена" (сообщение POST 1785) немедленно выключите систему, чтобы предотвратить потерю данных, и переставьте диски в их первоначальное положение.

Перемещение массивов между контроллерами

Вы можете перемещать целые дисковые массивы с одного контроллера на другой, а также объединять массивы, ранее организованные на нескольких контроллерах, в рамках одного контроллера. Для перемещения массивов необходимо отключить

питание сервера (и всех системных компонентов); в результате перемещения к одному контроллеру не должно быть подключено более 32 логических дисков (томов); кроме того, дисковый массив должен сохранить свои первоначальные настройки, и в нем не должно быть активных резервных дисков. Также на RAID-контроллере должно быть установлено новейшее микропрограммное обеспечение. Необходимо сразу переместить все диски массива, но их положение на контроллере назначения на этом этапе изменять нельзя. Выполнив все перечисленные условия, сделайте следующее.

1. Отключите питание системы.
2. Переместите массивы так, как запланировано (необходимо переместить все диски массива).
3. Возобновите подачу в систему электропитания.
4. Запустите утилиту настройки RAID-контроллера, чтобы просмотреть и проверить новые настройки дисков.

Сообщение об ошибке (сообщение POST 1724) должно указывать на добавление логических дисков к конфигурации и обновление настроек. При появлении сообщения об ошибке "настройка не выполнена" (сообщение POST 1785) немедленно выключите систему, чтобы предотвратить потерю данных и верните диски в их первоначальное положение. Если вы переводили массивы с многоканального контроллера на одноканальный, то, возможно, на экране появится сообщение об ошибке настройки. В таком случае сделайте следующее.

1. Возвратитесь к предыдущим настройкам многоканального контроллера.
2. Создайте резервные копии всех данных массива.
3. Переведите диски с многоканального контроллера на одноканальный.
4. Чтобы настроить массив, запустите утилиту настройки RAID-контроллера на одноканальном RAID-контроллере.
5. Восстановите данные в перемещенный массив.
6. Чтобы просмотреть и проверить новые настройки дисков или назначить резервные диски, запустите утилиту настройки RAID-контроллера.

Примечание

Если какие-либо диски отсутствуют или вышли из строя, возможна потеря всех данных в перемещенном массиве. Всякий раз, когда вы перемещаете массивы или вносите изменения в настройки RAID, следует проводить полное резервирование всех данных.

Рассмотрим систему с двумя RAID-контроллерами SCSI (у каждого из них свой дисковый массив). Предположим, что на контроллере 1 существует массив из четырех дисков (с идентификаторами 0, 1, 2 и 3), а на контроллере 2 — массив из двух дисков (с идентификаторами 0 и 1). Если вы переместите массив с контроллера 2 на контроллер 1, на контроллере 1 будет присутствовать массив А из четырех дисков (с идентификаторами 0, 1, 2 и 3) и массив В из двух дисков (после перераспределения у них будут идентификаторы 4 и 5). На контроллере 2 массивов не будет вообще.

Примечание

Во время этой процедуры вы можете добавить в массив резервный диск, но он не будет рассматриваться в роли резервного до тех пор, пока вы не запустите утилиту настройки RAID-контроллера.

Восстановление массива

Вы можете не только переместить массив, но и восстановить его на первоначальном контроллере в случае возникновения неисправностей на сервере, связанных с массивом или контроллером, или при модификациях сети. Сам процесс восстановления массива довольно прост *(см. разд. "Перемещение массивов между контроллерами" выше)*, но логическая последовательность действий, сопутствующих восстановлению массива на его исходном контроллере (или его перемещению на новый RAID-контроллер в случае выхода из строя старого), более сложна. Для восстановления массива необходимо отключить питание сервера (и всех системных компонентов); в результате перемещения к одному контроллеру не должно быть подключено более 32 логических дисков (томов); кроме того, массив должен сохранить свои первоначальные настройки, и в нем не должно быть активных резервных дисков. На RAID-контроллере должно быть установлено новейшее микропрограммное обеспечение. Выполнив все перечисленные условия, сделайте следующее.

Примечание

Приведенные ниже действия следует воспринимать лишь как общее руководство. Для получения конкретных инструкций для вашей серверной платформы и RAID-контроллера обратитесь к сопровождающей их документации. Любое отступление от инструкций производителя может привести к потере всех данных во всех перемещаемых массивах.

1. Отключите питание системы.
2. Переместите массив на его исходный контроллер (необходимо переместить все диски этого массива), но сохраните расположение дисков, характерное для данной конфигурации.
3. Восстановите подачу в систему электропитания.
4. Каждый из контроллеров будет сообщать об ошибке "отсутствующие диски" (сообщение POST 1789). Нажмите клавишу <F2>.
5. Для удаления массивов, потерявших работоспособность, запустите утилиту настройки RAID-контроллера.
6. Перезагрузите сервер.

Рассмотрим RAID-контроллер SCSI с массивом A, состоящим из четырех дисков (с идентификаторами 0, 1, 2 и 3), и массивом B, состоящим из двух дисков (с идентификаторами 4 и 5). При перемещении массива B обратно на контроллер 2 образуется промежуточное наличие четырех массивов — массив B на контроллере 1 и массив A на контроллере 2 сервер считает вышедшими из строя. Для удаления вышедших из строя массивов и восстановления исходной конфигурации из двух массивов вы должны запустить утилиту настройки RAID-контроллера.

Инструкции по обновлению/замене RAID-контроллера

Работая с сетями и сетевыми серверами, вам, вероятно, придется производить замену RAID-контроллера с целью обновления или ремонта системы. Процесс обновления контроллера в значительной степени зависит от его модели, поэтому в данном разделе представлены лишь некоторые общие инструкции для типичного RAID-контроллера SCSI (SmartArray 4250ES), которые помогут вам при обновлении оборудования. Всякий раз, прежде чем приступать к обновлению, создайте копию данных дискового массива. Обязательно проверьте наличие резервных копий и лишь после этого переходите к выполнению следующих действий.

Примечание

Если вы устанавливаете контроллер более современной модели, учтите, что старые драйверы не смогут обеспечить его корректную работу. Прежде чем заменять старый контроллер, необходимо установить драйверы для нового контроллера.

1. Запустите утилиту настройки системы сервера и запишите номер контроллера, с которого осуществляется загрузка, — эта информация обеспечит корректную загрузку сервера после установки новых устройств.
2. Убедитесь в том, что на сервере установлена последняя версия BIOS (при необходимости обновите BIOS).

   Переходите к инструкциям для вашей операционной системы и проверьте правильность загрузки драйверов. Выполнив эту задачу, возвращайтесь к выполнению следующих шагов.
3. Проверьте, отключен ли сервер.
4. Замените старый контроллер на новый.
5. Вставьте в дисковод компакт-диск с драйверами контроллера, включите сервер и запустите утилиту настройки системы сервера.
6. Проверьте соответствие номера контроллера, с которого осуществляется загрузка, вашим записям из шага 1. Вместо старого контроллера теперь должен появиться новый.
7. Сохраните все изменения, произведенные утилитой настройки системы.
8. Перезагрузите сервер и извлеките из дисковода компакт-диск с драйверами. На этом физическое обновление завершается.
9. Убедитесь в том, что все диски распознаются операционной системой так же, как и раньше, и что все работает нормально.
10. Если в вашей системе больше нет контроллеров массивов предыдущих версий, удалите старый драйвер контроллера — как правило, в этой ситуации появляются сообщения об ошибках и запрос на удаление драйвера.

Windows NT 4.0

Если вы используете операционную систему Windows NT, сделайте следующее.

1. Запустите Disk Administrator в Windows NT и присвойте дискам сигнатуры. Это гарантирует, что в процессе обновления оборудования буквенные обозначения

дисков не изменятся. После завершения обновления запустите Disk Administrator еще раз и убедитесь в том, что все данные на дисках сохранены.

2. Вставьте в дисковод компакт-диск с драйверами для нового контроллера и установите последние версии программ контроллера для Windows NT. Не перезагружайте систему (особенно если получите запрос о перезагрузке).
3. Чтобы вручную установить все новые драйверы с компакт-диска контроллера, откройте **Control Panel**, затем **SCSI Adapters** и **Have Disk**. Перейдите к файлу .INF, относящемуся к вашей модели контроллера. После выбора нужного контроллера (или семейства контроллеров) нажмите кнопку **OK**.
4. Войдите в ту же папку на компакт-диске, выберите **Open** и нажмите кнопку **OK**. Произойдет установка новых драйверов.
5. Выключите питание сервера.
6. Возвращайтесь к общим инструкциям, данным выше.

NetWare 4.2 и 5

Если вы пользуетесь операционной системой NetWare, сделайте следующее:

1. Включите дисковод для компакт-дисков. Если драйверы для него еще не загружены, введите в системной консоли `load cdrom` и нажмите клавишу <Enter>. После загрузки драйвера для CD-ROM введите в системной консоли `cd mount all` (только для NetWare 4.x) и нажмите клавишу <Enter>. В NetWare 5 монтаж компакт-диска через несколько секунд произойдет автоматически.
2. В системной консоли введите `volumes` и нажмите клавишу <Enter>. Запишите имя тома контроллера (например, CPQSMST430).
3. Обратитесь к имеющимся файлам драйверов. К примеру, в системной консоли введите `load cpqsmst430:cpqsupsw\nssd\install\cpqnssu` и нажмите клавишу <Enter>. Если нужно, замените ссылку `CPQSMST430` именем тома компакт-диска вашего нового контроллера.
4. Откройте список имеющихся файлов для вашего контроллера и согласно инструкциям к контроллеру выберите нужные файлы.
5. Выберите пункт **Install Selected Files** и нажмите клавишу <Enter>. Файлы драйвера будут скопированы в SYS:SYSTEM и C:\NWSERVER. После завершения копирования файлов нажмите клавишу <Enter>.
6. В появившемся окне выберите **Return To Main Menu** и нажмите клавишу <Enter>.
7. В главном меню выберите **Exit** и нажмите клавишу <Enter>. При появлении приглашения выберите **YES** и нажмите <Enter>.
8. В системной консоли введите `down` и нажмите клавишу <Enter>. Если нужно, введите `exit` и нажмите клавишу <Enter>, чтобы вернуться в командную строку DOS.
9. Оставьте диск с драйверами в дисководе.
10. Отключите питание сервера.
11. Возвращайтесь к общим инструкциям, представленным выше.

UnixWare 7.x

Если в качестве операционной системы вы используете UNIX, сделайте следующее:

1. С помощью SCO проверьте, нужно ли установить новые системные заплаты и установите их.
2. Загрузите компакт-диск с драйверами и выберите **Create Support Software**, чтобы создать набор дискет EFS. Выберите SCO UnixWare EFS и следуйте инструкциям.
3. Чтобы обновить драйвер IDA с дискеты HBA, введите `pkgadd -d diskette1 ida`. Это позволит обновить драйвер для нового контроллера, но также рекомендуется всегда устанавливать оставшуюся часть EFS 7.26.
4. Выполните повторную компоновку ядра и выключите сервер.
5. Возвращайтесь к общим инструкциям, представленным выше.

Инструкции по обновлению микропрограммного обеспечения контроллера

Время от времени серверы и факультативные устройства — такие как RAID-контроллер — должны получать обновление своих микропрограммных средств. Эти обновления действенно исправляют дефекты в предыдущих версиях микропрограммного обеспечения, решают вопросы несовместимости аппаратной части или операционной системы и реализуют новые возможности по мере их появления. Как правило, микропрограммное обеспечение хранится в микросхеме Flash BIOS (на большинстве современных материнских плат) и может быть без труда перепрограммировано с помощью утилиты флэш-загрузчика. Например, в линейке серверов и контроллеров Compaq обычно используется утилита ROMPaq. Так как перепрограммирование можно выполнить с помощью программных средств и файлов, обновления можно бесплатно скачать из Интернета, а затем установить, не открывая сервер и не снимая устройства расширения. На серверах Compaq ProLiant используются две утилиты ROMPaq:

Примечание

Прежде чем устанавливать на сервере новый RAID-контроллер, обновите BIOS.

- System ROMPaq. Эта утилита обновляет BIOS на всех серверах Compaq, поддерживающих флэш-память. Ей можно воспользоваться при установке нового RAID-контроллера на сервере Compaq, чтобы убедиться в том, что сервер реализует все возможности контроллера.
- Options ROMPaq. Эта утилита обновляет встроенное ПЗУ всех факультативных устройств Compaq, поддерживающих флэш-программирование. Ей можно воспользоваться при появлении новых версий микропрограммного обеспечения RAID-контроллера Compaq или диска SCSI, чтобы реализовать их дополнительные возможности.

Примечание

Если на вашем сервере установлено два RAID-контроллера (первичный и вторичный), проверьте, чтобы установленные на них версии микропрограммного обеспече-

ния совпадали. Функция резервирования контроллера работает только в том случае, если на обоих контроллерах установлены одинаковые версии микропрограммного обеспечения.

Создание дискет ROMPaq

Практически во всех случаях флэш-обновление производится с одной или нескольких дискет, которые можно создать при первой необходимости. Рассмотрим типичный процесс создания и применения дискет ROMPaq для серверов Compaq ProLiant и факультативных устройств. Чтобы создать дискету (дискеты) с утилитой ROMPaq, вам понадобится компакт-диск с драйверами RAID-контроллера (например, компакт-диск для Compaq SmartArray 4250ES), одна чистая дискета (для System ROMPaq) или до пяти чистых дискет (для Options ROMPaq), в зависимости от вашего сервера. Кроме того, вам нужен доступ к серверу или рабочей станции с загрузочным диском. Это может быть компьютер, в который вы собираетесь установить новый RAID-контроллер. Для создания дискет ROMPaq выполните следующие действия.

Примечание

Обратите внимание, что приведенная здесь последовательность действий является всего лишь примером. Подробные инструкции по флэш-обновлению можно получить из документации к вашему серверу и факультативным устройствам.

1. Загрузите сервер с компакт-диска Compaq.
2. В окне **Compaq System Utilities** выберите **Create Support Software**.
3. В окне **Diskette Builder** выберите либо **System ROMPaq**, либо **Options ROMPaq**.
4. Чтобы завершить создание дискет ROMPaq, следуйте инструкциям на экране.

Использование дискет System ROMPaq

Утилита System ROMPaq выполняет обновление BIOS на серверах Compaq (например, в линейке ProLinea). Если вы собираетесь установить новое устройство с расширенными возможностями (например, Compaq SmartArray 4250ES), то на вашем сервере должно быть установлено обновленное микропрограммное обеспечение, чтобы ваш сервер смог ими воспользоваться. Бывает трудно установить, когда нужно обновить микропрограммное обеспечение, поэтому при установке любого нового устройства на всех серверах следует запустить последнюю версию System ROMPaq. Чтобы запустить дискету System ROMPaq, сделайте следующее:

1. Вставьте дискету с System ROMPaq в дисковод сервера.
2. Загрузите сервер, включив его электропитание.
3. При появлении окна **Welcome** нажмите клавишу <Enter>.
4. В окне **Select A Device** выберите в списке программируемых устройств ваш сервер (возможно, он будет единственным элементом списка) и нажмите клавишу <Enter>.
5. В окне **Select An Image** вы сможете просмотреть данные о перепрограммируемых устройствах, а также текущую и последнюю версию ПЗУ. Нажмите клавишу <Enter>.

6. Проверьте информацию в окне **Caution**, а затем, чтобы перепрограммировать системное ПЗУ, нажмите клавишу <Enter>. Нажав клавишу <Esc>, вы можете отменить перепрограммирование и вернуться к экрану **Select An Image**.
7. Сообщение "Reprogramming Firmware" ("Перепрограммирование микропрограммного обеспечения") указывает на то, что системное ПЗУ находится в процессе перепрограммирования. Прерывать этот процесс нельзя, иначе система BIOS может быть повреждена. После завершения перепрограммирования вы получите соответствующее уведомление.
8. После того как ROMPaq завершит перепрограммирование системного ПЗУ, нажмите клавишу <Esc>, чтобы выйти из утилиты System ROMPaq.
9. Извлеките из дисковода дискету с System ROMPaq и перезагрузите сервер, выключив и немедленно включив электропитание (холодная перезагрузка сервера).
10. Если новые факультативные устройства (например, SmartArray 4250ES) еще не установлены, это можно сделать сейчас.

Использование дискет Options ROMPaq

Утилита Options ROMPaq выполняет обновление микропрограммного обеспечения факультативных устройств Compaq (типа Compaq SmartArray 4250ES). Бывает трудно уставить, когда нужно обновить микропрограммное обеспечение, поэтому при появлении новых обновлений запустите последнюю версию Options ROMPaq на всех устройствах. Чтобы запустить утилиту Options ROMPaq с дискеты, сделайте следующее:

1. Вставьте дискету #1 Options ROMPaq в дисковод сервера.
2. Загрузите сервер, включив его электропитание.
3. При появлении экрана **Welcome** нажмите клавишу <Enter>.
4. В окне **Select A Device** выберите из списка программируемых устройств то, которое вам нужно (например, **ALL COMPAQ SmartArray 4250ES**), и нажмите клавишу <Enter>.
5. Если на устройстве установлена та же или более современная версия микропрограммного обеспечения, чем версия на дискете Options ROMPaq, вы увидите сообщение "Обнаруженные файлы ПЗУ для выбранного устройства не являются более новыми, чем текущие" ("The ROM image files found for the device selected are not newer than the current ROM image"). Чтобы пропустить следующие три этапа, нажмите клавишу <Enter>.
6. Если на устройстве установлена более старая версия микропрограммного обеспечения по сравнению с версией на дискете Options ROMPaq, вы увидите экран **Select An Image** со списком устройств, которые предполагается перепрограммировать, а также данными о текущей и новой версиях ПЗУ. Нажмите клавишу <Enter>.
7. Просмотрите информацию, которая содержится на экране **Caution**, а затем нажмите клавишу <Enter>, чтобы перепрограммировать системное ПЗУ. Нажав клавишу <Esc>, вы можете отменить перепрограммирование и вернуться к экрану **Select An Image**.

8. Сообщение "Перепрограммирование микропрограммного обеспечения" ("Reprogramming Firmware") указывает на то, что системное ПЗУ находится в процессе перепрограммирования. Прерывать этот процесс нельзя, иначе микропрограммное обеспечение может быть повреждено. После завершения перепрограммирования вы получите соответствующее уведомление.
9. После того как утилита ROMPaq завершит перепрограммирование системного ПЗУ, нажмите клавишу <Esc>, чтобы выйти из утилиты System ROMPaq.
10. Извлеките из дисковода дискету с System ROMPaq и перезагрузите сервер путем выключения и немедленного включения электропитания (холодная перезагрузка сервера).

Поиск и устранение неисправностей RAID

В целом, RAID-контроллеры и серверы считаются одними из наиболее надежных современных аппаратных компонентов компьютера. Функции обеспечения отказоустойчивости большинства современных RAID-контроллеров позволяют произвести замену неисправных жестких дисков без потери данных (а часто даже без отключения питания сервера). Однако и дисковые массивы, и контроллеры тоже могут послужить причиной сбоев, а действия, предпринятые незамедлительно после возникновения неисправности, могут обеспечить сохранность ваших данных. В этой части главы рассмотрим методы выявления и устранения неисправностей дисков, а также различные неисправности RAID-контроллеров. Первым этапом восстановления после выхода из строя диска является выявление неисправности. В большинстве систем выход из строя диска обнаруживается следующим образом.

- Операционная система (или сетевая консоль) выводит сообщение о неисправности логического диска.
- На отсеке для дисков с горячим подключением на неисправных дисках горит светодиод.
- На передней панели сервера (типа Compaq ProLiant) горит светодиод, если неисправные диски расположены внутри корпуса, хотя это может свидетельствовать и о других сбоях, типа неисправности вентилятора или состоянии перегрева.
- Всякий раз при включении питания сервера появляется сообщение POST с указанием всех неисправных дисков.
- Диагностические средства RAID-контроллера, например, утилита ADU (Array Diagnostics Utility — утилита диагностики массива), создает список всех неисправных дисков.

Примечание

Сообщения операционной системы о снижении производительности системы или общих ошибках дисков не обязательно указывают на то, что диск вышел из строя. Для проверки воспользуйтесь средствами диагностики массива.

Управление отказами диска

Сервер сообщает о том, что диск вышел из строя. В зависимости от уровня отказоустойчивости, сеть при этом может функционировать, а может быть отключена.

В любом случае вам нужно немедленно попытаться устранить неисправность и предотвратить дальнейшую потерю данных. Если настройки вашего RAID-контроллера предусматривают поддержку аппаратных средств обеспечения отказоустойчивости, то для устранения неисправностей выполните следующее.

1. Найдите неисправный диск. Как правило, операционная система сообщает о сбое логического диска, но вам нужно выявить неисправный физический диск. Если на сервере (например, Compaq ProLiant) есть диски с горячим подключением, на их неисправность указывает светодиод (желтый светодиод неисправности диска на каждом лотке).
2. Оцените необходимость в отключении сервера. Если сервер, в котором находится неисправный диск, не поддерживает диски с горячим подключением, вам придется выключить сервер в обычном порядке. Если сервер поддерживает диски с горячим подключением, то сервер выключать не нужно.
3. Замените неисправный диск. Извлеките неисправный диск и замените его новым диском такой же емкости. На диске с горячим подключением светодиоды поочередно мигнут (после того, как диск установлен в отсеке). Это означает что соединение установлено. Светодиод состояния (если он установлен на сервере) в этом случае мигает, указывая на то, что контроллер распознал замену диска и начал процесс восстановления.
4. Перезагрузите сервер. Включите питание сервера (если необходимо).
5. Подождите, пока завершится процесс восстановления. Микропрограммное обеспечение RAID-контроллера восстановит информацию на новом диске, основываясь на данных остальных физических дисков в логическом дисковом массиве. При восстановлении на дисках с горячим подключением их светодиод состояния мигает. После завершения восстановления светодиод состояния начинает светиться в постоянном режиме.

В случае неисправности диска состояние соответствующего логического диска зависит от выбранного уровня отказоустойчивости. Так как в одном массиве физических дисков может содержаться несколько логических дисков с разными методами обеспечения отказоустойчивости, состояние отдельных логических дисков в рамках массива не обязательно одинаково. Если из строя выходят несколько дисков одновременно, что не предусмотрено уровнем отказоустойчивости, то отказоустойчивость признается неэффективной, а логический диск — неисправным. Если из строя вышел логический том, то все запросы операционной системы на получение доступа к этому логическому диску отклоняются по причине ошибки данных. Отклик системы на неисправности, как показано ниже, зависит от выбранного уровня RAID.

- RAID 0 (чередование). На уровне RAID 0 отказоустойчивость отсутствует, и дисковый массив не защищен от любых неисправностей дисков. Если один физический диск в дисковом массиве выйдет из строя, то все неотказоустойчивые логические диски в этом массиве также будут неисправны. Причиной этого является то, что данные расслаиваются по всем дискам массива.
- RAID 1 (зеркальное копирование). При таком типе отказоустойчивости неисправный диск заменяется на его копию. Зеркальное копирование обеспечивает восстановление нескольких неисправных дисков (за исключением случаев, когда оба неисправных диска являются копирующей парой). После замены неисправ-

ного диска, а также в случае активизации резервного диска, занимающего место неисправного диска RAID 1 пытается восстановить данные.

- Резервные диски. В случае выхода диска из строя резервный диск немедленно занимает его место (это происходит, если он назначен резервным и доступен). В процессе автоматического восстановления данных данные восстанавливаются с оставшихся дисков тома и записываются на резервный диск. После завершения создания резервного диска логический диск продолжает работать при полной отказоустойчивости и может справиться с любой последующей неисправностью дисков. Но если выход из строя другого диска произойдет до полного завершения создания резервного диска, резервный диск не сможет предотвратить потерю работоспособности логического диска. Кроме того, следует учесть, что неисправимые ошибки дисков способны помешать завершению процесса автоматического восстановления данных.

О замене дисков

Как правило, неисправные диски, установленные в лотках с возможностью горячего подключения, можно извлечь и заменить в условиях включенного питания системы и запоминающего устройства (диски с горячим подключением можно заменять и при отключенном питании). Но ни в коем случае нельзя отключать внешнее запоминающее устройство, если питание сервера включено. Это приводит к сбою всех дисков запоминающей системы, в результате чего отказоустойчивость будет нарушена. Во время установки диска с горячим подключением вся работа дисков в контроллере временно приостанавливается, пока диск раскручивается (около 20 секунд). Если такой диск установить в отказоустойчивой конфигурации при включенном питании сервера, восстановление данных на новом диске начинается автоматически (на это обычно указывает мигание светодиода). Замена дисков без горячего подключения должна производиться только при отключенном питании системы.

Чтобы убедиться в том, что вы собираетесь заменить именно тот диск, который вышел из строя, обязательно проверьте идентификационные перемычки SCSI, которые есть на всех дисках без возможности горячего подключения. Также проверьте, чтобы идентификационные перемычки SCSI были установлены в том же положении на новом диске. Расположение идентификационных перемычек SCSI зависит от модели диска, но они должны занимать одинаковое положение на новом диске и диске, подлежащем замене, что предотвратит возникновение конфликтов идентификаторов SCSI, которые могут нарушить отказоустойчивость.

Емкость новых дисков должна быть по меньшей мере равной емкости других дисков дискового массива. Если емкость нового диска не достаточна, контроллер немедленно забракует этот диск, даже не начиная процесс автоматического восстановления данных.

Примечание

Заменять неисправный диск следует только на новый или заведомо исправный диск. Иногда диск, который контроллер пометил как неисправный, после выключения и немедленного включения системы, а также после извлечения и повторной установки диска с горячим подключением может оказаться действующим. Но применение таких дисков крайне нежелательно, т. к. в конечном итоге из-за этого может произойти потеря данных.

Об автоматическом восстановлении данных (ADR)

Если диск в отказоустойчивой конфигурации заменить при отключенном питании системы, то при последующем запуске системы RAID-контроллер выводит сообщение POST. Это означает, что был обнаружен новый диск и что нужно запустить процесс *автоматического восстановления данных* (Automatic Data Recovery — ADR). Если это не сделать, логический диск остается в состоянии "готовности к восстановлению", и в ходе следующего перезапуска системы на экране появится тот же самый запрос.

До завершения процесса автоматического восстановления данных новые диски не считаются работающими. Любые диски, которые признаны неработающими, рассматриваются как вышедшие из строя при проверке нарушения отказоустойчивости. Например, если на логическом диске RAID 5, в составе которого нет ни одного резервного диска и есть один диск в процессе восстановления, выйдет из строя другой диск, то весь логический диск также выйдет из строя.

Как правило, для восстановления 1 Гбайт данных требуется примерно 15 минут. Фактическое время восстановления зависит от установленного приоритета восстановления по отношению к общему количеству процессов ввода/вывода, происходящих в период восстановления, скорости диска и количества дисков в массиве (RAID 4 и RAID 5). В конфигурациях RAID 4 и RAID 5 время восстановления колеблется от 10 минут на 1 Гбайт данных для трех дисков до 20 минут на 1 Гбайт данных для 14 дисков (при использовании жестких дисков Wide Ultra SCSI емкостью 9 Гбайт каждый).

Сбой автоматического восстановления данных

Если в ходе процесса автоматического восстановления данных светодиод состояния нового диска перестает мигать (в то время как все остальные диски в массиве находятся в рабочем состоянии), это может означать, что процесс был аварийно завершен из-за фатальной ошибки считывания с другого физического диска, которая произошла во время восстановления данных. Фоновый процесс автоматического мониторинга надежности обычно помогает избежать такой ситуации, но в некоторых случаях, например, при нарушении целостности сигнала в шине SCSI он бессилен. Перезагрузите систему, и сообщение POST должно подтвердить диагностику. Попробуйте запустить процесс автоматического восстановления данных еще раз. Если это не помогает устранить неисправность, рекомендуем создать копию всех данных в системе, провести анализ поверхности, а затем возобновить процесс восстановления.

Если в ходе процесса автоматического восстановления данных светодиод состояния нового диска перестает мигать, а новый диск выходит из строя (при этом загорается светодиод неисправности диска или гаснут другие светодиоды), это означает, что на новом диске появились фатальные ошибки. В таком случае следует извлечь новый диск и заменить его другим.

О нарушении отказоустойчивости

Если в результате выхода из строя нескольких дисков отказоустойчивость нарушается, то логический диск рассматривается как неисправный, а на хосте возникают фатальные ошибки, что в большинстве случаев приведет к потере данных. Установка новых дисков на этом этапе не улучшит состояние логического диска. В такой ситуации следует попробовать выключить всю систему, а затем включить ее вновь.

В некоторых случаях после этого нестабильный диск начинает работать (возможно, он будет работать достаточно долго, чтобы создать копии важных файлов).

Отказоустойчивость может нарушиться не только из-за неисправности дисков, причиной может послужить неисправность кабеля, сбой энергоснабжения запоминающей системы или случайное выключение пользователем внешней запоминающей системы при включенном хосте. В таких случаях физические диски заменять не нужно, но потеря данных все же может произойти (особенно если во время возникновения сбоя система была загружена). В случае, если неисправны диски, их следует заменить (после создания копий важных данных). После замены этих дисков отказоустойчивость может быть нарушена повторно, питание нужно будет выключить, а затем снова включить, а вам, вероятно, придется воссоздать разделы и восстановить все данные из резервных копий.

Примечание

Принимая во внимание возможность непредвиденного нарушения отказоустойчивости, необходимо регулярно создавать резервные копии всех логических дисков.

Удаление зарезервированного сектора

При создании любого массива с помощью RAID-контроллера на каждый входящий в него диск помещается зарезервированный сектор. С помощью зарезервированного сектора RAID-контроллер определяет, к какому массиву принадлежит диск. Кроме того, зарезервированный сектор содержит информацию о размещении файлов, необходимую для считывания и записи в массив. Время от времени зарезервированный сектор может быть поврежден или выйти из строя, в результате чего могут возникнуть подобные ситуации:

- невозможно провести успешное разделение и форматирование диска;
- имя тома при попытке удалить раздел с помощью FDISK становится нечитаемым, и завершить удаление невозможно;
- возникают сбои при считывании/записи на диски в массиве (например, фатальные ошибки или повреждение данных);
- во время перезагрузки массив постоянно входит в критический или автономный режим;
- возникают сбои при восстановлении зеркально копированных (RAID 1) и зеркально копированных/чередующихся (RAID 0+1) дисков.

Удаление зарезервированного сектора позволяет устранить большинство неисправностей, имеющих непосредственное отношение к ошибке "Bad Reserve Sector" ("Поврежденный зарезервированный сектор"). Для удаления зарезервированного сектора в среде с IDE RAID-контроллером типа FastTrak 66/100 выполните приведенные далее шаги.

Примечание

Прежде чем пытаться удалить зарезервированный сектор диска, необходимо создать резервную копию всего массива. При удалении зарезервированного сектора на диске, входящем в пару зеркально копированных дисков, следует в первую очередь удалить этот сектор с диска-копии, а на главном диске удалять зарезервированный

сектор нужно лишь в крайнем случае. Если же удалить зарезервированный сектор на любом из чередующихся дисков, то массив станет нефункциональным.

1. При появлении заголовка BIOS контроллера нажмите сочетание клавиш, необходимое для запуска утилиты установки контроллера (например, <Ctrl> + <F>).
2. Выберите **View Drive Assignments** и укажите диск с подозрением на неисправность.
3. Выберите удаление зарезервированного сектора. Появится сообщение о том, что зарезервированный сектор будет стерт. Для подтверждения удаления нажмите клавишу <Y>.
4. Повторите эти действия по отношению ко всем неисправным дискам массива.
5. Завершив выполнение задачи, перезагрузите систему.

Теперь восстановите дисковый массив, проведите его разделение и форматирование. Для настройки массива следует пользоваться FDISK и FORMAT. Перепишите данные из последней резервной копии.

Манипулирование ошибками

Микропрограммное обеспечение большинства RAID-контроллеров по запросу сервера выполняет встроенный процесс POST. Если на контроллере обнаружена ошибка, система выводит на экран соответствующий код POST, с помощью которого вы можете быстро расшифровать ошибку. В табл. 11.2 приводятся коды ошибок типичного RAID-контроллера и предлагаются действия по их исправлению.

Примечание

Подробные расшифровки кодов ошибок и решения по их устранению вы можете найти в документации к вашей модели RAID-контроллера.

Таблица 11.2. *Указатель типичных POST-кодов RAID-контроллера*

Сообщение	Описание
1702. SCSI Cable Error Detected. System Halted (Обнаружена ошибка кабеля SCSI. Система приостановлена)	Это сообщение указывает на неисправность, связанную с завершением или кабелем встроенного SCSI-контроллера серверной материнской платы. Проверьте завершение системы SCSI, если нужно, замените сигнальный кабель (кабели) SCSI
1720. Slot "x" Drive Array — SMART Hard Drive Detects Imminent Failure SCSI: Port "y": SCSI ID "x" (Дисковый массив на слоте "x" — жесткий диск SMART Hard Drive обнаружил предстоящий сбой SCSI: порт "y": идентификатор SCSI "x")	Указанный диск сообщил о состоянии прогнозирования ошибки SMART — в неопределенном будущем этот диск может выйти из строя. Если этот диск является частью неотказоустойчивой конфигурации, срочно создайте копию всех данных, замените диск, а после этого восстановите все данные. Если данный диск является частью отказоустойчивой конфигурации, то замените его при условии, что все остальные диски в массиве находятся в рабочем состоянии

***Таблица 11.2** (продолжение)*

Сообщение	Описание
1722. Slot "x" Drive Array — Redundant Controller Pair Not Operating Redundantly (Дисковый массив на слоте "x" — резервированная пара контроллеров работает вне режима резервирования)	Как правило, причиной этого является либо несовместимость моделей RAID-контроллеров, либо сбой связи между ними. В любом случае, RAID-контроллеры работают ненадлежащим образом. В рамках резервированной конфигурации модели обоих контроллеров должны быть одинаковы. Если это так, один из контроллеров или материнская плата неисправны и нуждаются в замене, или же на двух контроллерах установлены различные версии микропрограммного обеспечения, которые следует обновить. Наконец, возможно, что на платах ускорителей массивов установлен различный размер ОЗУ. Убедитесь в том, что при работе в режиме резервирования в обоих контроллерах установлены одинаковые ускорители
1723. Slot "x" Drive Array — SCSI Connection Problem (Дисковый массив на слоте "x" — неисправность соединения SCSI)	Для улучшения целостности сигнала при подключении внешних дисков в порт SCSI, на котором установлен внутренний SCSI-коннектор, этот коннектор нужно извлечь. Попробуйте отсоединить от RAID-контроллера интерфейсную плату внутреннего порта SCSI. Попытайтесь заменить двухконнекторную внутреннюю интерфейсную плату SCSI одноконнекторной. Попробуйте переустановить внутреннюю интерфейсную плату SCSI в порт 2 (при этом питание системы должно быть отключено). Попытайтесь переместить внешний кабель SCSI на порт 2 (питание системы должно быть отключено)
1724. Slot "x" Drive Array — Physical Drive Position Changes(s) Detected (Дисковый массив на слоте "x" — обнаружены изменения в расположении физического диска)	Это сообщение указывает на то, что после изменения расположения физического диска настройки логического диска были автоматически обновлены. Возможно, вы неправильно переустановили один или несколько дисков или неправильно назначили идентификаторы SCSI
1726. Slot "x" Drive Array — Array Accelerator Memory Size Change Detected (Дисковый массив на слоте "x" — обнаружены изменения объема памяти ускорителя массива)	Это сообщение указывает на то, что вследствие замены одного ускорителя массива (или контроллера) другим, с несовпадающим объемом памяти, произошло автоматическое обновление настроек ускорителя массива. Возможно, вам придется связать RAID-контроллер с подходящим ускорителем — в особенности при использовании согласованных RAID-контроллеров

Таблица 11.2 (продолжение)

Сообщение	Описание
1727. Slot "x" Drive Array — New Logical Drive(s) Attachment Detected (Дисковый массив на слоте "x" — обнаружено подключение нового логического диска (дисков))	При наличии более 32 логических дисков после этого сообщения должно последовать другое: "Auto-configuration failed: Too many logical drives" ("Автоконфигурация не выполнена: слишком много логических дисков"). Это сообщение указывает на то, что контроллер обнаружил дополнительный дисковый массив, который был подключен во время отключения питания системы. Информация о добавлении новых логических дисков была включена в настройки логического диска, но система поддерживает не более 32 логических дисков, поэтому дополнительные логические диски в конфигурацию добавлены не будут
1729. Slot 1 Drive Array — Disk Consistency Initialization in Progress (Дисковый массив на слоте 1 — выполняется инициализация согласованности дисков)	Производительность RAID 4 и RAID 5 может быть пониженной до тех пор, пока в процессе автоматического мониторинга надежности не будет завершена автоматическая фоновая инициализация согласованности по четности. Это сообщение обычно появляется после начальной настройки логических дисков RAID 4 или RAID 5. Данное сообщение POST об ошибке исчезает (а производительность контроллера повышается) после завершения инициализации данных четности в процессе автоматического мониторинга надежности
1762. Redundant Controller Operation is not Supported in this Firmware Version (Данная версия микропрограммного обеспечения не поддерживает работу контроллера в режиме резервирования)	При использовании двух RAID-контроллеров в одной системе версии их микропрограммного обеспечения должны быть одинаковыми. Удалите резервный RAID-контроллер или обновите его микропрограммное обеспечение. До устранения этого несоответствия контроллер будет оставаться заблокированным
1763. The Array Accelerator Card Is Detached — Please Reattach (Плата ускорителя массива отключена — пожалуйста, подключите ее)	Плата ускорителя на контроллере отсоединена или неисправна. Подключите или замените ускоритель. До устранения этой неисправности RAID-контроллер будет оставаться заблокированным
1764. Slot "x" Drive Array — Capacity Expansion Process Is Temporarily Disabled (Дисковый массив на слоте "x" — процесс наращивания емкости временно заблокирован)	Наращивание емкости дискового массива невозможно. В большинстве случаев причина этого заключается в том, что ускоритель массива отсоединен или неисправен. Проверьте установку ускорителя или замените его. Кроме того, возможно, что резервный аккумулятор ускорителя заряжен не полностью, и вплоть до завершения его подзарядки ускоритель будет недоступен.

***Таблица 11.2** (продолжение)*

Сообщение	Описание
(прод.)	Кроме того, процесс наращивания может быть прерван до завершения автоматического восстановления данных (ADR). Если ускоритель массива был извлечен, то для того, чтобы продолжить наращивание емкости, ускоритель нужно переустановить
1766. Slot "x" Drive Array Requires System ROM Upgrade (Дисковый массив на слоте "x" требует обновления ПЗУ)	Загрузите и установите на сервере последнюю версию BIOS
1768. Slot "x" Drive Array — Resuming Logical Drive Expansion Process (Дисковый массив на слоте "x" — возобновление процесса наращивания логического диска)	Такое сообщение появляется, если во время наращивания массива происходит сброс контроллера или выключение электропитания с его последующим включением
1769. Slot "x" Drive Array — Drive(s) Disabled Due to Failure During Expansion (Дисковый массив на слоте "x" — диск заблокирован вследствие сбоя в процессе наращивания)	В процессе наращивания массива данные были потеряны, из-за чего диски были временно заблокированы. Процесс наращивания был прекращен вследствие появления фатальных ошибок диска или ошибок ускорителя массива. Ускоритель массива неисправен или был извлечен, и данные процесса наращивания, возможно, потеряны. Зафиксируйте, что данные потеряны, разблокируйте логические диски, а затем восстановите данные с резервной копии. Если ускоритель массива неисправен, то после прекращения процесса наращивания замените ускоритель. **Внимание!** Ни в коем случае не отключайте систему и не заменяйте плату ускорителя в процессе расширения емкости
1774. Slot "x" Drive Array — Obsolete Data Found in Array Accelerator (Дисковый массив на слоте "x" — в ускорителе массива обнаружены устаревшие данные)	Данные, находящиеся на ускорителе, устарели по сравнению с данными на дисках, поэтому устаревшие данные были удалены. Это случается, если диски сначала отсоединили, затем использовали на другом контроллере и подключили вновь. Возможно, вам придется очистить ускоритель массива, а затем перезагрузить данные из резервных копий
1775. Slot "x" Drive Array — Storage System Not Responding (Дисковый массив на слоте "x" — запоминающая система не отвечает)	Проверьте выключатель электропитания и кабели запоминающей системы. Отключите электропитание системы при проверке разъемов питания и кабелей, а затем возобновите подачу электроэнергии. Помните, что питание на внешние диски необходимо подключать раньше, чем питание системы или одновременно с ним

Таблица 11.2 (продолжение)

Сообщение	Описание
1776. Slot "x" Drive Array — SCSI Bus Termination Error (Дисковый массив на слоте "x" — ошибка завершения шины SCSI)	Внешний и внутренний диски нельзя одновременно подключить к одному порту SCSI. К дискам подсоединены как внутренний, так и внешний коннекторы SCSI-порта (портов). Впрочем, при одновременном подключении к одной и той же шине SSI внешнего и внутреннего диска завершение этой шины происходит ненадлежащим образом. Пока эта неисправность не будет устранена, шина SCSI блокируется. Отключите питание сервера и проверьте кабели и завершение данного порта SCSI
1777. Slot "x" Drive Array — Server Storage Enclosure Problem Detected (Дисковый массив на слоте "x" — Обнаружена неисправность корпуса памяти сервера)	Произошел серьезный сбой управления корпусом сервера, и на экране могут появиться дополнительные сообщения об ошибке типа: *Cooling Fan Malfunction Detected (Обнаружена неисправность охлаждающего вентилятора). *Overheated Condition Detected (Обнаружено состояние перегрева). *Side-Panel Must Be Closed to Prevent Overheating (Во избежание перегрева боковая панель должна быть закрыта). *Redundant Power Supply Malfunction Detected (Обнаружена неисправность резервного энергоснабжения). *Wide SCSI Transfer Failed SCSI Port "y": Interrupt Signal Inoperative (Широкая передача SCSI не выполнена, порт "y" SCSI: сигнал прерывания недействителен). Чтобы проверить работоспособность охлаждающего вентилятора, поднесите к нему руку. На серверах типа tower и в запоминающих системах следует проверить охлаждающий внутренний вентилятор. Если вентилятор не работает, выявите препятствующие этому факторы и проверьте все внутренние коннекторы. Если боковая панель блока сервера была удалена, установите ее обратно. Проанализируйте возможность сбоя в подаче электропитания. Если светодиод питания запоминающей системы сервера светится оранжевым, а не зеленым, значит, произошел сбой резервного энергоснабжения. Проверьте кабели SCSI. Если сообщение указывает на неисправность кабеля SCSI, обратитесь к инструкциям вашего сервера по проводке кабелей. Если соединения проведены правильно, замените кабели данного порта — при этом вам нужно сделать так, чтобы сообщение POST исчезло

Таблица 11.2 (продолжение)

Сообщение	Описание
1778. Slot "x" Drive Array Resuming Automatic Data Recovery Process (Дисковый массив на слоте "x" возобновляет процесс автоматического восстановления данных)	С вашей стороны никаких действий не требуется. Это сообщение появляется в том случае, если в процессе автоматического восстановления данных произошел либо сброс RAID-контроллера, либо выключение и немедленное включение электропитания
1779. Slot "x" Drive Array — Replacement Drive(s) Detected or Previously Failed Drive(s) Now Appear to Be Operational: Port "y": SCSI ID "x" (Дисковый массив на слоте "x" — обнаружены новые диски, или ранее неисправные диски теперь определяются как действующие: порт "y"": идентификатор SCSI "x")	Это сообщение выводится один раз, сразу после замены диска, еще до восстановления данных из резервной копии. После установки нового диска x, заменившего неисправный, данные на нем следует восстановить с помощью резервной копии. Если это сообщение появляется, но диск x (распознаваемый с помощью его идентификатора SCSI) заменен не был, значит, произошел сбой этого диска. Проверьте электропитание диска и проводку сигнального кабеля
1783. Slot "x" Drive Array Controller Failure (Сбой контроллера дискового массива на слоте "x")	Если это сообщение появляется сразу после установки ПЗУ, значит, оно неисправно или плохо установлено. Проверьте подключение платы ускорителя массива и надежность установки RAID-контроллера на слоте. Попытайтесь обновить модули системного ПЗУ. В крайнем случае, замените RAID-контроллер
1784. Slot "x" Drive Array Drive Failure: SCSI Port "y" SCSI ID "x" (Неисправность диска в дисковом массиве на слоте "x": порт SCSI "y", идентификатор SCSI "x")	Указанные диски SCSI следует заменить. В первую очередь проверьте сигнальные кабели и убедитесь в устойчивости электроснабжения. Замените неисправный диск x и/или кабель (кабели)
1785. Slot 1 Drive Array Not Configured (Дисковый массив на слоте 1 не настроен)	К возникновению этой ошибки приводит много различных неисправностей, поэтому, прежде чем что-либо предпринять, необходимо проверить наличие каждой из нижеприведенных неисправностей. • Для настройки RAID-контроллера запустите утилиту настройки массива контроллера. • Ни одного диска не обнаружено. Выключите питание системы и проверьте все кабельные соединения SCSI, чтобы убедиться в исправности подключения дисков. • Объем памяти ускорителя массива был увеличен. Запустите утилиту настройки сервера. • Внешние кабели (кабель) подсоединены не к тем коннекторам портов SCSI. Чтобы не допустить потерю данных, отключите питание системы и поменяйте местами коннекторы портов SCSI.

Таблица 11.2 *(продолжение)*

Сообщение	Описание
(прод.)	• В ходе наращивания емкости расположение дисков изменить нельзя. Отключите питание системы и переставьте диски в соответствии с их исходным расположением (если их предыдущее положение неизвестно, воспользуйтесь расширенными диагностическими средствами дискового массива). • Расположение дисков было изменено. Чтобы предотвратить потерю данных, отключите питание системы и заново подключите диски к их исходному контроллеру. • Данные настройки указывают на расположение дисков, которое не может быть обеспечено средствами данного контроллера. Возможно, причина заключается в том, что диски переместили с контроллера, поддерживающего большее количество дисков, на контроллер, поддерживающий меньшее количество дисков. • Данные настройки свидетельствуют о том, что диски были настроены на контроллере с более современной версией микропрограммного обеспечения. Чтобы предотвратить потерю данных, подключите диски к исходному контроллеру или обновите версию микропрограммного обеспечения данного контроллера до уровня исходного
1786. Slot "x" Drive Array Recovery Needed: SCSI Port "y": SCSI ID "x" or Slot "x" Drive Array Recovery Needed. Automatic Data Recovery Previously Aborted: SCSI Port "y": SCSI ID "x" (Требуется восстановление дискового массива на слоте "x": порт SCSI "y": идентификатор SCSI "x" или требуется восстановление дискового массива на слоте "x": процесс автоматического восстановления данных ранее был прерван: порт SCSI "y": идентификатор SCSI "x")	Указанный диск (диски) SCSI нуждается в проведении автоматического восстановления данных. Вы можете выполнить восстановление данных на диске, но можете и отказаться от него. Обычно это сообщение появляется после замены диска в отказоустойчивой конфигурации при выключенном питании системы. В этом случае вы можете запустить процесс автоматического восстановления данных. Вариант сообщения POST 1786 о прерванном процессе автоматического восстановления данных появляется, если по какой-то причине предыдущая попытка восстановления была прервана (чтобы получить дополнительную информацию, запустите утилиту диагностики массива). Если диск, установленный взамен вышедшего из строя, также неисправен, попробуйте установить другой диск. Если восстановление было прервано из-за ошибки считывания с другого физического диска массива, сделайте копию всех читаемых данных массива, проведите диагностический анализ поверхности, а затем восстановите данные

***Таблица 11.2** (продолжение)*

Сообщение	Описание
1787. Slot "x" Drive Array Operating in Interim Recovery Mode: SCSI Port "y": SCSI ID "x" (Дисковый массив на слоте "x" работает в режиме предварительного восстановления: порт SCSI "y": идентификатор SCSI "x")	Указанные диски SCSI следует заменить. Это сообщение появляется после перезагрузки системы и напоминает вам о неисправности диска x и о применении отказоустойчивости. Замену диска x необходимо произвести как можно скорее. К появлению этой ошибки может привести ненадежное крепление или неисправность кабеля
1788. Slot "x" Drive Array Reports Incorrect Drive Replacement: SCSI Port "y": SCSI ID "x" (Дисковый массив на слоте "x" сообщает о неправильной замене диска: порт SCSI "y": идентификатор SCSI "x")	Указанные диски SCSI нужно было заменить или диски заблокированы из-за их неверной установки. Правильно установите диски. Вы можете либо продолжать работу (дисковый массив останется в заблокированном состоянии), либо перезагрузить систему (все данные будут потеряны). Для получения дополнительной информации следует воспользоваться средствами диагностики массива. Появление ошибки 1788 может быть обусловлено ненадежным подключением к диску силового кабеля или неисправностью кабеля SCSI. Если причиной появления этого сообщения является неисправное соединение силового кабеля, восстановите соединение и продолжайте работу. Если появление этого сообщения не связано с неисправностью силового кабеля и замена диска не производилась, то, вероятно, ошибка указывает на неисправность кабеля SCSI
1789. Slot "x" Drive Array Physical Drive(s) Not Responding: SCSI Port (y): SCSI ID (x) (Физический диск дискового массива на слоте "x" не отвечает: порт SCSI (y): идентификатор SCSI (x))	Это сообщение указывает на отсутствие (или неисправность) ранее действующих дисков после холодной или горячей перезагрузки. Проверьте кабели или замените указанные диски. Вы можете продолжить работу, тогда дисковый массив будет заблокирован, или отказаться от использования дисков, которые не отвечают, тогда если массив настроен на отказоустойчивость, будет активирован режим предварительного восстановления. Отключите систему и проверьте подключение кабелей. Если кабельное соединение исправно, замените диск
1792. Slot "x" Valid Data Found in Array Accelerator (На ускорителе массива обнаружены действительные данные на слоте "x")	Данные автоматически записываются в дисковый массив. Во время работы системы произошел сбой электроснабжения, или произошел перезапуск системы, когда данные находились в памяти ускорителя массива. Затем в течение допустимого периода времени электроснабжение было восстановлено, и данные с ускорителя были благополучно перенесены в дисковый массив

Таблица 11.2 (окончание)

Сообщение	Описание
1793. Slot "x" Drive Array — Array Accelerator Battery Depleted (Дисковый массив на слоте "x" — аккумулятор ускорителя массива разряжен)	Данные с ускорителя массива потеряны (одновременно появляется сообщение об ошибке 1794). Во время работы системы произошел сбой электроснабжения, когда данные находились в памяти ускорителя массива. В течение четырех дней питание не было возобновлено, и данные, находившиеся на ускорителе массива, были потеряны. Проверьте все файлы массива, т. к. данные могли быть повреждены
1794. Slot "x" Drive Array — Array Accelerator Battery Charge Low (Дисковый массив на слоте "x" — низкий заряд аккумулятора ускорителя массива)	Ускоритель массива временно заблокирован. Уровень заряда его аккумулятора ниже 90%, вследствие чего запланированные операции записи запрещены. После полной зарядки аккумулятора ускоритель массива будет автоматически разблокирован, и данное сообщение POST больше появляться не будет. Если резервные аккумуляторы не зарядятся в течение 36 часов (в условиях включенного питания), замените ускоритель массива или RAID-контроллер
1795. Slot "x" Drive Array — Array Accelerator Configuration Error (Дисковый массив на слоте "x" — ошибка конфигурации ускорителя массива)	Данные, хранящиеся на ускорителе массива, не согласованы с дисковым массивом; в результате этого ускоритель массива временно заблокирован. Установите соответствие ускорителя массива дисковому массиву или запустите утилиту настройки RAID-контроллера для удаления данных с ускорителя массива
1796. Slot "x" Drive Array — Array Accelerator Is Not Responding (Дисковый массив на слоте "x" — ускоритель массива не отвечает)	Ускоритель массива временно заблокирован и не отвечает. Замените ускоритель массива или RAID-контроллер
1797. Slot "x" Drive Array — Array Accelerator Read Error Occurred (Дисковый массив на слоте "x" — произошла ошибка считывания с ускорителя массива)	Данные на ускорителе массива потеряны, а сам ускоритель блокирован. Чтобы исправить эту ошибку, следует заменить ускоритель массива или RAID-контроллер, а затем восстановить данные из резервной копии
1798. Slot "x" Drive Array — Array Accelerator Write Error Occurred (Массив дисков на слоте "x" — произошла ошибка записи в ускоритель массива)	Ускоритель массива заблокирован из-за ошибки при записи. Чтобы исправить эту ошибку, следует заменить ускоритель массива или RAID-контроллер
1799. Slot "x" Drive Array — Drive(s) Disabled Due to Array Accelerator Data Loss (Дисковый массив на слоте "x" — диск(и) заблокированы из-за потери данных на ускорителе массива)	Данные, хранившиеся на ускорителе массива, были потеряны, вследствие чего диски были временно заблокированы. Вы можете либо продолжить работу с заблокированными логическими дисками, либо согласиться с потерей данных и разблокировать логические диски. Восстановите потерянные данные с резервных копий

Симптомы неисправностей

В дополнение к общим инструкциям по поиску и устранению неисправностей RAID, представленным выше, рассмотрим несколько конкретных типов неисправностей. В этой части главы представлены многие распространенные неисправности, имеющие отношение к системам RAID.

Симптом 11.1. Система зависает во время поиска устройств SCSI RAID

В большинстве случаев все сводится к неисправности терминирования SCSI (которое должно выполняться на обоих концах шины SCSI). Надежное завершение шины SCSI с обоих концов необходимо для того, чтобы между устройствами, которые на ней установлены, можно было передавать команды и данные. Проверьте терминирование шины SCSI и убедитесь в том, что нагрузка установлена лишь на концах цепочки (т. е. на плате RAID-контроллера и последнем диске SCSI). Проверьте проводку кабелей и надежность их подключения или попробуйте воспользоваться новым высококачественным кабелем SCSI. Каждое устройство SCSI должно иметь собственный уникальный идентификатор SCSI. Устройства, которые система не может распознать, возможно имеют одинаковые идентификаторы с другими устройствами. Проверьте наличие уникального идентификатора у каждого диска (обычно идентификаторы начинаются с ID0).

Симптом 11.2. После установки RAID-контроллера система не загружается

Система может не загружаться по различным причинам, но в большинстве случаев это объясняется ошибками, допущенными при установке контроллера.

- Проверьте основные моменты. В первую очередь следует проверить питание системы, а также надежность монтажа всех кабелей (в особенности кабелей дисков SCSI) и других устройств сервера.
- Проверьте установку устройств. Проверьте, чтобы установка, подключение и настройка контроллера были выполнены в соответствии с инструкциями производителя. Для выполнения полной настройки контроллера на сервере вам нужно выполнить настройку сервера и запустить утилиту настройки.
- Попробуйте сократить систему до минимума. Извлеките все компоненты, кроме минимального объема памяти и процессора (а также платы завершения процессора в многопроцессорных системах), и перезагрузите систему. По возможности проверьте все компоненты в отдельности (особенно процессоры и память) в заведомо исправной системе.
- Проверьте процессоры. Убедитесь в правильности установки процессоров. Если на многопроцессорной материнской плате установлен лишь один процессор, проверьте установку платы завершения процессора.
- Проверьте память. Удостоверьтесь в том, что все модули DIMM надежно установлены и полностью совместимы с материнской платой. К примеру, информацию о памяти, протестированной на модуле памяти Intel L440GX+, можно получить по адресу **support.intel.com/support/motherboards/server/L440GX/compat.htm**.
- Проверьте память ускорителя массива. Проверьте, чтобы на модуле RAID-кэша (он также называется "ускорителем массива") было установлено соответствующее

ОЗУ. К примеру, на контроллере Mylex AcceleRAID 250 применяется кэш-память EDO.

Симптом 11.3. Система не может обеспечить одновременное вращение всех дисков RAID

Жесткие диски потребляют много энергии, и крупная система RAID при одновременном раскручивании большого количества дисков может стать чрезмерной нагрузкой на источник питания (особенно при включении питания). Если диски RAID не вращаются в обычном режиме, что может быть причиной сбоев при загрузке, проверьте настройку RAID-контроллера и настройте систему RAID на вращение меньшего количества дисков или вращение дисков, только когда это необходимо. В некоторых случаях для обеспечения работоспособности большого количества дисков RAID может потребоваться установка второго источника питания (при условии, что корпус сервера и RAID-система поддерживают установку второго источника питания).

Симптом 11.4. При установке RAID-контроллера появляется сообщение об ошибке типа "Система BIOS не установлена"

В любом случае следует начинать с проверки подключенных жестких дисков — обычно эта ошибка появляется, когда ни одного жесткого диска не подключено (или они некорректно настроены). Как правило, данная проблема связана с несовместимостью в рамках центральной системы. Для успешной работы установленного RAID-контроллера PCI центральная система должна поддерживать версию 2.1 (или более позднюю) шины на слоте PCI с возможностью управления передачей данных по шине и современную версию BIOS с поддержкой той же возможности. Ознакомьтесь с документацией к центральной системе или материнской плате и проверьте согласованность в пределах системы. Если аппаратное обеспечение отвечает всем требованиям, свяжитесь с изготовителем системы для получения обновлений BIOS материнской платы.

Симптом 11.5. Возникают сбои при работе с RAID-контроллером IDE

Чаще всего неисправность такого типа возникает при работе с IDE-контроллерами типа FastTrak 100. В большинстве случаев эта неисправность вызвана использованием старой версии микропрограммного обеспечения. Сбои при работе с FastTrak 100 возникают при использовании драйвера версии 1.20 и более ранних версий. Следует обновить драйвер и BIOS до последних версий. Что касается FastTrak 100, загрузить драйвер 1.30 и BIOS версии 1.20 (или выше) можно с сайта **www.promise.com**.

Симптом 11.6. В массиве, созданном с помощью утилиты настройки RAID, задействовано слишком много дисков

Утилита настройки RAID (RAID Configuration Utility) предназначена для организации первого тома RAID. Она автоматически создает массив, используя до восьми доступных дисков, и помещает в массив том. Если вы захотите исключить из первого массива несколько дисков, запустите утилиту настройки RAID и обозначьте их как резервные (или отключите эти диски от SCSI-контроллера и источника питания). После создания с помощью утилиты настройки RAID на оставшихся дисках тома вы можете сделать дополнительные диски оперативными и настроить их посредством управляющего программного обеспечения RAID.

Симптом 11.7. Загрузочное устройство RAID SCSI не найдено

Обычно эта неисправность связана с настройкой сервера. Запустите утилиту CMOS Setup и настройте сервер таким образом, чтобы том RAID определялся как первичное загрузочное устройство (т. е. находился на первой позиции в списке загрузочных устройств). При физическом перемещении платы RAID-контроллера с одного слота PCI на другой, если том RAID управляется платой RAID, некоторые системы автоматически вносят изменения в отдельные настройки BIOS (такие как последовательность загрузочных устройств). Эта неисправность связана с тем, как работает BIOS, и возникает не во всех системах.

Симптом 11.8. Невозможна загрузка с RAID-контроллера типа IDE

Даже при правильной установке RAID-контроллера и его обнаружения системой, загрузка с него бывает невозможной из-за неправильной загрузочной последовательности, неопределенного массива, некорректного выбора массива или неверной записи в CMOS Setup. Всегда проверяйте, чтобы массив был определен. Если он определен, в BIOS контроллера есть опция, которая позволяет сделать массив загрузочным. Убедитесь в том, что применяемый массив отмечен как загрузочный. Для контроллеров типа FastTrak 100 это обозначается звездочкой рядом с номером массива в утилите FastBuild. Если рядом с записью массива звездочки нет, выделите ее и нажмите клавишу <Space>, чтобы сделать массив загрузочным. Если массив уже обозначен как загрузочный, проверьте CMOS Setup центральной системы и убедитесь в том, что в "Disk Drive Sequence", "System BIOS Boot Devices" стоит на первом месте, а "FastTrak RAID Controller" — на втором. Кроме того, проверьте, входит ли в загрузочную последовательность диск C:.

Симптом 11.9. Один из жестких дисков постоянно инициирует перекомпоновку массива или его работу в неоперативном режиме

Практически во всех подобных случаях мы имеем дело с неправильной проводкой кабеля или сбоем диска. К примеру, кабель SCSI может быть дефектным. Перекиньте этот кабель и диск, вызывающий сбои, на другой канал (например, с канала 2 на канал 3). Если в результате неисправность исчезнет, значит, первый канал неисправен — следует заменить RAID-контроллер. В противном случае, вероятно, поврежден кабель и его нужно заменить. Если неисправность остается, попытайтесь заменить жесткий диск.

Симптом 11.10. Не удается обнаружить все диски, подключенные к RAID-контроллеру

В большинстве таких случаев речь идет о некорректном терминировании SCSI (которое нужно выполнять на обоих концах шины SCSI). Надежное завершение шины SCSI с обоих концов необходимо для того, чтобы между устройствами, которые на ней установлены, можно было передавать команды и данные. Проверьте терминирование шины SCSI и убедитесь в том, что нагрузка установлена лишь на концах цепочки (т. е. на плате RAID-контроллера и последнем диске SCSI). Кроме того, проверьте проводку кабелей и надежность их подключения.

Каждое устройство SCSI должно иметь собственный уникальный идентификатор SCSI. "Отсутствующие" устройства, возможно, по ошибке используют те же идентификаторы, что и другие устройства. Проверьте наличие уникальных идентификато-

ров у каждого диска (обычно идентификаторы начинаются с ID0). Наконец, убедитесь в том, что к шине SCSI RAID-контроллера подключены только подходящие для этого диски. К примеру, запоминающие устройства на магнитной ленте и дисководы для компакт-дисков зачастую являются полноценными устройствами RAID, но из-за медленной передачи данных их установка на шине RAID SCSI запрещена — в лучшем случае она приведет к понижению производительности системы RAID. Проверьте, действительно ли на шине RAID SCSI установлены только высокопроизводительные жесткие диски. Если RAID-контроллер предусматривает отдельную шину SCSI для прочих устройств, то дисковод для компакт-дисков, запоминающие устройства на магнитной ленте и другие диски можно установить именно на ней.

Симптом 11.11. Обнаруживается, что диски UDMA случайным образом выпадают из массива

Как правило, это происходит с наиболее быстрыми дисками Ultra-DMA/66 или Ultra-DMA/100. В большинстве случаев RAID-контроллер не полностью соответствует стандартам UDMA 66/100 и не может с достаточной степенью надежности обеспечивать работу таких дисков на самых высоких скоростях передачи данных. Возможно, для усовершенствования поддержки UDMA вам придется обновить RAID-контроллер (или версию его BIOS). С другой стороны, вы можете отключить режим UDMA 66/100 работы дисков в рамках массива — обычно это делается с помощью утилиты от производителя дисков.

Симптом 11.12. Диски в массиве слишком часто выходят из строя

В большинстве случаев эту неисправность рассматривают как логический сбой, который требует восстановить данный диск (что, как правило, в результате приводит к понижению производительности запоминающей системы в процессе восстановления). Убедитесь в надежности проводки кабеля к диску и попробуйте установить новый высококачественный кабель. Если проблема сохранится, замените диск. Обязательно соблюдайте соответствие между новым диском и другими дисками массива.

Симптом 11.13. Видеокарта работает некорректно, несмотря на то, что разделяет ресурсы с RAID-контроллером

Как правило, причиной этого является конфликт на уровне ресурсов. Практически все RAID-контроллеры полностью соответствуют стандарту PnP, так что ресурсы, выделяемые различным устройствам, определяются PnP BIOS на материнской плате. Большинство контроллеров поддерживают совместное использование прерываний PCI, но, если такую поддержку обеспечивают не все задействованные устройства, применение этой техники невозможно. Если ваша материнская плата позволяет управлять назначением этих ресурсов, то вам, возможно, удастся устранить неисправность путем ручного регулирования распределения ресурсов. Кроме того, вы можете попробовать сбросить/очистить запись "PnP Configuration" в CMOS Setup. Если эта настройка блокирована, активируйте ее, затем сохраните изменения и перезагрузите систему. Или вы можете поменять слот PCI платы контроллера и переустановить контроллер на слот с более низким приоритетом.

Симптом 11.14. Сервер не загружается с сопроводительного компакт-диска

После установки RAID-контроллера вы обнаруживаете, что сервер отказывается запускаться с программного компакт-диска материнской платы.

Попробуйте предпринять следующее.

- Проверьте загрузочную последовательность. Возможно, порядок загрузочных приоритетов в BIOS настроен неправильно. Запустите серверную процедуру CMOS Setup (утилиту настройки сервера) и установите загрузочную последовательность таким образом, чтобы первым в списке стоял дисковод для компакт-дисков. Сохраните изменения и перезагрузите сервер.
- Проверьте конфигурацию контроллера. Большинство RAID-контроллеров требуют включения встроенной системы BIOS, причем ее функция "CD-ROM boot" ("загрузка с компакт-диска") также должна быть активирована. Возможно, вам придется обратиться к процедуре настройки контроллера (т. е. ввести сочетание клавиш <Alt>+<M> во время загрузки) и проверить правильность настройки этих элементов.

Симптом 11.15. Емкость дискового массива, о которой сообщает RAID-контроллер, значительно меньше фактической

К примеру, известно, что утилита SuperBuild BIOS контроллера Promise SuperTrak Pro сообщает о том, что емкость дисков Maxtor не превышает 5—7 Гбайт, хотя их фактическая емкость составляет 40 Гбайт. Почти в каждом подобном случае причина этого сбоя оповещения заключается в микропрограммном обеспечении RAID-контроллера и его служебной программе. Свяжитесь с производителем контроллера, чтобы получить обновление программного и микропрограммного обеспечения. В случае SuperTrack Pro эта неисправность вызвана использованием версии 1.0 BIOS и ISM Promise RAID версии b146. Обновите ISM Promise RAID до версии b156 и скачайте обновления микропрограммного обеспечения с сайта **support.promise.com /Support/Default.htm**.

Симптом 11.16. При работе с RAID-контроллером скорость передачи данных оказывается ниже запланированной

Практически во всех случаях низкая эффективность передачи данных обуславливается задержкой шины PCI между RAID-контроллером и другим устройством высокой пропускной способности (например, платой видеозахвата). К примеру, вы можете отметить наличие отброшенных кадров в процессе захвата видеосигнала в системе RAID. Если вы можете определить, какому устройству требуется дополнительная пропускная способность, попробуйте отключить или откорректировать производительность этого устройства, чтобы обеспечить дополнительную пропускную способность шины PCI для RAID-контроллера; в крайнем случае, снимите это устройство. Иначе вам придется откорректировать уровень использования PCI RAID-контроллером (если это возможно), но это почти во всех случаях приводит к общему снижению производительности дискового массива.

Симптом 11.17. Сбои появляются, когда система пытается воспользоваться диском "горячего резерва" (hot spare) или "горячей замены" (hot swap)

Во многих случаях вы можете столкнуться с замораживанием процесса восстановления или с тем, что утилита управления дисковым массивом (типа FastCheck для контроллера Promise FastTrak 66/100) не может обнаружить неисправные и вновь установленные диски.

Попробуйте сделать следующее.

- Проверьте микропрограммное обеспечение. Убедитесь в том, что вы используете самую последнюю версию микропрограммного обеспечения для RAID-контроллера.
- Проверьте драйверы и программное обеспечение. Убедитесь в том, что вы установили самые последние версии драйверов и служебных программ для вашего RAID-контроллера в используемой вами операционной системе. При необходимости установите более свежие версии драйверов и служебных программ.
- Избавьтесь от фоновых программ. Уменьшите количество дополнительных программ, работающих в фоновом режиме, которые могут помешать работе утилиты проверки диска RAID.
- Проверьте диск. Протестируйте диск на другом контроллере и/или компьютере, чтобы убедиться в его исправности.
- Удалите зарезервированный сектор. Возможно, вам придется удалить с жесткого диска "зарезервированный сектор", а затем дождаться, пока система заново обнаружит и переустановит диск. Помните, что удаление "зарезервированного сектора" на любом диске массива приводит к уничтожению всех данных на этом диске; поэтому сначала выполните полное резервирование данных системы.

Симптом 11.18. При наличии в системе SCSI-контроллера появляются трудности с разделением и форматированием дискового массива

Возможно, появятся указания "ошибочной емкости", поврежденных зарезервированных секторов или других проблем, связанных с загрузкой или операционной системой. Если в системе присутствует контроллер дисков SCSI, компьютер будет пытаться загрузиться с того контроллера, который он первым "увидит". Чтобы один из контроллеров система обнаруживала раньше другого, вы должны сделать так, чтобы его система BIOS загружалась первой. Как правило, добиться этого можно путем манипуляций с адресом BIOS, установленном на плате. Впрочем, в случае с контроллерами, работающими полностью на базе PnP (типа FastTrak 100), ресурсы, которые использует плата, управляются только PnP BIOS материнской платы. Слоту PCI с наивысшим приоритетом (как правило, слот 1 PCI) назначается самый нижний адрес BIOS, который загружается первым; следовательно, возможно, вам придется поменять платы расширения местами так, чтобы RAID-контроллер был установлен на слоте с наивысшим приоритетом. Некоторые утилиты CMOS Setup поддерживают режим "Scan Order Toggles" ("переключение порядка поиска"), который определяет, каким образом будет происходить поиск загрузочных устройств среди слотов PCI и встроенных устройств. В других случаях вам, возможно, удастся устранить эту неисправность, изменив "загрузочную последовательность" в CMOS Setup системы таким образом, что приоритет "SCSI" будет ниже, чем приоритет диска C: или дискового массива RAID.

Симптом 11.19. Во время обращения к массиву вы сталкиваетесь с повреждением данных или блокированием диска

Возможно, вы столкнетесь с этим во время разделения или форматирования массива. В этом случае выполните то, что описано далее.

- Проверьте кабели. Сигнальные кабели диска могут быть неисправны или плохо подсоединены. Еще раз проверьте соединения и при необходимости замените сигнальные кабели.

- Проверьте CMOS Setup. Запустите CMOS Setup и убедитесь в том, что генерация тактовых импульсов материнской платы и шины PCI происходит в рамках допустимых уровней. К примеру, разгон материнской платы может привести к увеличению скорости шины PCI, в результате чего на RAID-контроллере могут появиться ошибки данных. Попробуйте восстановить в CMOS Setup установки "BIOS Defaults".
- Проверьте память RAID. Память (ускоритель массива) RAID-контроллера, возможно, неисправна. Убедитесь в том, что память RAID-контроллера соответствует требованиям и правильно установлена. Замените модуль памяти RAID-контроллера. Попробуйте установить память от другого надежного производителя.
- Установите драйверы набора микросхем. Большинству современных материнских плат нужны драйверы для активизации таких сложных функций, как управление передачей данных по шине или поддержка AGP. Обязательно установите самую последнюю версию драйверов материнской платы (например, драйверы VIA "4-in-1" для материнских плат на базе VIA).

Симптом 11.20. При копировании файлов на сервер, испытывающий повышенную нагрузку на диски, появляются ошибки

Известно, что такая ситуация может сложиться в средах Windows 2000 и Windows NT при больших объемах сетевых передач файлов на сервер; как правило, она обозначается как "Error 3013", например:

```
Error 3013, The redirector has timed out to <servername>
```

Подобные блокировки перенаправления по времени могут приводить к неудачному завершению операций записи на сервер. Существует множество причин появления ошибок, связанных с блокировкой перенаправления по времени, но это ошибка обычно появляется из-за неисправности диспетчера кэша при записи крупных файлов на диск в системе с большим объемом памяти. Доступная пропускная способность к диску меньше, чем пропускная способность, необходимая записывающему устройству для завершения своей задачи за один цикл, так что в конечном итоге может получиться, что записывающее устройство будет удерживать ресурсы файла довольно долго. Для завершения операции записи требуется слишком много времени, и происходит блокировка перенаправления по времени на компьютере-клиенте. Как правило, эта проблема происходит, когда клиенты Windows NT 4.0 подключаются к серверу с Windows 2000, а на сервере применяется такая система RAID, которая снижает пропускную способность диска — например, RAID 5 (чередование с контролем по четности). Чтобы устранить этот сбой, установите последний служебный пакет для Windows 2000 и/или Windows NT.

Симптом 11.21. Вы столкнулись с ошибкой типа "Сканирование механизма № 2 шины PCI"

Ошибка такого типа обычно появляется при загрузке с загрузочного диска Windows 98 (например, при подготовке к чистой установке Windows NT 4.0 или Windows 2000). Почти всегда она имеет отношение к распределению ресурсов и происходит, когда системный BIOS выделяет определенные ресурсы RAID-контроллеру. Вам следует выяснить у производителя RAID-контроллера рекомендуемые варианты распределения ресурсов. К примеру, такая неисправность встречается при работе с

Promise SuperTrak Pro, а способ ее устранения приводится по адресу **support.promise.com/techsupport/trouble/scanning_pci_bus_using_Mechanism_2.htm**.

Симптом 11.22. После установки RAID-адаптера операционная система не загружается

Почти всегда эта неисправность связана с настройкой аппаратного обеспечения (и не имеет отношения к драйверу операционной системы). Запустите CMOS Setup, проверьте распределение прерываний PCI и убедитесь в том, что RAID-контроллеру присвоено уникальное прерывание — этот контроллер не должен использовать прерывание совместно с другими устройствами. Кроме того, вы можете попробовать переместить RAID-контроллер на слот PCI с более высоким приоритетом. В некоторых случаях перед установкой операционной системы приходится инициализировать и настраивать дисковый массив.

Симптом 11.23. При запуске Windows NT/2000 происходит внутренняя ошибка FTDISK

Если первичный диск в вашей операционной системе выходит из строя (или переходит в неоперативный режим) с включенной функцией зеркального отображения на RAID 1, Windows NT/2000 продолжает работать с дублированного диска и сигнализирует реестру текущего диска, отражая состояние сбоя зеркального отображения. При попытке перезапустить Windows NT/2000 вы увидите ошибку типа

```
STOP: 0x00000058 FTDISK_INTERNAL_ERROR
```

В Windows NT/2000 эта схема защиты используется потому, что когда первичный диск находится в неоперативном режиме, обработка продолжается на дублированном диске — при необходимости повторного запуска системы с первичного диска все данные, сохраненные на дублированном диске, были бы потеряны. Чтобы избежать потери данных, сделайте следующее.

1. Чтобы загрузиться с дублированного (вторичного) системного диска, воспользуйтесь загрузочной дискетой Windows.Fault Tolerance.
2. Запустите Disk Administrator. Обратите внимание на то, что первичный раздел диска операционной системы выделен красным. Первичному диску соответствует имя C: — его необходимо поменять на другое имя. Выделите раздел, выберите **Fault Tolerance**, а затем — **Break Mirror**. В меню **Partition** выберите **Commit Changes Now**.
3. После появления двух независимых разделов следует завершить резервирование на магнитной ленте того самого дублированного диска, с которого вы работаете — именно на нем содержатся самые последние данные, а также вся информация, сохраненная с момента выхода из строя первичного диска операционной системы.
4. Обозначьте первичный раздел на вторичном диске как активный (возможно, потребуется перезагрузка).
5. Удалите первичный раздел диска — с тем, чтобы получить возможность заново дублировать текущую операционную систему на первичном диске. Выберите первичный раздел диска, а затем **Delete** в меню **Partition**. Теперь выберите **Commit Changes Now** в том же меню.

Примечание

В случае если был дублирован весь диск C: (и на нем нет другого первичного раздела, который можно было бы определить как "активный"), Disk Administrator, возможно, не позволит удалить активный раздел. Для этого диск нужно переместить в положение вторичного незагрузочного диска (SCSI ID 1 и выше или же вторичный диск IDE). Или чтобы вручную удалить загрузочный флаг из таблицы разделов, вы можете воспользоваться программой Norton Utilities Disk Editor (DISKEDIT.EXE).

6. Проведите повторное зеркальное копирование дисков. Выделите текущий раздел диска операционной системы, а затем, удерживая клавишу <Ctrl>, выделите свободное пространство, созданное во время выполнения шага 5. Выберите **Establish Mirror** в меню **Fault Tolerance**. В меню **Partition** выберите **Commit Changes Now**.
7. Убедитесь в том, что зеркальное копирование прошло успешно — для этого нужно выйти из Disk Administrator, затем перезапустить его и проверить состояние зеркального копирования.
8. После успешного завершения зеркального копирования последняя копия ваших данных находится на первичном диске; к сожалению, на данном этапе перезагрузиться с первичного диска нельзя, ведь он — лишь дублированный диск. Повторите шаг 2.
9. Отметьте раздел как "активный", если он является первичным загрузочным разделом.
10. Выполните стандартное завершение работы и перезагрузитесь с первичного диска операционной системы. После запуска Windows удалите этот раздел и организуйте зеркальное копирование — этим вы восстановите отказоустойчивую конфигурацию уровня RAID 1.

Симптом 11.24. При использовании определенных RAID-контроллеров появляются сбои в работе режима ожидания

Некоторые RAID-контроллеры (например, Mylex DAC960) недостаточно хорошо восстанавливаются при возвращении хоста с установленным программным обеспечением Windows 2000 из режима ожидания. Это объясняется тем, что некоторые RAID-контроллеры не полностью совместимы с ACPI. Чтобы устранить эту неисправность, обновите BIOS RAID-контроллера (а возможно, и его драйверы), замените RAID-контроллер моделью, совместимой с ACPI, или блокируйте режим ожидания на хосте.

Дополнительные ресурсы

Adaptec: **www.adaptec.com**.

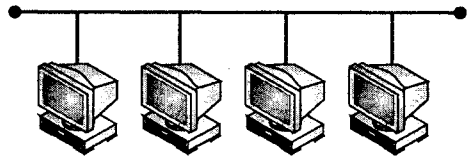
Compaq: **www.compaq.com**.

Gateway: **www.gateway.com**.

Intel: **www.intel.com**.

Promise: **www.promise.com**.

Tekram: **www.tekram.com**.



ГЛАВА 12

Адаптеры SCSI и поиск неисправностей

Для сетевых серверов и высокопроизводительных рабочих станций необходимы быстрые и надежные запоминающие подсистемы, которые способны координировать большое количество различных дисков и не нуждаются в наличии множества контроллеров. Интерфейс SCSI (Small Computer System Interface — интерфейс малых компьютерных систем) был представлен в 1986 г. и постепенно стал ведущим интерфейсом, применяемым на серверах и в приложениях с высокими требованиями к хранению данных. Система, оснащенная одним типичным адаптером SCSI, может обеспечивать одновременную работу до семи устройств SCSI, линейно соединенных одним кабелем. Современный сервер с хост-адаптером SCSI одной из последних версий (таким как хост-адаптер Adaptec 39160, показанный на рис. 12.1) способен работать даже с 30 устройствами SCSI, размещенными на двух независимых каналах контроллера, обеспечивающих скорость передачи данных до 160 Мбайт/с. В этой главе дан обзор технологии аппаратных средств SCSI, рассматривается типичный

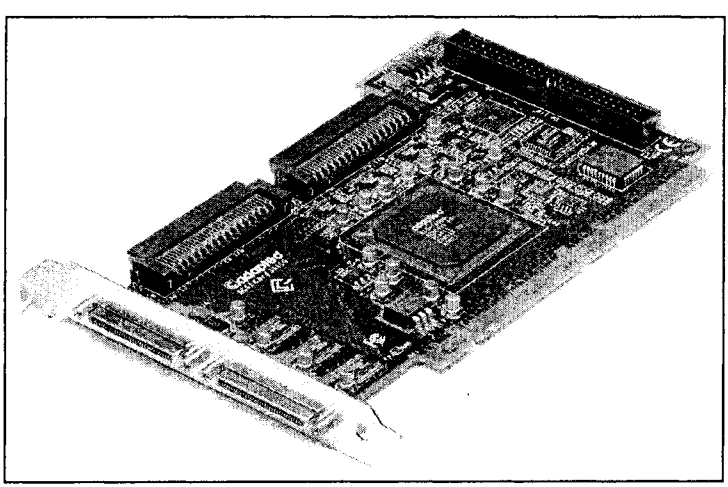


Рис. 12.1. Двухканальный адаптер SCSI Ultra160 модели Adaptec 39160 (публикуется с разрешения Adaptec)

вариант аппаратной и программной установки и приведены решения многих распространенных неисправностей SCSI.

Введение в SCSI

В идеале, периферийные устройства не должны зависеть от работы микропроцессора. Компьютер должен лишь отправлять периферийному устройству команды и данные и ждать, пока оно ответит (так работают принтеры). Параллельный и последовательный порты являются интерфейсами уровня физических устройств. Для компьютера безразлично, какое устройство подключено к такому порту. Другими словами, вы можете взять принтер, произведенный 12 лет назад, подключить его к новой системе на базе AMD Athlon и благодаря тому, что через интерфейс отсылаются лишь данные и команды, он будет прекрасно работать. В этом и заключается выраженный в самых общих словах принцип действия SCSI. Можно проектировать, разрабатывать и интегрировать компьютеры и периферийные устройства, не заботясь об аппаратной совместимости — эта совместимость полностью обеспечивается интерфейсом SCSI.

С практической точки зрения, SCSI — это шина и набор команд. Шиной называется организация физических проводников и оконечных нагрузок, причем у каждого проводника есть собственное имя и назначение. Набор команд — это ограниченный набор инструкций, с помощью которого и происходит взаимодействие компьютера и периферийных устройств через физическую шину. Шина SCSI применяется в системах, которые стремятся достичь независимости устройств. К примеру, интерфейс SCSI воспринимает все жесткие диски одинаково (исключением является лишь их общая емкость); то же касается оптических дисков, принтеров и т. д. Любое устройство SCSI можно заменить другим устройством, при этом, не внося никаких изменений в систему; установка устройства SCSI на шину требует немногим больше обновления драйвера. Так как интеллект SCSI располагается не в компьютере, а в самом периферийном устройстве, компьютер может применять лишь небольшой набор стандартных команд для осуществления передачи данных между ним и периферийным устройством.

Варианты SCSI

Давайте рассмотрим эволюцию интерфейса SCSI, пути его развития и распространения. История SCSI началась в 1979 г., когда компания Shugart Associates (старожилы, возможно, помнят ее как одного из первых производителей жестких дисков) выпустила стандарт системного интерфейса Shugart Associates (Shugart Associates Systems Interface, SASI). В 1982 г. в Национальном институте стандартизации США (American National Standards Institute, ANSI) был сформирован комитет X3T9.2 с целью развития стандарта SASI (впоследствии он был переименован в SCSI, поскольку ANSI не может называть стандарт в честь продукта). Диски и интерфейсы SCSI, разработанные в соответствии с новым стандартом X3T9.2 SCSI, назывались SCSI-1, хотя на самом деле стандарт SCSI-1 (ANSI X3.131-1986) стал официальным лишь в 1986 г. SCSI-1 предусматривал 8-битовую шину системного уровня, которая была способна обеспечивать работу до восьми устройств и развивать скорость передачи данных до 5 Мбайт/с. Впрочем, задержка в процессе стандартизации привела к возникновению множества проблем конфигурации и совместимости в сборках SCSI-1. В табл. 12.1 приведено сравнение спецификаций каждого стандарта SCSI.

Таблица 12.1. Сравнение основных свойств SCSI

Обозначение	Название	МГц	Разрядность шины	Мбайт/с	Мбит/с
SCSI-1	SCSI-1	5	8	5	40
Fast SCSI	SCSI-2	10	8	10	80
Fast-Wide SCSI	SCSI-2/SCSI-3	10	16	20	160
Ultra SCSI	SCSI-3	20	8	20	160
Ultra-Wide SCSI	SCSI-3	20	16	40	320
Ultra2 SCSI	SCSI-4	40	8	40	320
Ultra2-Wide SCSI	SCSI-4	40	16	80	640
Ultra3 SCSI	Ultra 160	40*2[1]	8	80	640
Ultra3-Wide SCSI	Ultra 160	40*2[1]	16	160	1280
Ultra 4 SCSI	Ultra 320	Не определено			
Ultra4-Wide SCSI	Ultra 320	Не определено			

[1] Основная частота Ultra3 не отличается от Ultra2 (40 МГц), но Ultra3 передает 2 байта за такт, таким образом удваивая общую пропускную способность.

Примечание

Предполагалось, что SCSI-1 обеспечит поддержку всех устройств SCSI, но производители слишком свободно обошлись с новым стандартом. Результатом явились частые трудности, связанные с установкой и совместимостью устройств SCSI-1, которые теоретически должны были работать вместе безо всяких проблем. В настоящее время все устаревшие адаптеры SCSI-1 следует обновить до систем SCSI-3.

Еще раньше в 1986 г. (даже до ратификации стандарта SCSI-1) началась работа над стандартом SCSI-2, в котором предполагалось преодолеть многие трудности, связанные со скоростью и совместимостью, которые имели место в SCSI-1. К 1994 г. Национальный институт стандартизации США одобрил стандарт SCSI-2 (X3.131-1994). SCSI-2 разрабатывался с расчетом на обратную совместимость с SCSI-1, но при этом предусматривал несколько разновидностей. Fast SCSI-2 (Fast SCSI) удвоил тактовую частоту шины SCSI и позволил передавать данные по 8-битовой шине данных SCSI со скоростью 10 Мбайт/с. Wide SCSI-2 (Wide SCSI) также увеличил исходную скорость передачи данных в два раза, т. е. до 10 Мбайт/с, но вместо первоначальной 8-битовой шины данных в нем должна была применяться 16-битовая (при этом тактовая частота SCSI оставалась без изменений). В расчете на более крупную шину данных в Wide SCSI применяется 68-контактный кабель, заменивший традиционный 50-контактный. Кроме того, Wide SCSI способен обеспечивать работу до 16 устройств SCSI. Затем разработчики объединили свойства быстрого и широкого режимов и создали Fast Wide SCSI-2 (Fast Wide SCSI), обеспечивающий передачу данных по 16-битовой шине данных со скоростью 20 Мбайт/с. Где бы вы

ни встретили упоминания о Fast SCSI, Wide SCSI или Fast Wide SCSI, знайте, что речь всегда идет о реализациях SCSI-2.

Но на этом совершенствование SCSI не завершилось. В 1993 г. (еще до принятия SCSI-2) в Национальном институте стандартизации США началась разработка стандарта SCSI-3. Предусматривалась обратная совместимость SCSI-3 с устройствами SCSI-2 и SCSI-1. Преимущества стандарта SCSI-3 реализованы во многих устройствах и контроллерах SCSI. Эти типичные устройства SCSI-3 обычно называются Fast-20 SCSI (также Ultra SCSI-3 или Ultra-SCSI). В Ultra-SCSI применяется тактовая частота шины SCSI в 20 МГц, а 8-битовая шина данных помогает добиться скорости передачи данных 20 Мбайт/с. В рамках SCSI-3 16-битовую шину данных использует Wide Fast-20 SCSI (также Ultra Wide SCSI-3 или Ultra Wide SCSI), обеспечивающий скорость передачи данных 40 Мбайт/с. Дальнейшая разработка SCSI была связана с появлением реализаций SCSI-4. Стандарт SCSI-4 включает вариант Fast-40 SCSI (также Ultra2 SCSI-4 или Ultra2 SCSI), использующий тактовую частоту шины 40 МГц и обеспечивающий скорость передачи данных в 40 Мбайт/с на 8-битовой шине данных. 16-битовая версия шины данных известна под именем Wide Fast-40 SCSI (также Ultra2 Wide SCSI-4 или Ultra2 Wide SCSI); предполагается, что она должна обеспечивать передачу данных на скорости 80 Мбайт/с. Если вы встретите упоминания Ultra2 или Fast40, можете быть почти уверены, что имеете дело со сборкой SCSI-4.

Но и на этом развитие стандарта SCSI не остановилось. Стандарт Ultra3 SCSI (также Ultra160) предусматривает применение тактовой частоты шины в 40 МГц "с двойной передачей" (double transitioned). В результате на той же шине в 40 МГц эффективность передачи данных удваивается и составляет 80 Мбайт/с. Стандарт Ultra3 Wide SCSI предусматривает применение 16 информационных бит вместо 8. На той же тактовой частоте шины в 40 МГц с "двойной передачей" Ultra3 Wide SCSI позволяет достичь скорости передачи данных в 160 Мбайт/с. Стандарты Ultra360 (Ultra4) SCSI еще не полностью определены, но можете быть уверены, что появятся еще более скоростные реализации. Кроме того, имейте в виду, что SCSI традиционно является параллельной шиной — таким образом, одновременно по параллельной линии данных передается 8 или 16 бит данных. SCSI-3 предлагает три новых последовательных схемы соединения. Они обозначаются как архитектура SSA (Serial Storage Architecture — архитектура последовательной памяти), волоконно-оптический канал (Fibre Channel) и IEEE 1394 (FireWire). Такие последовательные схемы обеспечивают более высокие скорости передачи данных, чем параллельные шины, но при этом они не являются обратно совместимыми с SCSI-2 или SCSI-1.

Линейный и дифференциальный методы

Сигнальный провод, применяемый в шине SCSI, определенным образом влияет на ее производительность. Как правило, в SCSI используются два метода проводки: линейный и дифференциальный. У обоих есть свои преимущества и недостатки.

Функционирование *однопроводного (линейного)* (single-ended, SE) *межсоединения* полностью соответствует названию — отдельный сигнал передается от инициатора к цели по одному проводу. Для передачи любого сигнала требуется лишь один провод. Нагрузочные резисторы на обоих концах кабеля помогают поддерживать допустимые уровни сигналов. Общий провод заземления (обратный) обеспечивает начало

отсчета для всех однопроводных соединений. К сожалению, однопроводная схема не отличается высоким шумовым сопротивлением, и поэтому длина кабелей, проведенных с использованием этого метода, обычно не превышает 6 м, а скорость передачи данных при этом ограничивается 5 МГц. Для достижения более высоких скоростей длина кабеля должна составлять 1,5 м. Несмотря на эти недостатки, однопроводная организация получила довольно широкое распространение в силу своей простоты.

В *дифференциальном* (differential, DIF) *межсоединении* для передачи каждого сигнала используется два провода (в отличие от одного общего обратного провода). Дифференциальный сигнал обеспечивает прекрасное шумовое сопротивление, т. к. он не зависит от общего обратного провода. Это позволяет проводить более протяженные кабели (до 25 м) и развивать большую скорость (10 МГц). Поддерживать целостность сигнала помогают нагрузочные резисторы, помещаемые на каждом конце кабеля. Но дифференциальная проводка сложнее однопроводных интерфейсов. Интерфейс SCSI LVD (Low-Voltage Differential — низковольтный дифференциальный интерфейс) — это развивающийся стандарт, определенный в документе SPI-2 SCSI-3; в нем предусматривается работа при напряжении 3,3 В, а не 5 В. LVD предназначен для обеспечения более высоких скоростей передачи данных и сочетает преимущества однопроводной и дифференциальной шин SCSI. LVD менее чувствителен к электромагнитным шумам и позволяет достигать высоких скоростей передачи данных на больших расстояниях, чем при использовании однопроводного кабеля. Интерфейс LVD предназначен для применения со спецификациями Ultra-2 SCSI и Ultra 160/m. LVD напрямую не совместим с однопроводным межсоединением, но его устройства пользуются многорежимными драйверами, которые автоматически определяют тип шины и переключают устройство на соответствующий режим работы. Это позволяет устанавливать устройства LVD/SE на однопроводной шине, не настраивая для этого переключатели или джамперы. Таким образом, LVD внедряется постепенно, без убытков от вложений в однопроводные устройства. Впрочем, при использовании устройства LVD/SE на однопроводной шине преимущества LVD исчезают, даже при подключении к шине LVD/SE хотя бы одного однопроводного устройства она переключается в однопроводной режим (со всеми его ограничениями).

Длина шины

Как вы уже знаете, устройства SCSI соединяются между собой шлейфовым методом с помощью 50- или 68-контактного кабеля. Суммарная протяженность этого кабеля и составляет общую длину шины SCSI. Когда имеются только внутренние устройства SCSI, длина шины измеряется от адаптера SCSI до крайнего устройства SCSI в цепочке (оконечного устройства). Если речь идет только о внешних устройствах SCSI, длина шины измеряется от адаптера SCSI до крайнего внешнего устройства SCSI в цепочке (оно также должно быть конечным). Если в цепочке присутствуют как внутренние, так и внешние устройства SCSI, длина шины измеряется от крайнего внешнего устройства до последнего внутреннего устройства. Существуют ограничения на длину шины SCSI. С годами шины SCSI стали быстрее, и рабочая длина сократилась. В табл. 12.2 приведены значения максимальных длин шины SCSI при использовании однопроводного, дифференциального и низковольтного дифференциального (LVD) методов соединения.

Таблица 12.2. Значения длин шин SCSI

Обозначение	Однопроводной метод	Дифференциальный метод	Низковольтный дифференциальный метод (LVD)
SCSI-1	6 м	25 м	12 м [2]
Fast SCSI	3 м	25 м	12 м [2]
Fast Wide SCSI	3 м	25 м	12 м [2]
Ultra SCSI	1,5–3 м	До 25 м	До 12 м
Wide Ultra SCSI	До 3 м	До 25 м	До 12 м
Ultra2 SCSI	[1]	25 м	12 м
Wide Ultra2 SCSI	[1]	25 м	12 м
Ultra3 SCSI	[1]	25 м	12 м
Wide Ultra3 SCSI	[1]	25 м	12 м

[1] На скоростях Ultra2 и Ultra3 однопроводной и высокомощный дифференциальный методы не определены.

[2] Только если все устройства, установленные на шине, поддерживают LVD.

Оконечные нагрузки

При передаче высокочастотных сигналов по смежным проводам эти сигналы гасятся и на всем протяжении кабеля создают помехи друг другу. Это естественное и достаточно хорошо изученное электрическое явление (в *гл. 8* вы уже познакомились с ним — тогда оно было представлено в виде затухания). В компьютерах целостность сигналов SCSI обеспечивается благодаря применению на обоих концах информационного кабеля силовых резисторов, которые "подтягивают" до уровня питающего напряжения активные сигналы. Встроенные нагрузочные резисторы на дисководах и платах контроллеров уже находятся в большинстве высокочастотных информационных кабелей компьютеров. Небольшая резисторная схема называется оконечной нагрузкой (терминатором). Так как к кабелю флоппи-дисковода или к IDE-кабелю можно теоретически присоединять ограниченное количество устройств, проектировщиков не особенно заботила оконечная нагрузка — они просто везде ставили резисторы. В условиях SCSI к кабелю шины можно подключить до восьми устройств. Кабель SCSI также должен заканчиваться оконечной нагрузкой, но расположение нагрузочных резисторов зависит от того, какие устройства присоединяются к шине и где они устанавливаются. В результате терминирование становится важным элементом схем и поиска неисправностей SCSI. Плохое или неправильное терминирование может приводить к периодическим неисправностям, связанным с передачей сигналов. Ниже приведены некоторые общие инструкции по организации оконечной нагрузки.

- Терминированию подлежат последние устройства в цепочке (на кабеле) SCSI. В условиях внутренней сборки необходимо завершить хост-адаптер SCSI и последнее (крайнее) внутреннее устройство; прочие устройства должны оставаться без оконечной нагрузки. При внешней сборке нужно завершить хост-адаптер

SCSI и последнее (крайнее) внешнее устройство. В смешанной (внутренней/внешней) сборке хост-адаптер SCSI, как правило, остается без оконечной нагрузки, а терминируются крайнее внутреннее и внешнее устройства SCSI.

- Внутренние устройства Ultra160 и Ultra2 (например, диски) производятся с отключенным терминированием, причем эту настройку изменить нельзя. Терминирование этих внутренних устройств обеспечивается встроенной оконечной нагрузкой на конце внутреннего 68-контактного кабеля LVD SCSI.
- Терминирование устройств Wide SCSI, Narrow SCSI и Ultra SCSI, как правило, осуществляется либо путем ручной установки находящихся на них перемычек или переключателей, либо посредством физического удаления или установки на этих устройствах одного или нескольких модулей резисторов. Это традиционные средства выбора оконечных нагрузок.
- Терминирование большинства внешних устройств SCSI осуществляется путем снятия или установки блока оконечной нагрузки SCSI в транзитный порт последнего такого устройства. Впрочем, терминирование некоторых внешних устройств SCSI включается или отключается путем установки переключателя на их задней панели.
- На плате хост-адаптера SCSI Adaptec по умолчанию устанавливается автоматическое терминирование, что является предпочтительным методом. Это означает, что терминирование будет включаться и отключаться тогда, когда плата сочтет то или иное действие необходимым. Большинство производителей хост-адаптеров не рекомендуют менять эту настройку по умолчанию.

Как правило, терминирование является либо активным, либо пассивным. Пассивное терминирование предполагает простое подключение к устройству SCSI резисторного блока. Пассивные резисторы питаются от линии TERMPWR. Пассивное терминирование эффективно на коротком расстоянии (приблизительно до 1 м) и обычно оптимально для кабелей внутри ПК, но на большем расстоянии он может стать причиной сбоя. В активных оконечных нагрузках предусматривается наличие управляемых источников питания, что делает оптимальным их применение на кабелях, проложенных на большие расстояния (например, кабели, с помощью которых подключаются внешние устройства SCSI типа страничных сканеров), а также в системах Wide SCSI. В большинстве реализаций SCSI-2 (и более поздних) применяются активные оконечные нагрузки. Вариантом активного терминирования является терминирование FPT (Forced Perfect Termination — полное силовое терминирование). Терминирование FPT подразумевает наличие диодных фиксаторов, которые предотвращают выбросы и провалы сигнала. Благодаря этому эффективность применения терминирования FPT в сочетании с протяженными кабелями SCSI возрастает.

Идентификаторы и номера логических устройств SCSI

Обычная шина SCSI способна обеспечивать работу до восьми устройств, которые называются *логическими модулями*; каждое из них распознается с помощью идентификатора ID. Это означает, что каждому устройству, установленному на шине, должен соответствовать уникальный идентификационный номер (0—7). Если два устройства используют один и тот же идентификатор, возникает конфликт. Как правило, на адаптере SCSI и на каждом устройстве SCSI идентификаторы устанавливаются с помощью перемычек или DIP-переключателей (рис. 12.2). Обычно адаптеру SCSI присваивается идентификатор ID7, первому жесткому диску SCSI — ID0,

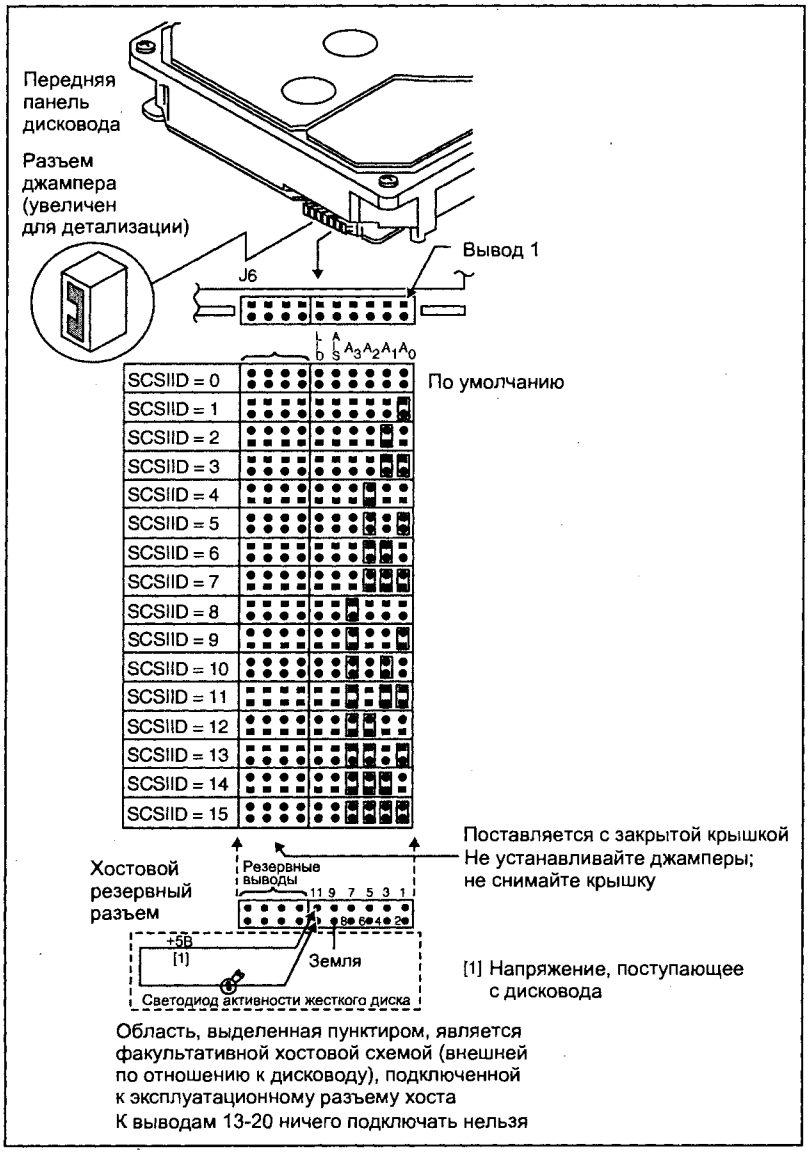


Рис. 12.2. Установка перемычки идентификатора SCSI (публикуется с разрешения Seagate)

а второму — ID1. Всем остальным устройствам обычно соответствуют идентификаторы от ID2 до ID6. Широкая (16-битовая) шина SCSI способна обеспечивать работу до 16 устройств, идентификаторы для которых распределяются в диапазоне от 0 до 15. Adaptec 39160 предусматривает два 16-битовых канала и поэтому может поддерживать до 30 устройств SCSI — в двух 16-битовых каналах возможны 32 идентификатора, от этого числа отнимается по одному идентификатору для контроллеров

каждого канала, и в конечном счете остается 30 доступных идентификаторов. Ниже приводятся некоторые рекомендации, связанные с идентификаторами SCSI.

- Во внутренних устройствах SCSI идентификаторы обычно устанавливаются с помощью настройки перемычек.
- Во внешних устройствах SCSI идентификаторы обычно устанавливаются с помощью переключателя, который находится на их задней панели.
- Идентификационные номера SCSI не обязательно должны быть последовательными, потому что номера хост-адаптера SCSI и других устройств различны.
- На шине SCSI идентификатор 7 имеет наивысший приоритет. Приоритет оставшихся идентификаторов (в убывающем порядке) таков: от 6 до 0, затем от 15 до 8.
- В большинстве систем на базе шины SCSI хост-адаптеру присваивается идентификатор 7, благодаря чему он получает наивысший приоритет. Во многих шинных адаптерах SCSI наподобие Adaptec 39160 обоим каналам шины SCSI заранее присваивается идентификатор ID7, причем изменять эту настройку не рекомендуется.
- Большинству внутренних жестких дисков SCSI производитель присваивает идентификатор ID0.
- Если вы пользуетесь 8-битовыми устройствами SCSI, им необходимо присваивать идентификаторы 0, 1, 2, 3, 4, 5 или 6. Идентификатор ID0 рекомендуется назначать первому жесткому диску SCSI.
- Если ваш компьютер загружается с жесткого диска SCSI, то во внутренней настройке хост-адаптера SCSI, как правило, должен приводиться тот же идентификатор, что и у загрузочного диска. К примеру, при загрузке с контроллера Adaptec 39160 настройка **Boot SCSI ID** утилиты SCSI Select должна соответствовать идентификатору SCSI того устройства, с которого производится загрузка. По умолчанию в **Boot SCSI ID** для первого жесткого диска SCSI устанавливается идентификатор 0. В большинстве случаев изменять эту настройку не требуется.

Номера логических устройств (LUN — Logical Unit Numbers) похожи на идентификаторы SCSI, т. к. они обеспечивают распознавание устройств SCSI. Но номера LUN обозначают устройства внутри устройств — разделы в рамках идентификаторов. Каждый идентификатор SCSI от 0 до 7 может включать до восьми номеров LUN (в SCSI-3 64 LUN), или восемь подустройств каждого отдельно взятого идентификатора устройства. Предположим, что вам понадобилось разместить на шине SCSI более восьми устройств. С одной стороны, можно сделать так, чтобы ваши устройства реагировали на идентификатор SCSI; с другой стороны, каждое из них, имея уникальный ID, может отвечать на номер LUN. К примеру, если у вас есть три жестких диска (E:, F: и G:), то всем им можно сопоставить ID2, но при этом диску E: можно присвоить LUN0, диску F: — LUN1, а диску G: — LUN2. Такая схема часто используется в системах SCSI RAID, когда количество устройств превышает количество доступных идентификаторов SCSI. К сожалению, пользователь SCSI не может самостоятельно принять решение о распределении LUN — аппаратное обеспечение должно быть спроектировано с соответствующим расчетом. Номера LUN используются довольно редко, и многие адаптеры SCSI их не проверяют, но этот метод немного увеличивает скорость сканирования шины. При наличии устройства, использующего LUN (например, дисковода с автоматической сменой компакт-дисков), вам, возможно, придется активировать поддержку LUN с помощью драйве-

ра устройства или BIOS хост-адаптера. Windows 2000 позволяет просматривать распределение идентификаторов SCSI и LUN между установленными устройствами SCSI (рис. 12.3).

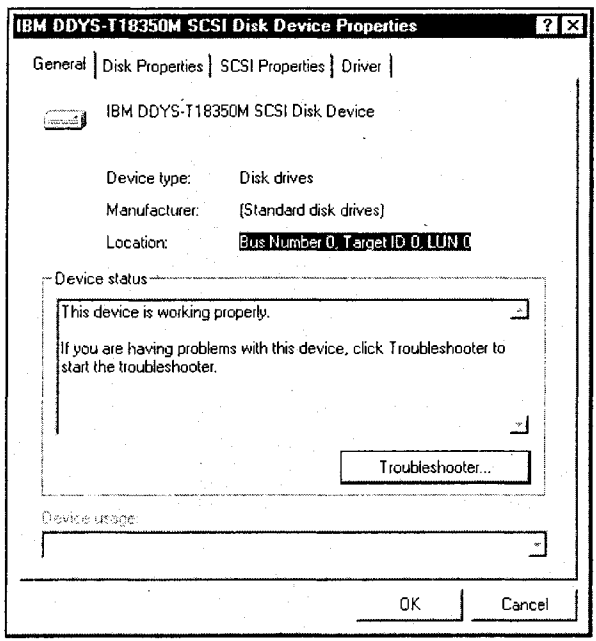


Рис. 12.3. Применение диспетчера устройств (Device Manager) Windows 2000 для проверки распределения идентификаторов и LUN между устройствами SCSI

Функционирование шины SCSI

Теперь, когда вы получили представление о принципах архитектуры шины SCSI и ее структуре, рассмотрим, как этот интерфейс работает в нормальных условиях. Для подключения устройства к шине используются одни и те же проводники, поэтому устройство может получить контроль над шиной только после того, как оно получит на это разрешение от всех остальных устройств. Попытка получения доступа к шине называется этапом разрешения конфликтов *(фазой арбитража)*. После того как устройство (например, контроллер SCSI) получило право управлять шиной, оно должно установить связь с устройством, с которым предполагает обмениваться данными. Этот процесс вызова устройства называется *фазой вызова*. После того как связь установлена, может начинаться передача данных. В этой части главы будут подробно рассмотрены процедура согласования и передача информации по шине SCSI.

Согласование

Доступ и использование шины SCSI должны быть согласованы между устройствами. Согласование начинается тогда, когда шина свободна, а линии занятости (Busy, BSY) и выбора (Select, SEL) простаивают. Устройство начинает процедуру арбитра-

жа, активируя линию BSY и свою линию идентификации данных (информационный бит D0—D7 в зависимости от устройства). Если в одно и то же время получить контроль над шиной пытаются несколько устройств, выигрывает устройство с более высоким ID. Выигравшее устройство (инициатор) пытается заполучить целевое устройство (исполнителя) путем выдачи сигнала в линию SEL и линии идентификации данных (информационный бит D0—D7). После этого инициатор освобождает линию BSY, а требуемое целевое устройство, подтверждая выбор, устанавливает эту линию. Затем инициатор освобождает линии SEL и шину данных. Теперь можно начинать передачу информации.

Информация

Выбранное целевое устройство контролирует передачу данных и ее направление. Передача длится до тех пор, пока целевое устройство не освободит линию BSY, возвращая шину в состояние незанятости. Если для подготовки какого-либо блока информации потребуется слишком много времени, целевое устройство может завершить соединение, воспользовавшись для этого сообщением о разъединении (disconnect). Впоследствии оно попытается установить соединение еще раз, вновь запустив процедуры арбитража и вызова.

В ходе передачи информации инициатор сообщает целевому устройству, что нужно делать при поступлении команды, и на *фазе исходящих сообщений* определяет режим передачи данных. На *фазе исполнения команд* за сообщением следует определенная команда SCSI. После отправки команды начинается передача данных, проходящая на *фазах ввода и/или вывода данных*. Во время командного этапа целевое устройство уступает управление инициатору. К примеру, в самой команде может содержаться запрос на передачу дополнительной информации. После получения этой команды целевое устройство сообщает инициатору, была ли она успешно выполнена или нет, возвращая информацию о состоянии на *фазе состояния*. Наконец, команда завершается, когда на *фазе входящих сообщений* целевое устройство отсылает инициатору отчет о ее выполнении. Рассмотрим простой пример передачи информации по SCSI.

1. Этап свободной шины. Система простаивает.
2. Арбитражный этап. Устройство получает контроль над шиной.
3. Этап вызова. Происходит вызов устройства.
4. Этап исходящих сообщений. Целевое устройство подготавливает передачу данных.
5. Командный этап. Отправка команды.
6. Этап ввода данных. Обмен данными.
7. Этап состояния. Обозначает результаты обмена.
8. Этап входящих сообщений. Обозначает окончание обмена данными.
9. Этап свободной шины. Система простаивает.

Установка системы SCSI

На сегодняшний день почти все хост-адаптеры SCSI являются устройствами PnP, предназначенными для выполнения автоматического обнаружения и распределения

ресурсов в слоте PCI материнской платы. Впрочем, большая часть сбоев, связанных с хост-адаптерами SCSI, начинаются при первой установке платы в системе — как правило, из-за неверной установки аппаратного и программного обеспечения. В этой части главы вашему вни.ланию предлагается общий обзор процесса установки адаптера SCSI и настройки SCSI BIOS; исходя из этого вы сможете проверить, все ли этапы вы прошли во время самостоятельного выполнения установки.

Примечание

Если в состав вашей материнской платы входит хост-адаптер SCSI, то вы можете пропустить этапы, связанные с установкой, и сосредоточиться на вопросах настройки SCSI.

Установка внутреннего оборудования

Для реализации SCSI в условиях сервера или рабочей станции требуется установка в системе хост-адаптера SCSI (его также называют "контроллером") и по крайней мере одного устройства SCSI. Установка обычного хост-адаптера SCSI состоит из нижеперечисленных этапов.

1. Остановите систему, затем выключите компьютер и выдерните из розетки шнур питания.
2. Открутите шурупы крепления наружного корпуса, снимите корпус и положите его (вместе с шурупами) в безопасное место.
3. Если вы собираетесь поменять старый хост-адаптер SCSI на новую, более быструю модель, для начала вам нужно снять старый адаптер. Отключите от него внутренний и внешний кабели SCSI. Открутите с корпуса винты крепления кронштейна старой платы SCSI и выньте старый адаптер из слота. Поместите адаптер SCSI на поверхность, защищенную от статических зарядов, или в антистатический пакет.
4. Определитесь с тем, в какой слот вы будете устанавливать плату нового хост-адаптера SCSI. Для большинства современных хост-адаптеров требуется 32-битовый слот PCI, хотя некоторые более старые платы SCSI можно устанавливать в слот ISA. Некоторые современные платы SCSI устанавливаются в 64-битовый слот PCI (обычно он есть на серверных материнских платах). Найдите свободный слот PCI с управлением передачей данных по шине, подходящий для вашей модели платы адаптера SCSI. Снимите с нужного слота заглушку (если она еще не снята) и сохраните винт для монтажа кронштейна.
5. Установите новую плату хост-адаптера SCSI. Нажмите на плату равномерно и с усилием, чтобы она полностью вошла в гнездо. Не нажимайте на плату слишком сильно, иначе вы можете сломать хост-адаптер или даже повредить материнскую плату. С помощью винта зафиксируйте плату SCSI на корпусе компьютера.
6. При подключении любых внутренних устройств SCSI вставьте 50- или 68-выводной коннектор SCSI, находящийся на конце внутреннего плоского кабеля SCSI, в разъем платы SCSI. Обязательно совместите выводы 1 на обоих коннекторах.
7. При желании подключите кабель светодиода активности жесткого диска к соответствующему коннектору платы SCSI. Тогда светодиод, который имеется на передней панели большинства корпусов, будет обозначать активность шины SCSI.

8. Выполните все необходимые соединения с внешней шиной SCSI (которая может, к примеру, присоединять сканер или внешние дисководы SCSI).

Шина SCSI требует надлежащего терминирования и отсутствия дублированных идентификаторов SCSI. Прежде чем пытаться перезагрузить компьютер, проверьте идентификаторы каждого устройства SCSI и убедитесь в правильности установки оконечных нагрузок на концах цепочки SCSI.

Примечание

Если в составе вашей материнской платы есть встроенный хост-адаптер SCSI, не забывайте, что он может быть терминирован по умолчанию. Если отключить терминирование встроенного адаптера не удастся, то, возможно, вам придется пользоваться либо внешними, либо внутренними устройствами SCSI, но совмещать их вы не сможете. За точной информацией о подобных ограничениях обратитесь к документации к вашей материнской плате.

Замечания о подключении к SCSI

Хотя интерфейс SCSI обеспечивает размещение широкого спектра устройств, при их установке зачастую возникают некоторые трудности, о которых вы должны знать. Как правило, перед подключением к хост-адаптеру устройства SCSI необходимо проверить три пункта: идентификаторы SCSI, оконечные нагрузки и подсоединение силовых кабелей. Ниже приводятся некоторые рекомендации по настройке идентификаторов SCSI и оконечных нагрузок на различных устройствах.

Примечание

Так как конкретные процедуры настройки зависят от устройства, точные инструкции можно получить только из документации к устройству.

Проверьте идентификаторы SCSI

Каждому хост-адаптеру и устройству SCSI должен соответствовать уникальный идентификатор. К примеру, ID7 является идентификатором каждого из каналов платы SCSI Adaptec 39160, и любому устройству, подключенному к одному из этих каналов, необходимо присвоить идентификационный номер SCSI в диапазоне от 0 до 15. В пределах отдельного канала SCSI не может быть двух устройств с одинаковыми идентификаторами. Если компьютер загружается с жесткого диска SCSI, идентификатором этого диска должен быть 0. (Большинству жестких дисков SCSI нулевой идентификатор SCSI присваивается еще производителем.) Идентификаторы SCSI внутренних устройств обычно устанавливаются при помощи перемычек, а идентификаторы внешних устройств, как правило, настраиваются посредством соответствующего переключателя на их задней панели.

Установите оконечную нагрузку кабеля

Чтобы добиться надежной передачи данных по шине SCSI, на устройствах, находящихся на концах каждого кабеля, должна быть установлена оконечная нагрузка (или активирована). Напротив, с устройств, находящихся между концами кабеля, оконечные нагрузки должны быть сняты (или их внутренние функции терминирования должны быть отключены). При подключении устройств Ultra160 или Ultra2 SCSI шина SCSI должна быть терминирована либо на конце кабеля (с помощью посто-

янной оконечной нагрузки), либо с помощью отдельного нагрузочного коннектора. Ultra SCSI и более ранние однопроводные устройства могут завершать шину напрямую. При использовании оконечной нагрузки Ultra SCSI на шине LVD Ultra160 и Ultra2 SCSI ей придется переключиться в однопроводной режим, в результате чего скорость и длина кабеля будут ограничены. По этой причине, прежде чем устанавливать устройства Ultra160 SCSI, необходимо убедиться в наличии кабеля Ultra160 или Ultra2, или оконечной нагрузки.

Подключение внутренних устройств Ultra160 и Ultra2

Для подключения внутренних устройств Ultra160 и Ultra2 SCSI необходим специальный 68-выводной внутренний низковольтный дифференциальный кабель (LVD, Low-Voltage Differential). Если ваши кабели не промаркированы, имейте в виду, что LVD выглядит как витая пара из плоских лентовидных кабелей между коннекторами устройств. Некоторые кабели ламинированы, что обеспечивает их плоскую установку. В конец внутреннего LVD-кабеля обычно встроена оконечная нагрузка. Хост-адаптеры SCSI типа Adaptec 39160 предусматривают использование двух отдельных каналов Ultra160 SCSI, причем на каждом из них присутствует по одному внутреннему коннектору LVD/SE, к которому можно подключать внутренние устройства SCSI. Для подключения внутренних устройств Ultra160 или Ultra2 необходимо сделать следующее:

1. Найдите 68-выводной кабель LVD SCSI (он может принимать форму витой пары или быть плоским). В большинстве случаев устройства Ultra160 и Ultra2 SCSI следует подключать к каналу, на котором не установлены старые устройства Ultra SCSI. Это позволит обеспечить максимальную скорость передачи данных на устройствах Ultra160 и Ultra2 SCSI.
2. Подключите нетерминированный конец кабеля (кабелей) к внутреннему коннектору (коннекторам) LVD/SE на адаптере SCSI.
3. Подключите внутренние устройства Ultra160 и Ultra2 SCSI к другим кабельным коннекторам, начиная с коннектора на терминированном конце кабеля.
4. Подведите силовой кабель от внутреннего источника питания вашего компьютера к каждому внутреннему устройству SCSI.

Примечание

Во внутренних устройствах Ultra160 и Ultra2 SCSI функция терминирования отключается производителем, причем эту настройку изменить нельзя. Должное терминирование обеспечивается оконечной нагрузкой на конце кабеля LVD SCSI.

Подключение устройств Wide SCSI

Устройства Wide SCSI можно подключить к внутренним коннекторам LVD/SE. Впрочем, обычно рекомендуется подсоединять их к коннектору LVD/SE канала A SCSI, а все новые устройства Ultra160 и Ultra2 — устанавливать на канале B SCSI. Чтобы подключить устройство Wide SCSI, сделайте следующее.

1. Найдите 68-выводной внутренний кабель Wide SCSI.
2. Подключите один конец кабеля к внутреннему 68-выводному коннектору канала A на хост-адаптере SCSI.

3. Подключите другой конец кабеля к терминированному устройству Ultra/Fast Wide SCSI.
4. При наличии других устройств Ultra/Fast Wide SCSI их следует подключить к коннекторам, расположенным между двумя концами кабеля. Убедитесь в том, что эти устройства не терминированы.
5. Подведите силовой кабель от внутреннего источника питания вашего компьютера к каждому внутреннему устройству.

Подключение внутренних устройств Ultra/Fast Narrow SCSI

При наличии устройств Ultra/Fast Narrow SCSI со стандартными 50-выводными коннекторами их можно подключить к 50-выводному внутреннему коннектору SE Narrow SCSI. Чтобы подключить такое устройство, сделайте следующее.

1. Найдите 50-выводной внутренний кабель Ultra Narrow SCSI.
2. Подключите один конец кабеля к внутреннему 50-выводному коннектору SE Narrow SCSI на хост-адаптере SCSI.
3. Подключите другой конец кабеля к терминированному устройству Ultra/Fast Narrow SCSI.
4. При наличии других устройств Ultra/Fast Narrow SCSI их следует подключить к коннекторам, расположенным между двумя концами кабеля. Убедитесь в том, что эти устройства не терминированы.
5. Подведите силовой кабель от внутреннего источника питания вашего компьютера к каждому внутреннему устройству.

Подключение внешних устройств SCSI

Внешние устройства Ultra160 и Ultra2 SCSI подключаются к 68-выводным внешним коннекторам LVD/SE SCSI. Для каждого внешнего устройства требуется 68-выводной внешний кабель VHDCI LVD SCSI. Для подключения внешних устройств SCSI необходимо сделать следующее.

1. Подключите один конец внешнего кабеля SCSI к одному из внешних коннекторов Ultra160 на хост-адаптере SCSI (типа платы SCSI Adaptec 39160). Чтобы достичь максимальной скорости передачи данных, следует подключать к внешним коннекторам SCSI исключительно устройства Ultra160 и Ultra2 SCSI. Кроме того, не стоит устанавливать на один и тот же канал SCSI платы хост-адаптера старые устройства SCSI и новые устройства Ultra160 и Ultra2 SCSI.
2. Подключите другой конец кабеля к SCSI-коннектору, расположенному на задней панели внешнего устройства. При установке только одного внешнего устройства его необходимо терминировать и перейти к шагу 4.
3. Подсоедините другие внешние устройства SCSI путем последовательного соединения каждого устройства с предыдущим (по принципу цепочечной топологии). Оконечную нагрузку следует ставить лишь на то устройство, которое является конечным в цепочке.
4. Подключите силовые кабели ко всем внешним устройствам и к компьютеру.

Замечания о дисках SCSI

Процесс подключения и терминирования дисков SCSI довольно прост, но с настройкой таких устройств связано несколько нюансов, которые следует иметь в виду. Нижеследующие рекомендации призваны помочь вам извлечь максимальную пользу из новых и уже установленных дисков SCSI.

- При подключении жесткого диска SCSI к новому хост-адаптеру нужно произвести повторное разделение и повторное форматирование жесткого диска. Прежде чем перемещать жесткий диск, следует создать резервную копию всех содержащихся на нем данных! Возможно, вам придется выполнить низкоуровневое форматирование диска SCSI, воспользовавшись для этого утилитой, встроенной в микропрограммное обеспечение хост-адаптера SCSI.
- Каждый жесткий диск SCSI должен быть физически отформатирован на низком уровне, разделен и логически отформатирован; только после этого его можно использовать для хранения данных. Большинство дисков SCSI форматируются производителем. Если предварительное форматирование вашего жесткого диска SCSI выполнено не было (а ваш компьютер работает в среде DOS или Windows), вы можете произвести его форматирование с помощью команд DOS FDISK или FORMAT.
- При использовании двухканального хост-адаптера SCSI подключите устройства LVD (Ultra160 и Ultra2) SCSI к каналу B SCSI, а устройства SCSI без интерфейса LVD — к каналу A SCSI. Это позволяет устройствам LVD SCSI работать с максимальной производительностью, составляющей 160 или 80 Мбайт/с соответственно. Или вы можете подключить устройства LVD SCSI к обоим каналам SCSI. В случае совмещения в рамках одного канала SCSI устройств SCSI с интерфейсом LVD и без него скорость передачи данных устройств LVD SCSI упадет до уровня производительности устройств SCSI без LVD, т. е. до 40 Мбайт/с.
- Терминирование внутренних устройств SCSI Ultra2 и Ultra160 отключается производителем, причем изменить эту настройку нельзя. Терминирование обеспечивается оконечной нагрузкой на конце внутреннего кабеля LVD SCSI.

Совмещение устройств SCSI с устройствами других типов

Хост-адаптер SCSI можно установить на компьютере, в котором уже есть контроллер другого типа (например, EIDE или Ultra-DMA). Но смешивать типы устройств на одном интерфейсе нельзя: устройства SCSI должны быть подключены к хост-адаптеру SCSI, устройства EIDE/UDMA — к соответствующему контроллеру и т. д. Если установить хост-адаптер и диски SCSI на компьютере, который загружается с диска другого типа, компьютер продолжит загружаться с этого диска до тех пор, пока вы не внесете изменения в настройки CMOS системы. Если вы предполагаете использовать диски SCSI лишь для получения дополнительного пространства хранения файлов, менять настройки не нужно. Если BIOS материнской платы вашего компьютера поддерживает функцию загрузочной спецификации BIOS (BBS, BIOS Boot Specification), то выбор нового загрузочного устройства не должен представлять сложности. В табл. 12.3 приводятся инструкции по применению различных типов дисков в рамках одной системы.

Таблица 12.3. Особенности загрузки систем, оснащенных SCSI

Поддерживает ли BIOS BBS?	Вы хотите, чтобы компьютер загружался с диска SCSI?	Тогда сделайте следующее:
Нет	Нет	Ничего делать не нужно. Допустимо совместное применение дисков SCSI и дисков других типов
Нет	Да	Запустите программу CMOS Setup. Для настройки **Primary Hard Disk** следует задать значение **None** или **Not Installed** (сверьтесь с документацией к компьютеру). Если вы загружаетесь с диска SCSI, то не сможете пользоваться жесткими дисками другого стандарта
Да	Нет	Ничего делать не нужно. Допустимо совместное применение дисков SCSI и дисков других типов
Да	Да	Запустите программу CMOS Setup и выберите в качестве загрузочного устройства диск SCSI. Допустимо совместное применение дисков SCSI и дисков других типов

Установка программного обеспечения

После установки аппаратной части вашего нового хост-адаптера SCSI пришло время установить драйверы адаптера SCSI и прикладные программы, которые будут необходимы для идентификации этого устройства операционной системой. Ниже представлены этапы, из которых обычно складывается эта процедура в средах Windows 2000, NT, 98 и NetWare, но при работе в других операционных системах (например, в UnixWare или Linux) вам следует ознакомиться с рекомендациями, содержащимися в документации к адаптеру. Устанавливать корпус системы пока рано; нужно лишь подсоединить к компьютеру шнур питающего напряжения и приготовиться к повторному запуску системы.

Примечание

Чтобы получить информацию о функциях адаптера SCSI и инструкции по установке его программного обеспечения, обратитесь к файлу README на диске с драйверами для адаптера SCSI.

Установка драйверов для Windows 2000

Практически все современные хост-адаптеры SCSI являются устройствами Plug-and-Play, и операционная система Windows 2000 обнаруживает их автоматически. Если вы хотите обеспечить поддержку SCSI со стороны сервера или рабочей станции, или обновить соответствующие драйверы, то для установки драйвера Window 2000 в системе Windows 2000 необходимо сделать следующее.

1. Установите плату хост-адаптера SCSI.
2. Включите питание компьютера. Windows 2000 обнаружит хост-адаптер SCSI и запустит мастер **Found New Hardware** (Обнаружено новое устройство). Нажмите кнопку **Next**.
3. Выберите **Display a list of the known drivers for this device so that I can choose a specific driver** (Вывести список известных драйверов для этого устройства, чтобы я мог выбрать один из них) и нажмите кнопку **Next** (Следующий).
4. В списке **Hardware Types** (Типы устройств) выберите **SCSI and RAID controllers** (SCSI- и RAID-контроллеры) и нажмите кнопку **Next**.
5. Нажмите кнопку **Have Disk** (Имеется диск). В результате откроется диалоговое окно **Install From Disk** (Установка с диска).
6. Поместите в дисковод для гибких дисков дискету с драйвером хост-адаптера SCSI, затем введите местонахождение драйвера для Windows 2000 (например, a:\w2k) и нажмите кнопку **OK**.
7. Выберите драйвер, подходящий для данного устройства (например, QLogic QLA1280, 64-bit PCI DUAL LVD SCSI HBA), и нажмите кнопку **Next**. Windows 2000 сообщит о том, что мастер готов к инсталляции драйвера. Теперь еще раз нажмите кнопку **Next**.
8. При появлении диалогового окна **Digital Signature Not Found** (Цифровая подпись не найдена) нажмите кнопку **Yes**, а затем — кнопку **Finish**.
9. Наконец, чтобы перезагрузить систему, нажмите кнопку **Yes**.

Обновление драйверов для Windows 2000

Время от времени, в целях исправления ошибок или повышения производительности устройства, может появиться необходимость в обновлении драйвера SCSI. Если вы обновляете драйвер для уже установленного хост-адаптера SCSI, сделайте следующее.

1. Выберите **Start** (Пуск), **Programs** (Программы), **Administrative Tools** (Администрирование), **Computer Management** (Управление компьютером).
2. Двойным щелчком выберите **System Tools** (Служебные программы), а затем **Device Manager** (Диспетчер устройств).
3. Двойным щелчком выберите **SCSI and RAID controllers**.
4. Двойным щелчком выберите нужный хост-адаптер SCSI (например, QLogic QLA1280, 64-bit PCI DUAL LVD SCSI HBA), а затем перейдите на вкладку **Driver** (рис. 12.4).
5. Нажмите кнопку **Update Driver**. В результате появится диалоговое окно **Upgrade Device Driver Wizard** (Мастер обновления драйвера устройства). Нажмите кнопку **Next**.
6. Выберите **Display a list of the known drivers for this device so that I can choose a specific driver** (Вывести список известных драйверов для этого устройства, чтобы я мог выбрать один из них) и нажмите кнопку **Next**.
7. Нажмите кнопку **Have Disk**. После этого появится диалоговое окно **Install From Disk**.

8. Поместите в дисковод дискету с драйвером QLogic, затем введите местонахождение драйвера для Windows 2000 (например, a:\w2k) и нажмите кнопку **OK**.
9. Выберите SCSI-адаптер (например, QLogic QLA1280, 64-bit PCI DUAL LVD SCSI HBA) и нажмите кнопку **Next**. Windows 2000 сообщит о том, что мастер готов к установке драйвера. Теперь еще раз нажмите кнопку **Next**.
10. В случае появления диалогового окна **Digital Signature Not Found** (Цифровая подпись не найдена) нажмите кнопку **Yes**.
11. Нажмите кнопку **Finish**; затем, чтобы перезапустить систему, нажмите **Yes**.

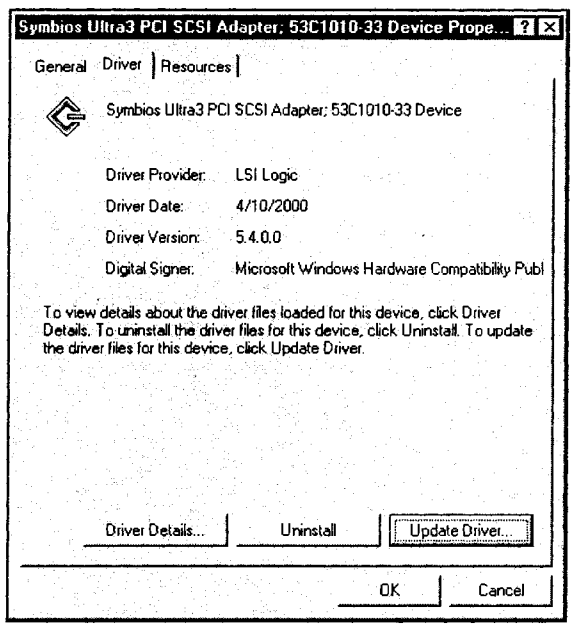


Рис. 12.4. В операционной системе Windows 2000 обновление драйверов SCSI проводится на вкладке **Driver** диалогового окна свойств (**Properties**) данного устройства

Установка драйверов для Windows NT

Процедура установки драйверов для Windows NT немного отличается от той, что принята в Windows 2000, но основные принципы остаются неизменными. Чтобы выполнить установку драйвера Windows NT в системе Windows NT 4.0, необходимо сделать следующее.

1. На рабочем столе выберите **My Computer** (Мой компьютер), **Control Panel** (Панель управления), **SCSI Adapters**.
2. Перейдите на вкладку **Driver** и нажмите кнопку **Add** (Добавить).
3. Вставьте в дисковод дискету с драйвером хост-адаптера SCSI для NT, а затем нажмите кнопку **Have Disk**.

4. Введите путь к драйверу Windows NT, расположенному на дискете (например, a:\nt), и нажмите кнопку **OK**.
5. Выберите подходящий драйвер (например, QLogic QLA1280, 64-bit PCI DUAL SCSI LVD HBA) и нажмите кнопку **OK**.
6. Извлеките из дисковода дискету и нажмите кнопку **Yes**, чтобы перезагрузить систему.

Обновление драйверов для Windows NT

Время от времени, в целях исправления ошибок или повышения производительности устройства, может появиться необходимость в обновлении драйвера SCSI. Если вы хотите обновить установленный драйвер SCSI для Windows NT, сделайте следующее.

1. Откройте окно командной строки DOS.
2. Перейдите из текущего каталога в каталог, в котором находится драйвер для Windows NT (например, `cd \winnt\system32\drivers`).
3. Сделайте резервную копию старого драйвера. Ее можно сохранить в тот же каталог с расширением .SAV — оно будет обозначать сохраненный файл (например, `copy ql1280.sys ql1280.sav`).
4. Вставьте в дисковод дискету с новым драйвером хост-адаптера SCSI.
5. Скопируйте новый драйвер, заменив им старый (например, `copy a:\nt\ql1280.sys`).
6. Чтобы загрузить новый драйвер, необходимо перезапустить систему.

Установка драйверов для NetWare

Чтобы определить подходящий драйвер хост-адаптера SCSI в среде NetWare, нужно воспользоваться режимом реального времени. Для установки драйверов SCSI в системе NetWare 4.x/5.x необходимо сделать следующее:

1. Запустите NetWare и с помощью серверной командной строки (:) загрузите программу NetWare Install. К примеру, в среде NetWare 4.11 или 4.2 следует ввести `load install`. В системе NetWare 5.x нужно ввести `load nwconfig`.
2. В главном меню выберите **Driver options**.
3. Выберите **Configure disk and storage device drivers** (Настроить диск и драйверы запоминающего устройства).
4. Выберите **Select an additional driver** (Выбрать дополнительный драйвер).
5. Чтобы установить драйвер, не включенный в список, нажмите клавишу <Insert>.
6. Поместите в дисковод дискету с драйвером хост-адаптера SCSI.
7. Чтобы выбрать подходящий драйвер .HAM, нажмите клавишу <Enter>.
8. Чтобы скопировать драйвер с дискеты в каталог на сервере, нажмите кнопку **Yes**.
9. Если к плате SCSI подключен привод CD-ROM, вам нужно будет загрузить файл CDROM.NLM (например, ввести `load cdrom.nlm`), поставляемый в комплекте NetWare, что позволяет создавать тома CD-ROM на сервере.

10. При подключении нескольких устройств LUN (таких как устройства смены лент) следует добавить к строке LOAD ключ /LUN (например, `load ql1280.ham slot=xx /lun`).
11. Если устройства SCSI требуют обеспечения поддержки ASPI, вы должны загрузить модуль NWASPI.CDM, поставляемый в комплекте NetWare (например, ввести `load nwaspi.cdm`).

Установка драйверов для Windows 98

Хотя операционная система Windows 98/ME не самый удачный выбор для серверных приложений, она широко применяется для рабочих станций, а также обеспечивает поддержку хост-адаптеров SCSI. Для установки драйвера хост-адаптера SCSI в системе с операционной системой Windows 98 сделайте следующее.

1. Установите новый хост-адаптер SCSI.
2. Перезагрузите систему. После обнаружения в слоте PCI платы хост-адаптера SCSI на экране появится окно **New Hardware Found** (Обнаружено новое оборудование).
3. Вставьте в дисковод дискету с драйвером SCSI и нажмите кнопку **Next**.
4. Выберите **Display a list of all the drivers in a specific location, so you can select the driver you want** (Вывести список всех драйверов, находящихся в определенном месте, чтобы вы могли выбрать подходящий драйвер) и нажмите кнопку **Next**.
5. При появлении приглашения выбрать тип устройства выберите **SCSI Controllers** и нажмите кнопку **Next**.
6. Нажмите кнопку **Have Disk**, введите путь к новому драйверу a:\win9x и нажмите кнопку **OK**.
7. Проверьте, выбран ли новый адаптер SCSI (например, Qlogic QLA1280 LVD PCI Dual SCSI Adapter), и нажмите кнопку **Next**.
8. Нажмите **Next** еще раз, а затем, когда мастер обнаружит обновленный драйвер, нажмите кнопку **Finish**.
9. При появлении соответствующего приглашения извлеките дискету из дисковода и перезагрузите систему.

Настройка BIOS SCSI

Большинство хост-адаптеров SCSI, устанавливаемых в виде устройства расширения или встроенных в серверную материнскую плату, используют BIOS (или микропрограммное обеспечение) для настройки своих различных функций. Чаще всего достаточно настроек SCSI BIOS, принимаемых по умолчанию, и необходимость в изменении конфигурации хост-адаптера отсутствует. Но иногда вам может потребоваться изменить настройки по умолчанию при конфликте между настройками устройств, при необходимости оптимизировать производительность системы или активизировать специальные функции SCSI (например, низкоуровневое форматирование жесткого диска SCSI). В этой части главы рассматриваются принимаемые по умолчанию настройки типичного хост-адаптера SCSI компании Adaptec и объясняется значение многих настроек SCSI BIOS, с которыми вы можете столкнуться. Настройки, которые обычно принимаются по умолчанию, приведены в табл. 12.4.

Таблица 12.4. *Общие настройки SCSI BIOS для хост-адаптера SCSI*

Опции SCSI Select	Допустимые настройки	Настройка по умолчанию
Опции интерфейса шины SCSI		
Host Adapter SCSI ID (идентификатор SCSI хост-адаптера)	0–15	7
SCSI Parity Checking (проверка четности SCSI)	Enabled (включено); Disabled (отключено)	Enabled
Host Adapter SCSI Termination (терминирование хост-адаптера SCSI)	Канал A: Automatic (автоматическое), Low On/High On (низкое включить/высокое включить), Low Off/High Off (низкое выключить/высокое выключить), Low Off/High On (низкое выключить/высокое включить)	Automatic
	Канал B: Automatic, Enabled, Disabled	Automatic
Опции загрузочного устройства		
Boot Channel (канал загрузки)	A First (сначала A), B First (сначала B)	A First
Boot SCSI ID (идентификатор загрузочного SCSI)	0–15	0
Boot LUN Number (загрузочный номер LUN)	0–7	0
Конфигурация устройств SCSI		
Sync Transfer Rate, MB/s (скорость синхронной передачи, Мбайт/с)	160; 80,0; 53,4; 40,0; 32,0; 26,8; 20,0; 16,0; 13,4; 10,0; ASYN (асинхронная передача)	160
Initiate Wide Negotiation (инициировать широкое согласование)	Yes (да), No (нет)	Yes (Enabled)
Enable Disconnection (разрешить отсоединение)	Yes, No	Yes (Enabled)
Send Start Unit Command (отсылать команду стартового устройства)	Yes, No	Yes (Enabled)
Enable Write Back Cache (включить кэш на запись)	Yes, No, N/C (No Change, без изменений)	N/C (No Change)
BIOS Multiple LUN Support (поддержка множественных LUN со стороны BIOS)	Yes, No	No (Disabled)

Таблица 12.4 (окончание)

Опции SCSI Select	Допустимые настройки	Настройка по умолчанию
Include in BIOS Scan (включить в поиск BIOS)	Yes, No	Yes (Enabled)
Расширенные конфигурационные опции		
Reset SCSI Bus at IC Initialization (сбрасывать шину SCSI при инициализации интегральной схемы)	Enabled, Disabled	Enabled
Display <CTRL><A> Messages during BIOS initialization (выводить сообщения <Ctrl><A> во время инициализации BIOS)	Enabled, Disabled	Enabled
Extended BIOS Translation for DOS Drives > 1 GB (преобразование расширенной системы BIOS для дисков DOS > 1 Гбайт)	Enabled, Disabled	Enabled
Verbose/Silent Mode (расширенный/бесшумный режим)	Verbose (расширенный), Silent (бесшумный)	Verbose
Host Adapter BIOS (BIOS хост-адаптера)	Enabled, Disabled: Scan Bus (отключено: сканировать шину), Disabled: Not Scan (отключено: не сканировать шину)	Enabled
Domain Validation (проверка достоверности домена)	Enabled, Disabled	Enabled
Support Removable Disks Under BIOS as Fixed Disks (в условиях BIOS обеспечивать работу съемных дисков как несъемных)	Disabled, Boot Only (только загрузочный), All Disks (все диски)	Disabled
BIOS Support for Bootable CD-ROM (поддержка BIOS загрузочных приводов CD-ROM)	Enabled, Disabled	Enabled
BIOS Support for Int 13 Extensions (поддержка BIOS расширений Int 13)	Enabled, Disabled	Enabled

Примечание

Данные инструкции и опции представлены здесь лишь для примера, и их конкретные реализации зависят от адаптера SCSI. Указания по навигации меню и опции, доступные в вашем хост-адаптере, можно найти в руководстве пользователя хост-адаптера.

Применение SCSI BIOS

Доступ к микропрограммному обеспечению хост-адаптера SCSI можно получить сразу после выполнения процедуры POST, когда система позволит войти в CMOS Setup. В ходе процесса инициализации вы увидите сообщение типа

```
Press <Ctrl><A> for SCSISelect Utility
```

Чтобы запустить утилиту SCSI Setup (SCSISelect), необходимо ввести указанное сочетание клавиш. При наличии нескольких доступных каналов вы можете указать тот из них, с которым хотите работать (например, канал A или канал B). В появившемся меню установок с помощью клавиш стрелок вы можете переходить от одной опции к другой, а выбирать их клавишей <Enter>. После завершения просмотра или изменения опций SCSI нажмите клавишу <Esc>, пока не появится приглашение выйти из программы и сохранить изменения. Выберите **Yes**, и система выполнит перезагрузку.

Настройки SCSI BIOS

Запустив утилиту SCSI BIOS, вы сможете изменить большое количество настроек и рабочих параметров, среди которых есть и нижеперечисленные (значения по умолчанию приведены в скобках).

- Host Adapter SCSI ID (идентификатор SCSI хост-адаптера) (7). Установка идентификатора SCSI для платы SCSI. Большинству плат SCSI (в том числе и Adaptec 39160) присваивается идентификатор 7, с помощью которого они получают наивысший приоритет в рамках шины SCSI. Как правило, эту настройку менять не нужно.
- SCSI Parity Checking (проверка четности SCSI) (Enabled, включено). Во включенном (Enabled) состоянии эта функция проверяет точность передачи данных по шине SCSI. Отключать эту настройку следует лишь в том случае, если какое-либо устройство SCSI, подключенное к хост-адаптеру SCSI, не поддерживает проверку четности.
- Host Adapter SCSI Termination (терминирование хост-адаптера SCSI) (Automatic, автоматически). Определяет настройку терминирования платы SCSI. По умолчанию принято значение Automatic, что позволяет плате SCSI при необходимости изменять эту настройку. В большинстве случаев изменять эту настройку не следует.
- Boot Channel (канал загрузки) (A First, сначала A). Если компьютер загружается с устройства SCSI, этот параметр определяет, к какому из двух каналов SCSI это загрузочное устройство подключено. Внесенные в этот параметр изменения автоматически применяются к обоим каналам SCSI. На хост-адаптерах SCSI с одним каналом эта опция недоступна.
- Boot SCSI ID (идентификатор загрузочного SCSI) (0). Определяет идентификатор SCSI загрузочного устройства; по умолчанию приравнивается к нулю. Как правило, эту настройку менять не нужно. Внесенные в этот параметр изменения автоматически применяются к обоим каналам SCSI.
- Boot LUN Number (загрузочный номер LUN) (0). Определяет, с какого номера логического модуля (LUN) загрузочного устройства производится загрузка. Эта настройка действительна лишь в том случае, если активирована функция Multiple LUN Support (поддержка множественных LUN). Внесенные в эту настройку изменения автоматически применяются к обоим каналам SCSI.

- Sync Transfer Rate (скорость синхронной передачи) (160). Определяет максимальную скорость синхронной передачи данных, поддерживаемую платой SCSI. Как правило, нужно оставить максимальное значение 160 Мбайт/с, принимаемое по умолчанию.
- Initiate Wide Negotiation (инициировать широкое согласование) (Yes, да). При значении Yes плата SCSI осуществляет 16-битовую передачу данных (широкое согласование). При значении No плата SCSI использует 8-битовую передачу данных, кроме случаев, когда устройство SCSI подает специальный запрос на выполнение широкого согласования. Задавать значение No нужно тогда, когда вы пользуетесь 8-битовым устройством SCSI, которое в условиях 16-битовой передачи данных зависает или обнаруживает другие проблемы, связанные с производительностью.
- Enable Disconnection (разрешить отсоединение) (Yes, да). В значении Yes эта настройка позволяет устройству SCSI отсоединяться от шины SCSI. Сохранять значение Yes следует в том случае, если к плате SCSI подключено два или несколько устройств SCSI. Если к ней подключено только одно устройство SCSI, значение No позволяет немного повысить производительность.
- Send Start Unit Command (отсылать команду стартового устройства) (Yes, да). Если установлено значение Yes, то при запуске устройству SCSI отсылается команда Start Unit Command (команда стартового устройства). (Три следующих настройки не действуют, если система BIOS платы SCSI отключена; обычно это система включается по умолчанию.)
- Enable Write Back Cache (включить кэш на запись) (N/C, без изменений). С помощью этой опции можно включать или выключать кэш с обратной записью, расположенный на подключенных к хост-адаптеру дисках SCSI. Оптимальная производительность диска обычно обеспечивается настройкой по умолчанию (N/C).
- BIOS Multiple LUN Support (поддержка множественного LUN со стороны BIOS) (No, нет). Сохранить значение No следует в том случае, если устройство не имеет множественных номеров LUN. При значении Yes SCSI BIOS обеспечивает поддержку загрузки устройства SCSI с множественными номерами LUN (например, дисковода с автоматической сменой компакт-дисков, в котором возможен одновременный доступ к нескольким дискам).
- Include in BIOS Scan (включить в поиск BIOS) (Yes). Если установлено значение Yes, то при запуске SCSI BIOS включает данное устройство в процедуру поиска BIOS.
- Reset SCSI Bus at Initialization (сбрасывать шину SCSI при инициализации) (Enabled). Если установлено значение Enabled, плата SCSI вызывает сброс шины в ходе ее инициализации при включении и после полного сброса.
- Display Messages during BIOS Initialization (выводить сообщения во время инициализации BIOS) (Enabled). Если установлено значение Enabled, то во время запуска центральной системы SCSI BIOS выводит загрузочное сообщение (например, "Press <CTRL><A> for SCSI Select Utility"). Если эта функция отключена, вызов утилиты SCSI BIOS производится путем нажатия необходимых клавиш после появления заголовка SCSI BIOS. Внесенные изменения автоматически применяются к обоим каналам SCSI.

- Extended BIOS Translation for DOS Drivers > 1 GB (расширенная трансляция адресов системой BIOS для дисков DOS > 1 Гбайт) (Enabled). При установленном значении Enabled для жестких дисков SCSI емкостью более 1 Гбайт предусматривается расширенная схема трансляции адресов. Эта настройка актуальна лишь для DOS 5.0 и более поздних систем и не требуется в операционных системах типа NetWare или Linux/UNIX.

Примечание

В результате изменения схемы трансляции адресов все данные, находящиеся на диске, уничтожаются. Перед выполнением этой процедуры содержимое дисков нужно обязательно резервировать.

- Verbose/Silent Mode (расширенный/скрытый режим). При выборе значения Verbose система BIOS платы SCSI в ходе запуска выводит на экран данные о модели хост-адаптера. При значении Silent это сообщение во время запуска не отображается. Внесенные в эту настройку изменения автоматически применяются к обоим каналам SCSI.
- Host Adapter BIOS (BIOS хост-адаптера) (Enabled). Эта функция включает и отключает систему BIOS платы SCSI. Внесенные изменения автоматически применяются к обоим каналам SCSI. Если вы хотите, чтобы система SCSI BIOS сканировала и инициализировала все устройства SCSI, оставьте эту настройку разрешенной. Если устройства на шине SCSI (например, приводы CD-ROM) управляются программными драйверами и не нуждаются в применении BIOS, и при этом вы не хотите, чтобы BIOS сканировала шину, установите значение Disabled: Not Scan (отключено: не сканировать). Если необходимость в использовании системы BIOS отсутствует, но вы хотите, чтобы BIOS сканировала находящиеся на шине SCSI устройства, и в то же время вам требуется разогнать определенное устройство, задайте значение Disabled: Scan Bus (отключено: сканировать шину). (Когда система SCSI BIOS отключена, четыре нижеследующих опции недействительны.)
- Domain Validation (проверка достоверности домена) (Enabled). Для каждого устройства на шине SCSI эта настройка определяет оптимальную скорость передачи и соответствующим образом устанавливает значения скоростей. Кроме того, она выводит результирующую скорость передачи данных. Внесенные изменения автоматически применяются к обоим каналам SCSI.
- Support Removable Disks Under BIOS as Fixed Disks (средствами BIOS обеспечивать работу съемных дисков как несъемных) (Disabled). Эта настройка определяет, какие съемные носители поддерживаются системой BIOS платы SCSI. В отключенном состоянии съемные диски вообще не рассматриваются как жесткие диски. Так как эти диски не управляются BIOS, для их работы необходимо наличие программных драйверов. В режиме Boot Only (только загрузочный) в качестве жесткого диска рассматривается только тот съемный диск, который отмечен как загрузочное устройство. В режиме All Disks (все диски) жесткими дисками считаются все съемные диски, поддерживаемые BIOS.
- BIOS Support for Bootable CD-ROM, поддержка BIOS загрузочных приводов CD-ROM (Enabled). При включении этой настройки SCSI BIOS позволяет системе загружаться с привода CD-ROM.

- BIOS Support for Int 13 Extensions (поддержка BIOS расширений Int 13) (Enabled). При значении Enabled система BIOS платы SCSI обеспечивает поддержку расширений Int 13h. Эту настройку можно как включить, так и отключить (если ваша система не поддерживает стандарт Plug-and-Play).

Поиск неисправностей SCSI

Что касается самой шины, то для нее неисправности нехарактерны — провода и коннекторы не могут самопроизвольно выйти из строя. Впрочем, чтобы убедиться в сохранности физических соединений (особенно после установки или настройки новых устройств), проверить проводку, коннекторы и схему (схемы) оконечной нагрузки не помешает. Среди областей, возникновение неисправностей в которых наиболее вероятно, стоит назвать установку, настройку и функционирование устройств на шине.

Локализация неисправностей

Предположим, что установка устройств SCSI была произведена правильно; тогда сбои могут происходить в ходе их нормальной эксплуатации. Первым показателем неисправности обычно бывает сообщение об ошибке, генерируемое операционной системой или прикладной программой. К примеру, возможно, не отвечает жесткий диск SCSI, центральная система не определяет плату хост-контроллера SCSI и т. д.

Преимуществом архитектуры SCSI является то, что в ее рамках неисправность сравнительно просто локализовать с помощью интуитивных умозаключений. Рассмотрим типичную систему SCSI с одним инициатором (хост-контроллером) и одним целевым устройством (например, с жестким диском). Жесткий диск может перестать работать либо из-за собственного сбоя, либо из-за неисправности хост-контроллера. Если в ответ на попытки обращения к диску генерируются ошибки, значит, неисправность, вероятно, кроется в самом диске. Если перед выводом ошибки обращения к диску не происходит, значит, неисправен хост-контроллер. В качестве другого примера рассмотрим сборку в составе одного инициатора и двух или нескольких целевых устройств (например, жесткого диска и привода CD-ROM). Если работать перестают и жесткий диск, и CD-ROM, значит, скорее всего, вышел из строя хост-адаптер, т. к. именно он управляет обоими целевыми устройствами. Если не функционирует лишь одно из устройств (а другое работает), значит, видимо, неисправность нужно искать именно в этом устройстве.

Общие рекомендации по поиску неисправностей

Какие бы меры предосторожности вы ни предприняли, предотвратить все возможные неисправности во время установки или замены устройств SCSI вам не удастся. Но при последовательной установке устройств область поиска неисправностей значительно снижается. Первым диагностическим средством при установке устройств SCSI для вас должно послужить сообщение об инициализации SCSI BIOS. Если при запуске системы это сообщение не появляется, высока вероятность неисправности самого хост-адаптера. Либо он неправильно установлен, а его система BIOS отключена, либо адаптер вышел из строя. Проверьте, назначен ли адаптеру соответствующий идентификатор (как правило, ID 7). Попробуйте воспользоваться новым или

запасным адаптером SCSI. Если сообщение об инициализации адаптера, как и ожидалось, появляется, то неисправность, вероятно, имеет отношение к установке драйвера. Проверьте установку и любые переключатели командной строки для драйверов каждого устройства. При установке жесткого диска SCSI на место дисков IDE необходимо убедиться в том, что все предыдущие ссылки на жесткие диски исключены ("выведены") из настроек CMOS путем задания значений "отсутствует" (none) или "не установлено" (not installed). Если старые ссылки не удалены, система будет пытаться загрузиться с дисков IDE, которых уже нет.

Имейте в виду, что ошибочные настройки идентификаторов SCSI могут привести к системным проблемам вроде "призраков" дисков — дисков, которые, как утверждает система, установлены, но операции записи и считывания с которых невозможны. С назначенными идентификаторами также отказываются работать некоторые периферийные устройства. В случае появления затруднений при взаимодействии с установленным устройством, попробуйте назначить ему другой идентификатор и убедитесь в том, что он не используется другими устройствами. Не удивляйтесь тому, что некоторые типы кабелей плохо работают со сборками SCSI. Проверьте правильность расстановки оконечных нагрузок. Убедитесь в том, что все внешние устройства SCSI получают питание еще до инициализации системы (если это возможно). Если неисправность сохранится, попробуйте воспользоваться другими кабелями. Ниже представлен краткий контрольный список.

- ❒ Проверьте питание всех устройств SCSI (убедитесь в том, что мощности источника питания хватает на все подключенные устройства SCSI).
- ❒ Проверьте 50- или 68-выводной сигнальный кабель, с помощью которого производится подключение всех устройств SCSI. Это должен быть высококачественный кабель, надежно закрепленный на каждом из таких устройств.
- ❒ Проверьте ориентацию каждого коннектора на кабеле SCSI. Вывод 1 должен быть правильно размещен.
- ❒ Проверьте идентификатор SCSI каждого устройства. Дублирование идентификаторов разрешается исключительно в случае применения обозначений LUN. Возможность дублирования возникает при использовании большого количества устройств SCSI, например — в системе RAID.
- ❒ Проверьте надежность терминирования обоих концов кабеля SCSI и убедитесь в том, что оконечные нагрузки находятся в активном состоянии.
- ❒ Проверьте настройки контроллера SCSI (IRQ, I/O, адреса BIOS и другие параметры). Убедитесь в том, что контроллер SCSI не конфликтует с другими устройствами в системе.
- ❒ Проверьте систему BIOS хост-адаптера SCSI. В случае, если загрузка с жестких дисков SCSI не происходит, SCSI BIOS, как правило, можно отключить. Это также упростит настройку устройств. Возможно, чтобы устранить неисправности, связанные с производительностью или совместимостью, вам нужно обновить BIOS хост-адаптера.
- ❒ Запустите CMOS Setup и проверьте настройки дисков. Если в системе есть диски SCSI, но отсутствуют жесткие диски IDE/EIDE, убедитесь в том, что записи CMOS для дисков настроены на "none" (отсутствует) или "not installed" (не установлено).

- Запустите CMOS Setup и проверьте настройки шины PCI. Убедитесь в том, что слот PCI, в который установлен хост-адаптер SCSI, активен и использует уникальное прерывание (обычно оно называется IRQ A). Кроме того, следует активировать функцию управления передачей данных по шине.
- Проверьте наличие драйверов реального режима — это актуально для DOS и вариантов сетевых операционных систем типа NetWare. При работе в среде DOS проверьте, установлены ли в файлах CONFIG.SYS и AUTOEXEC.BAT все необходимые драйверы хост-адаптера и устройств, не являющихся жесткими дисками.
- При работе в среде Windows 98/ME/NT/2000 следует проверить наличие всех необходимых драйверов защищенного режима для хост-адаптера и устройств SCSI. Хост-адаптер SCSI должен надлежащим образом идентифицироваться мастером адаптеров SCSI (SCSI Adapters Wizard).
- Если неисправности возникают только в среде Windows 98/ME/NT/2000, попробуйте понаблюдать за драйверами реального режима. Иногда драйверы SCSI реального режима конфликтуют с драйверами SCSI защищенного режима. Если система SCSI нормально работает в DOS, но некорректно в Windows, попробуйте временно отключить драйверы DOS в загрузочных файлах.

Симптомы неисправностей

Даже наилучшим образом спроектированные сборки SCSI время от времени выходят из строя, а те системы SCSI, что уже работают, будут функционировать не вечно. Рано или поздно вам придется столкнуться с неисправностью SCSI. В этой части главы мы опишем разнообразные признаки неисправности SCSI, с которыми вы, возможно, столкнетесь, и способы устранения неисправностей.

Симптом 12.1. Появляется ошибка типа "Устройство подключено, но не готово"

Такая ошибка указывает на то, что центральная система не получила ответа на запрос данных, направленный установленному устройству SCSI (т. е. жесткому диску). Запустите утилиту SCSI BIOS Setup и задайте значение Yes параметра **Send Start Unit Command** для идентификатора устройства SCSI (к примеру, первому жесткому диску SCSI обычно присваивается идентификатор ID0). Убедитесь в том, что в настройках подозрительного устройства значится разгон при включении питания. Эта настройка, как правило, выполняется с помощью перемычки на самом устройстве; чтобы узнать конкретные установки перемычек обратитесь к документации устройства.

Симптом 12.2. Появляется ошибка типа "Неудачный запрос стартового устройства"

Системе SCSI BIOS не удалось инициировать команду Send Start Unit (отсылать команду стартового устройства) одному из установленных устройств SCSI. В первую очередь убедитесь в том, что данное устройство надежно подключено к источнику питания. Далее запустите утилиту SCSI BIOS Setup и отключите для этого устройства настройку Send Start Unit Command. Если проблема повторится, возможно, неисправно устройство SCSI и его нужно заменить.

Симптом 12.3. Появляется ошибка типа "Отказ по времени в ходе..."

В ходе попытки обмена информацией с устройством SCSI произошла непредвиденная блокировка по превышению лимита времени. Для начала убедитесь в правильности терминирования шины SCSI и надежности подключения всех силовых и сигнальных кабелей. Затем изолируйте потенциально неисправные устройства SCSI — попробуйте отсоединить их кабели от платы SCSI, а затем перезагрузить компьютер. Если система успешно запустится, то значит, вероятнее всего, неисправно отключенное устройство SCSI.

Симптом 12.4. Появляется ошибка, в соответствии с которой "на однопроводных коннекторах терминировано слишком много устройств"

Система SCSI BIOS обнаружила на однопроводном (SE) сегменте кабеля более двух терминированных устройств. Проверьте оконечные нагрузки на 68- или 50-выводных внутренних однопроводных коннекторах, имея в виду, что терминирование должно быть выполнено лишь на последнем устройстве SCSI каждого кабеля. Удалите или отключите оконечные нагрузки на устройствах, расположенных между концами кабелей. Если ни к одному из таких коннекторов устройства SCSI не подключены, задайте для опции терминирования SCSI BIOS коннектора SE значение Automatic (автоматически) или Enable (включить).

Симптом 12.5. Появляется ошибка, в соответствии с которой "на однопроводных коннекторах установлено недостаточное терминирование"

Система SCSI BIOS обнаружила на однопроводном сегменте кабеля менее двух терминированных устройств. Проверьте оконечные нагрузки на 68- или 50-выводных внутренних однопроводных коннекторах, учитывая, что терминирование должно быть задействовано лишь на последнем устройстве SCSI каждого кабеля. Удалите или отключите оконечные нагрузки на устройствах, расположенных между концами кабелей. Если ни к одному из таких коннекторов устройства SCSI не подключены, задайте для опции терминирования SCSI BIOS коннектора SE значение Automatic (автоматически) или Enable (включить).

Симптом 12.6. Появляется ошибка, в соответствии с которой "на коннекторах LVD/SE терминировано слишком много устройств"

Система BIOS платы SCSI обнаружила на сегменте LVD/SE кабеля более чем два терминированных устройства. Проверьте оконечные нагрузки на внутреннем и/или внешнем 68-выводных коннекторах LVD/SE. Необходимо терминировать только последнее устройство SCSI каждого кабеля. Удалите или отключите оконечные нагрузки на устройствах, расположенных между концами кабелей. Если ни к одному из таких коннекторов устройства SCSI не подключены, задайте для опции терминирования SCSI BIOS коннектора LVD/SE значение Automatic (автоматически) или Enable (включить).

Симптом 12.7. Появляется ошибка, в соответствии с которой "на коннекторах LVD/SE установлено недостаточное терминирование"

Система BIOS платы SCSI обнаружила на сегменте LVD/SE кабеля менее двух завершающих устройств. Проверьте оконечные нагрузки на внутреннем и/или внеш-

нем 68-выводных коннекторах. Удалите или отключите оконечные нагрузки на устройствах, расположенных между концами кабелей. Если ни к одному из таких коннекторов устройства SCSI не подключены, задайте для опции терминирования SCSI BIOS коннектора LVD/SE значение Automatic (автоматически) или Enable (включить).

Симптом 12.8. После первоначальной установки SCSI система не загружается с флоппи-дисковода

Возможно, код ошибки, соответствующий этой неисправности, будет выведен на экран, но этого может и не произойти. В первую очередь следует проверить хост-адаптер SCSI. Есть вероятность внутренней неисправности адаптера, конфликтующего с операциями системы. Убедитесь в правильности настроек адаптера и неизменности положений всех его перемычек. Если адаптер оборудован диагностическими светодиодами, проверьте, не сигнализируют ли они о появлении сбоев. Если да, то следует заменить плату адаптера. Если после установки жесткого диска SCSI его светодиод беспрерывно светится, то, вероятно, направление сигнального кабеля SCSI между этим диском и адаптером выбрано неправильно. Кабель диска необходимо проложить надлежащим образом.

Посмотрите, какое сообщение SCSI BIOS выводится на экран при запуске системы. Если это сообщение вообще не появляется, убедитесь в отсутствии конфликта на уровне адресов ПЗУ между адаптером SCSI и ПЗУ или другими платами расширения. Попробуйте назначить адаптеру SCSI новый адрес. Если на адаптере установлен драйвер режима ожидания BIOS, попытайтесь изменить эту настройку. При появлении сообщения об ошибке, в соответствии с которым хост-адаптер SCSI, расположенный по определенному адресу, не обнаружен, проверьте его настройку ввода/вывода.

В состав большинства современных хост-адаптеров SCSI входит контроллер гибких дисков. Это может привести к конфликту с другим таким же контроллером. Если вы хотите продолжать пользоваться существующим контроллером гибких дисков, обязательно отключите этот контроллер, встроенный в адаптер. Или при желании оставить встроенный контроллер необходимо отключить существующий порт контроллера гибких дисков.

Симптом 12.9. Система не загружается с жесткого диска SCSI

Для начала запустите системную утилиту CMOS Setup. При установке в системе ПК дисков SCSI соответствующая ссылка на жесткий диск в CMOS Setup должна быть изменена на "none" (отсутствует) или "not installed" (не установлено) — при этом предполагается, что жесткие диски IDE/EIDE в системе использоваться не будут. Если старые ссылки на жесткий диск еще не ликвидированы, сделайте это сейчас, сохраните изменения, произведенные в CMOS Setup, и перезагрузите систему. Если проблема сохранится, проверьте, назначен ли данному жесткому диску SCSI идентификатор ID0. Чтобы узнать, как идентификатор устанавливается на конкретной модели диска, обратитесь к документации к диску.

Теперь обратите внимание на контроль по четности SCSI — во всех устройствах SCSI этот параметр должен быть установлен единообразно. Помните, что контроль по четности SCSI должен быть включен или отключен на всех без исключения устройствах SCSI — если хотя бы одно устройство в цепочке SCSI не поддерживает

контроль по четности, его необходимо отключить на всех устройствах. Проверьте кабели SCSI и убедитесь в том, что все они надежно установлены и терминированы. Наконец, не забывайте, что жесткий диск должен быть надлежащим образом разделен и отформатирован. Если это не так, выполните загрузку с гибкого диска и в соответствии со всеми требованиями, пользуясь FDISK и FORMAT, подготовьте жесткий диск.

Симптом 12.10. Когда загрузочным является другой жесткий диск, диск SCSI не отвечает

Технически это возможно — пользоваться диском SCSI (который может быть, например, диском D:), когда функция загрузочного диска исполняется диском IDE/EIDE. Если в таких условиях диск SCSI не отвечает, проверьте настройки CMOS и убедитесь, что ссылки на диск 1 (SCSI) ликвидированы (т. е. ему соответствует настройка "none" или "not installed"). Сохраните внесенные в CMOS Setup изменения и перезагрузите систему. Если неисправность сохранится, убедитесь в том, что для диска SCSI назначен идентификатор SCSI ID1 (соответствующий несистемному диску). Затем проверьте соответствие настроек контроля по четности во всех устройствах SCSI. Если контроль по четности включен в одних устройствах, но отключен в других, система SCSI может работать неустойчиво. Наконец, проверьте кабели SCSI и убедитесь в том, что все они надежно установлены и терминированы. Неправильная проводка кабелей и ошибочная расстановка оконечных нагрузок вполне могут препятствовать нормальной работе системы SCSI. Если проблема сохранится, попробуйте воспользоваться другим жестким диском.

Примечание

В современных хост-адаптерах SCSI применяется система BIOS, которая позволяет дискам SCSI загружаться даже при наличии в компьютере дисков IDE/EIDE. В подобной конфигурации определить, какое устройство будет загрузочным — A:, C: или SCSI, — помогает настройка "Boot Order" (загрузочная последовательность) утилиты CMOS Setup.

Симптом 12.11. Когда загрузочным является один диск SCSI, другой жесткий диск того же типа не отвечает

Как правило, это происходит в двухдисковой системе, в которой используется два диска SCSI. Запустите CMOS Setup и убедитесь в том, что в записях обоих дисков стоят значения "none" (отсутствует) или "not installed" (не установлено). Сохраните изменения, произведенные в CMOS Setup. Идентификатором SCSI загрузочного диска должен быть ID0, а дополнительного диска — ID1 (чтобы узнать, как выбрать идентификаторы SCSI, обратитесь к документации диска). На жестких дисках должны присутствовать разделы DOS; кроме того, они должны быть отформатированы. Если это не так, необходимо создать эти разделы (FDISK) и отформатировать диски (FORMAT). Убедитесь в том, что установки контроля по четности (его разрешение или отключение) всех дисков системы SCSI не противоречат друг другу. Если в одних устройствах контроль по четности используется, а в других — нет, система SCSI может работать некорректно. Убедитесь в надежности монтажа и терминирования всех кабелей SCSI. Если проблема сохранится, попробуйте последовательно заменить каждый жесткий диск.

Симптом 12.12. Система работает нестабильно. Компьютер зависает, или адаптер SCSI не может обнаружить диски

Такое неустойчивое функционирование может быть обусловлено несколькими факторами. Прежде чем предпринимать какие-либо действия, убедитесь в том, что причиной возникновения проблемы не является прикладное программное обеспечение, которым вы в это время пользовались. Нестабильные или дефектные программы способны серьезно повлиять на работу системы. Попробуйте запустить другие приложения и проверьте, будет ли система зависать и во время их работы (кроме того, воспользуйтесь диагностическими утилитами DOS, сопровождающими хост-адаптер). Проверьте каждое устройство SCSI и убедитесь в том, что установки контроля по четности (его разрешение или отключение) всех дисков в рамках системы SCSI не противоречат друг другу. Если в одних устройствах контроль по четности применяется, а в других он отключен, система SCSI может работать нестабильно. Проверьте правильность и надежность подключения всех кабелей SCSI. Кроме того, следует убедиться в том, что кабели должным образом терминированы.

Причиной этой неисправности может быть конфликт на уровне распределения ресурсов между хост-адаптером SCSI и другой платой в системе. Проверьте каждую плату расширения в рамках системы и убедитесь в том, что ни одна из них не использует те же IRQ, DMA и адрес I/O, что и хост-адаптер (или зайдите в **Device Manager** (Диспетчер устройств) в операционной системе Windows). В случае обнаружения конфликта следует внести изменения в ту плату адаптера, которая была установлена последней. Если проблема сохранится, попробуйте установить новую плату адаптера диска.

Симптом 12.13. Выводится код ошибки 096xxxx

Это диагностический код ошибки, который указывает на наличие неисправности, связанной с 32-битовой платой хост-адаптера SCSI. Проверьте эту плату, убедитесь в правильности и надежности ее монтажа. Она не должна быть закорочена ни на одну другую плату или кабель. Попробуйте последовательно по одному отключать устройства SCSI. Если при этом нормальная производительность будет восстановлена, вы будете знать, что за неисправность ответственно последнее демонтированное устройство (в ходе подобной локализации неисправностей вам, возможно, придется блокировать драйверы и переустанавливать оконечные нагрузки). Если неисправность сохранится, удалите, а после этого заново установите все устройства SCSI или воспользуйтесь новой платой адаптера SCSI.

Симптом 12.14. Выводится код ошибки 112xxxx

Это диагностический код ошибки, который указывает на наличие неисправности, связанной с 16-битовой платой адаптера SCSI. Проверьте эту плату и убедитесь в правильности и надежности ее монтажа. Она не должна быть закорочена ни на одну другую плату или кабель. Попробуйте последовательно по одному отключать устройства SCSI. Если при этом нормальная производительность будет восстановлена, вы будете знать, что за неисправность ответственно последнее демонтированное устройство (возможно, в ходе подобной локализации неисправностей вам придется блокировать драйверы и переустанавливать оконечные нагрузки). Попробуйте установить новую плату хост-адаптера SCSI.

Симптом 12.15. Выводится код ошибки 113xxxx

Это диагностический код ошибки, который указывает на наличие проблемы, связанной с конфигурацией адаптера SCSI системы (материнской платы). Если на материнской плате установлена постоянная память SCSI BIOS, убедитесь в том, что она отвечает современным требованиям, правильно и надежно установлена. Если неисправность сохранится, попробуйте заменить микросхему контроллера SCSI материнской платы (если это возможно) или установите новую материнскую плату. Возможно, поврежденный контроллер SCSI материнской платы удастся локализовать, отключив его, а затем установив плату хост-адаптера SCSI.

Симптом 12.16. Выводится код ошибки 210xxxx

Этот код ошибки указывает на повреждение жесткого диска SCSI. Проверьте надежность подключения к диску силового и сигнального кабелей. Убедитесь в правильности расстановки оконечных нагрузок на кабеле SCSI. Попытайтесь заново выполнить разделение и форматирование жесткого диска SCSI. Если неисправность сохраняется, установите новый жесткий диск SCSI.

Симптом 12.17. Устройство SCSI отказывается взаимодействовать с адаптером SCSI, хотя по отдельности они работают нормально

Часто это проявление несовместимости между устройством и хост-адаптером. Несмотря на то, что SCSI-2 и более поздние стандарты поддерживают совместимость между устройствами и контроллерами, до сих пор встречаются ситуации, когда они просто не могут работать совместно. Проверьте, нет ли в документации к устройству упоминаний о его совместимости с вашим контроллером (возможно, с конкретной платой контроллера). Если вы встретите предупреждения об их несовместимости, попробуйте воспользоваться альтернативными настройками перемычек или DIP-переключателей, которые позволяют сгладить несовместимость устройств. Позвоните в службу технической поддержки компании-производителя данного устройства и попытайтесь узнать о недавно обнаруженных дефектах и последних исправлениях (к числу которых могут относиться, например, обновленная система SCSI BIOS, драйвер устройства SCSI или драйвер хост-адаптера). Если неисправность сохранится, установите аналогичное устройство от другого производителя (например, накопитель на магнитной ленте Connor вместо подобного ему накопителя Mountain).

Симптом 12.18. Появляется сообщение об ошибке, в соответствии с которым "контроллер SCSI отсутствует"

Можно смело предположить, что контроллер либо неисправен, либо плохо установлен. Проверьте параметры установки хост-адаптера (включая настройки IRQ, DMA и I/O) и убедитесь в правильности установки драйверов устройств. Если система опять не обнаружит контроллер, попробуйте установить его в другой системе. Если он не будет работать и в новой среде, значит, он вышел из строя и нуждается в замене. Но если в новой системе контроллер работает, значит, исходная система, вероятно, не поддерживает все функции, связанные с вызовом по прерыванию 15h, которые необходимы для настройки адаптеров SCSI (в качестве примера можно привести хост-адаптер SCSI AMI). Попробуйте обновить ПЗУ системы BIOS, в особенности если текущая версия BIOS устарела. А также обновите систему BIOS SCSI или драйвера хост-адаптера.

Симптом 12.19. Хост-адаптер SCSI на шине PCI не обнаруживается, а заголовок SCSI BIOS не отображается

Часто это происходит при установке новых хост-адаптеров SCSI на шине PCI. Центральная система должна соответствовать версии PCI REV.2.1 (или более поздней), а материнская плата должна поддерживать мосты PCI-PCI (PPB, PCI-to-PCI Bridges) и управление передачей данных по шине. Как правило, эта неисправность (или ограничение) связана с наборами микросхем старых материнских плат PCI, поэтому вполне возможно, что та же плата адаптера SCSI PCI будет безо всяких проблем работать в более новой системе. Если система не поддерживает PPB, вы не сможете пользоваться адаптером SCSI PCI. В таком случае есть два варианта: перейти на адаптер SCSI на шине ISA или установить новую материнскую плату с современным набором микросхем.

Симптом 12.20. Во время загрузки появляется сообщение об "ошибке конфигурации хост-адаптера"

Практически во всех случаях эта проблема связана с конфигурацией слота PCI для хост-адаптера SCSI. Попробуйте назначить слоту PCI адаптера SCSI прерывание (IRQ) или повысить его приоритет (обычно это делается с помощью CMOS Setup). Или переместите плату PCI в слот PCI с более высоким приоритетом. Убедитесь в том, что прерывание, выделенное слоту PCI адаптера SCSI, не конфликтует с другими устройствами в системе.

Симптом 12.21. Появляется сообщение об ошибке типа "функции SCSI не используются"

Даже если адаптер и устройства SCSI надлежащим образом установлены и настроены, остается несколько возможных причин возникновения такой ошибки. Во-первых, если ни одного физического жесткого диска SCSI в системе не установлено, убедитесь в том, что соответствующие таким дискам драйверы в ней также отсутствуют. Кроме того, если система BIOS хост-адаптера SCSI включена, драйверов жестких дисков (например, находящихся в CONFIG.SYS) в системе также быть не должно. В этом случае необходимости в драйверах жестких дисков нет, но, если отключить SCSI BIOS, их можно оставить. Наконец, такая ошибка может появиться, если определенный жесткий диск был отформатирован на другом контроллере SCSI, не поддерживающем ASPI, или использует специализированный формат. К примеру, контроллеры Western Digital работают только с жесткими дисками Western Digital. В таком случае установите более универсальный контроллер.

Симптом 12.22. Появляется сообщение об ошибке типа "загрузочная запись не обнаружена"

Как правило, эта простая неисправность может быть связана с несколькими возможными причинами. Во-первых, вполне возможно, что данный диск не был разделен (FDISK) и отформатирован как загрузочный диск (FORMAT). В таком случае следует провести повторное разделение и форматирование жесткого диска. При разделении и форматировании диска с помощью сторонней утилиты (например, TFORMAT), на ее вопрос о том, следует ли сделать данный диск загрузочным, нужно выбрать "Y". Наконец, возможно, диск форматировался на контроллере другого производителя. Если дело именно в этом, то нужно просто провести повторное разделение и форматирование диска на текущем контроллере.

Симптом 12.23. Появляется сообщение об ошибке типа "устройство не отвечает — загрузка драйвера прервана"

В большинстве случаев эта неисправность обуславливается довольно простыми факторами — например, устройство SCSI может быть не включено, или его проводка может быть некорректной. Убедитесь в том, что устройства SCSI подключены и должным образом подсоединены к кабелям. В других случаях, когда устройство SCSI включено, не проходит команда INQUIRY — это значит, что устройство SCSI неисправно или не поддерживается данным хост-адаптером. Возможно, устройство нуждается в изменении принятых по умолчанию положений перемычек (к примеру, диск должен раскручиваться и проходить самостоятельную подготовку). Кроме того, нельзя исключать возможность совместного использования одного идентификатора SCSI двумя устройствами. Проверьте все устройства SCSI и убедитесь, что они располагают уникальными идентификаторами SCSI. Возможно, загруженный драйвер не соответствует типу установленного устройства. Чтобы проверить, правильный ли драйвер загружен для конкретного типа диска, нужно открыть CONFIG.SYS (к примеру, TSCSI.SYS соответствует жесткому диску, а не приводу CD-ROM).

Симптом 12.24. Появляется сообщение об ошибке типа "неизвестное устройство SCSI" или "ожидание устройства SCSI"

Жесткий диск SCSI не загрузился в качестве первичного диска — проверьте, назначен ли для первого жесткого диска идентификатор SCSI ID0. Убедитесь в том, что данный диск разделен и отформатирован как первичный диск. В случае необходимости загрузитесь с гибкого диска — при этом в CONFIG.SYS не должно быть загружено никаких драйверов, кроме менеджера ASPI; затем отформатируйте диск. Помимо прочего, вполне вероятно, что оконечные нагрузки на кабеле SCSI проставлены некорректно (или HARD DISK не обеспечивает TERMPWR для хост-адаптера). Проверьте терминирование кабеля и сигнал TERMPWR.

Симптом 12.25. Появляется сообщение об ошибке типа "ошибка CMD XX"

Как правило, это случается в ходе процесса FORMAT. "XX" является кодом производителя (чтобы выяснить, что означает это сообщение, вам придется связаться с этим производителем). Наиболее часто встречающаяся в процессе разделения диска неисправность заключается в том, что он отформатирован не на низком уровне. Если дело в этом, запустите утилиту низкоуровневого форматирования, сопровождающую диск SCSI или встроенную в хост-адаптер SCSI, а затем попытайтесь выполнить разделение еще раз. Если смысл ошибки заключается в чем-то другом, вероятно, вам придется предпринять другие действия. Какие именно — зависит от характера ошибки.

Симптом 12.26. После появления заголовка системы BIOS адаптера SCSI выводится сообщение типа "идет поиск целевого устройства SCSI с LUN 0"

Система приостанавливается примерно на 30 с, а затем заявляет, что "система BIOS не установлена, устройство INT 13h не найдено". После этого система загружается в нормальном режиме. В большинстве случаев это связано с тем, что BIOS пытается обнаружить жесткий диск с идентификатором SCSI ID0 или ID1, который отсутствует. Если к хост-адаптеру не подключено ни одного жесткого диска SCSI, SCSI BIOS рекомендуется отключить.

Симптом 12.27. При появлении заголовка SCSI BIOS система зависает

Как правило, эта проблема обусловлена неисправностью оконечной нагрузки. Убедитесь в том, что устройства SCSI, расположенные в конце цепочки SCSI (либо внешне, либо внутренне), терминированы. Проверьте уникальность всех идентификаторов устройств и удостоверьтесь в отсутствии системных конфликтов на уровне использования ресурсов (таких как адреса BIOS и I/O, а также прерывания). Возможно, вам придется отключить функцию затенения памяти (Shadow RAM) в CMOS Setup.

Симптом 12.28. Во время запуска системы выводится заголовок SCSI BIOS, но после этого появляется сообщение об "ошибке диагностики хост-адаптера"

Либо адрес порта платы хост-адаптера конфликтует с адресом порта другой платы, либо адрес порта платы был изменен на 140h при включенной системе BIOS. Некоторые хост-адаптеры SCSI способны пользоваться BIOS при применении адреса порта 140h, так что вам следует поискать конфликты I/O. Возможно, хост-адаптер SCSI придется перенастроить.

Симптом 12.29. В среде Windows 9x/ME программа Adaptec EasySCSI вызывает ошибку из-за недействительности страницы

При переустановке версии 4.0x программы Adaptec EZ-SCSI есть возможность появления следующего сообщения об ошибке:

```
ADPST32 caused an invalid page fault in module MSCUISTF.dll at 015f:007dlbf7
```

После вывода этого сообщения об ошибке компьютер может зависнуть. Эта неисправность возникает, если в вашей системе установлен адаптер SCSI Adaptec 3940UW Dual Channel, причем ранее в SCSI Explorer (входящем в состав EZ-SCSI 4.0x) были установлены значения Enable (включить) настроек **Write** и **Read Cache** (кэш записи и кэш чтения). К аналогичному эффекту может привести деинсталляция программы EZ-SCSI, а затем, еще перед попыткой ее переустановки, перезагрузка компьютера. Следует восстановить установки по умолчанию микропрограммного обеспечения SCSI BIOS.

1. Перезагрузите компьютер. При появлении заголовка SCSI BIOS нажмите сочетание клавиш <Ctrl>+<A> — так вы откроете программу SCSI BIOS Setup.
2. В программе SCSI BIOS Setup нажмите клавишу <F6> (или другую подходящую клавишу), чтобы восстановить заводские настройки по умолчанию. В случае применения двухканального хост-адаптера SCSI эту операцию необходимо выполнить по отношению к обоим каналам.
3. Выключите компьютер, а затем вновь включите его.
4. Деинсталлируйте, а затем переустановите программное обеспечение EZ-SCSI.

Симптом 12.30. Вы сталкиваетесь с трудностями при работе с контроллером SCSI BusLogic на шине PCI

Когда в вашей системе установлен контроллер SCSI PCI BusLogic, Windows **Device Manager** выводит рядом с соответствующей ему записью пиктограмму восклица-

тельного знака в желтом круге, или же производительность системы оказывается ниже, чем вы ожидали. Такие трудности могут происходить в случае, если плата BusLogic не настроена в качестве "истинного" устройства PCI.

Чтобы настроить плату BusLogic как "настоящее" устройство PCI, снимите перемычки, находящиеся на ее нижнем правом крае. После удаления этих перемычек плату можно пронумеровать. Если оставить перемычки на плате, она воспринимается как "действующее" устройство и не нумеруется системой PnP. Кроме того, при этом диапазон I/O приравнивается не к высокому адресу PCI, а к стандартному адресу (например, 330h, 334h, 130h или 134h). Как правило, если номер версии, обозначенный в верхнем правом углу платы BusLogic, — -01-4.23K или версия более поздняя, плата может работать в истинном режиме PCI, и перемычки следует удалить. Если же версия старше -01-4.23K, их стоит оставить на плате.

Симптом 12.31. Вы сталкиваетесь с трудностями при работе с контроллером SCSI Adaptec и приводом CD-RW

При запуске Windows 98 компьютер может зависать, а при попытке обращения к дискам скорость его работы может понижаться. Эта проблема возникает при использовании хост-адаптера SCSI Adaptec AHA-2940U2W совместно с приводом CD-RW SCSI. Файл драйвера AIC78U2.MPD, сопровождающий адаптер SCSI Adaptec AHA-2940U2W, не является полностью совместимым с операционной системой Windows 98. Чтобы устранить эту неисправность, загрузите с Web-сайта Adaptec файл 7800W9X.EXE. Этот самораспаковывающийся файл содержит обновленные драйверы для адаптера SCSI Adaptec AHA-2940U2W.

Симптом 12.32. После обновления Windows 98 не может обнаружить привод CD-ROM SCSI

Когда программа Windows 98 Setup перезагружает компьютер в первый раз, она может потерпеть неудачу при обращении к приводу CD-ROM SCSI, в результате чего могут появляться сообщения об ошибках при обнаружении файлов (имена файлов варьируют в зависимости от аппаратного обеспечения системы). После завершения работы Setup при попытке запуска Windows 98 компьютер может зависнуть, а на черном экране будет отображаться только мерцающий курсор. В большинстве случаев это связано с тем, что файл HIDE120.COM (связанный с диском LS120) загружается из файла AUTOEXEC.BAT. Откройте файл AUTOEXEC.BAT и отключите (закомментируйте) командную строку HIDE120 — например, так:

```
REM d:\lsl120\hide120.com
```

Дополнительные ресурсы

Adaptec: **www.adaptec.com**.

Ancot: **www.ancot.com**.

Maxtor: **www.maxtor.com**.

Qlogic: **www.qlogic.com**.

Quantum: **www.quantum.com/src/**.

Руководство по SCSI: **www.delec.com/guide/scsi/**.

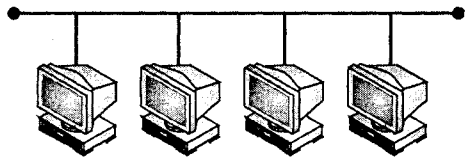
Ассоциация производителей устройств SCSI: **www.scsita.org**.

Seagate: **www.seagate.com**.

Статьи Symbios: **www.lsilogic.com**.

Спецификации Symbios: **www.symbios.com/x3t10**.

Western Digital: **www.wdc.com**.



ГЛАВА 13

Повторители, концентраторы и коммутаторы

За редким исключением, в процессе развития сети (локальной или глобальной) в нее добавляют новые сетевые устройства. Некоторые аппаратные средства, такие как повторители, концентраторы и коммутаторы, просто организуют взаимодействие между рабочими станциями в рамках одной локальной сети, в то время как другое сетевое оборудование — мосты, маршрутизаторы и шлюзы — предоставляют возможность обмена информацией между двумя географически удаленными областями или различными сетевыми топологиями. Различия между этими устройствами, относящиеся к их уровню интеллекта и сложности, в первую очередь обуславливаются теми уровнями модели OSI (Open System Interconnection — взаимодействие открытых систем), на которых они работают. В этой главе мы рассмотрим первую из приведенных групп сетевого аппаратного обеспечения, т. к. все эти устройства, как правило, используются в локальной сети.

Повторители

Подобно любому электрическому сигналу, качество передачи данных по мере прохождения значительных расстояний имеет тенденцию к ухудшению. Такое ухудшение сигнала называется *затуханием*; зачастую оно ограничивает диаметр сети передачи данных всего несколькими сотнями метров. К примеру, в сетях с тонким коаксиальным кабелем или 10Base2 длина шины (т. е. общая длина всех сегментов кабеля) не может превышать 185 м. Для преодоления этого ограничения на размеры сети и увеличения протяженности сети на тонком коаксиальном кабеле до 925 м были созданы повторители для передачи данных в сетях Ethernet.

Примечание

Повторители применяются не только в проводных электрических сетях, но и в оптических и беспроводных сетях.

Повторитель представляет собой довольно простое устройство, работающее на физическом уровне (или на уровне 1 модели OSI) и выполняющее функцию усиления сигнала, проходящего в той среде, к которой он подключен. Сигнал входит на повторитель с одного из его портов, затем усиливается и заново синхронизируется, и, наконец, в усиленной форме ретранслируется через все остальные порты. В стан-

дартных повторителях есть лишь два порта, но на более современных или многопортовых повторителях портов может быть больше.

В сети на тонком коаксиальном кабеле можно создавать до пяти сегментов с помощью четырех повторителей; в то же время лишь в трех из этих сегментов могут располагаться рабочие станции. Оставшиеся два сегмента используются исключительно для увеличения протяженности сети и не могут содержать рабочие станции. Это ограничение, связанное с повторителями в сетях Ethernet, получило название правила 5-4-3; своему существованию оно обязано задержкам прохождения сигнала при избыточной протяженности сети. По мере разрастания сети время прохождения сигнала из одного конца в другой увеличивается; из-за этого рабочая станция X в одной части сети может испытывать трудности при определении того, когда рабочая станция Y, находящаяся в другой части сети, осуществляет передачу — в результате возрастает частота коллизий. При возникновении сбоев в работе сети на тонком коаксиальном кабеле с использованием повторителей имеет смысл переместить сервер или серверы, находящиеся в данной сети, ближе к середине ее сегментов. Делать это не обязательно, но благодаря этому любой рабочей станции для установления соединения с сервером нужно пройти не более двух повторителей; в результате небольшие сбои в сети, вероятно, исчезнут.

Так как повторители работают на физическом уровне, они могут устранять помехи и усиливать принимаемый сигнал, но исправление поврежденного сигнала является для них невыполнимой задачей. Кроме того, повторители не имеют возможности определять направление передачи данных; таким образом, такие устройства не способны обеспечить разделение сетей на множество коллизионных доменов. Впрочем, в непритязательности повторителей заключаются и определенные преимущества — так, повторитель можно установить в сети, практически (или совсем) не меняя ее конфигурацию. Нужны лишь источник питания и кабель — и, в соответствии со своим названием, повторитель будет повторять все, что получит.

Концентраторы и модули доступа к среде

В процессе перевода сетей с коаксиальной инфраструктуры на витую пару понадобилось новое устройство, которое должно было принимать сигнал от одной рабочей станции в сети на основе витой пары и передавать его другой. Проблема заключалась в том, что в большинстве сетей на основе витой пары в пределах отдельно взятого сегмента сети находится более двух рабочих станций; одной витой пары между двумя устройствами было недостаточно. С этой целью для витой пары был спроектирован многопортовый повторитель. В сетях Ethernet это устройство называют *концентратором*, а в кольцевых сетях с маркерным доступом — модулем MAU (Media Access Unit — модуль доступа к среде).

Концентраторы

Как и повторитель, концентратор работает на физическом уровне (или уровне 1 модели OSI), выполняя простую функцию ожидания передач на один из своих портов RJ-45. При получении передачи или сигнала концентратор выполняет его усиление, повторную синхронизацию, а затем — повторную передачу на любой другой порт, к которому подключена рабочая станция или сервер. Так как концентратор является

устройством усиления, максимальное расстояние от него до каждой подключенной к нему рабочей станции не может превышать 100 м.

Классы концентраторов

Принимая решение о том, какой концентратор лучше установить, важно понимать, что не все они одинаковы. Существует три различных группы концентраторов, причем функциональность каждой последующей группы выше, чем предыдущей. Этими тремя основными классами концентраторов являются пассивные, активные и интеллектуальные — как правило, для каждого из них существуют разновидности с 4—48 портами RJ-45 Ethernet.

- *Пассивные.* Такие концентраторы просто принимают сигнал с одного порта и безо всякого усиления передают его на все другие узлы. В результате, концентратор этого типа можно применять только в очень небольших средах, где расстояние между рабочими станциями сравнительно невелико, а общая длина всего кабеля не превышает 100 м. Такие концентраторы являются самыми дешевыми.
- *Активные.* Для обеспечения передачи сигнала в более крупных сетях активный концентратор осуществляет усиление и повторную синхронизацию сигнала перед его ретрансляцией. Такое расширение функциональных возможностей концентратора позволяет размещать рабочие станции и серверы на расстоянии 100 м от концентратора, к которому они подключены, без риска ухудшения сигнала вследствие его затухания. Дополнительное преимущество сетей с активными концентраторами состоит в том, что в них происходит меньше коллизий, т. к. хостам не приходится выполнять повторную передачу пакетов с незначительными ошибками передачи из-за синхронизации.
- *Интеллектуальные.* Интеллектуальные концентраторы — это активные концентраторы с некоторыми дополнительными функциями, связанными с удаленным управлением. Концентраторы этого класса являются наиболее дорогими, но при этом они способны создавать статистические отчеты об использовании сети и о возникающих в ней ошибках и, кроме того, они располагают средствами удаленного подключения или отключения каждого из своих портов, что может пригодиться при выполнении задач, связанных с безопасностью или устранением неисправностей. Статистическая информация, как правило, предоставляется несколькими способами, в том числе через последовательную консоль, через командную строку (Telnet) или графический пользовательский Web-интерфейс, а также средствами протокола сетевого управления SNMP (Simple Network Management Protocol — простой протокол сетевого управления).

Следует отметить, что все концентраторы существуют в различных вариантах, поддерживаемых стандартом Ethernet, включая 10BaseT и 100BaseT. Некоторые концентраторы поддерживают один из этих стандартов, а современные концентраторы поддерживают оба стандарта с помощью метода, называемого *автосогласованием*. Важно убедиться в том, что сетевые адаптеры рабочих станций и подключенные к ним концентраторы поддерживают один и тот же стандарт Ethernet — к примеру, сетевой адаптер на основе 10BaseT, подключенный к концентратору 100BaseT или Fast Ethernet, работать не будет. Кроме того, обращаясь к Fast Ethernet, спецификация IEEE 802.3u подразделяет концентраторы и повторители на две группы: класс I и класс II. Различие между этими двумя классами заключается в количестве концен-

траторов или повторителей, которые могут располагаться между двумя хостами в сети. К примеру, в классе I предусматривается наличие между любыми двумя хостами только одного концентратора или повторителя, а в классе II этих устройств в аналогичных условиях может быть два. Это ограничение обусловлено той задержкой, которую каждое из вышеупомянутых устройств вносит в работу сети Fast Ethernet.

Установка концентраторов

За исключением интеллектуальных концентраторов, большинство концентраторов можно устанавливать в сети без предварительного конфигурирования. Так как они схожи с повторителями (в том, что концентраторы лишь повторяют сигнал и не связаны с отправителем или предполагаемым получателем любого отдельно взятого пакета), зачастую нет необходимости и в последующей настройке. Однако при установке интеллектуальных концентраторов может потребоваться изменение конфигурации для обеспечения доступа к их функциям управления.

Что касается технический стороны вопроса, для подключения концентратора нужно лишь подсоединить его к источнику питания, а кабели RJ-45 проложить между рабочей станцией и концентратором. Показателем успешного соединения между концентратором и рабочей станцией является непрерывный сигнал светодиода связи на концентраторе и на сетевом адаптере рабочей станции. Кроме того, если концентратор поддерживает несколько скоростных режимов (10 и 100 Мбит/с), он указывает и на скорость порта.

Если концентратор не располагает достаточным количеством портов, то для расширения сети можно организовать цепочку из двух или нескольких концентраторов 10BaseT. При отсутствии иных указаний производителя возможна группировка только двух концентраторов 100BaseT класса II, причем расстояние между ними не должно превышать 5 м. Такое соединение концентраторов обычно осуществляется с помощью специального гнезда RJ-45, предназначенного для соединения концентраторов. В некоторых концентраторах этот порт для соединения концентраторов имеет те же возможности, что и обычный порт рабочей станции, на что указывает настраиваемый пользователем переключатель, с помощью которого определяется режим работы такого порта. Кроме того, в современных или наращиваемых концентраторах может присутствовать BNC-порт для коаксиального кабеля 10Base2, предназначенный для группообразования (trunking), и даже специальный порт и кабель для высокоэффективного взаимодействия между концентраторами.

Примечание

Если на концентраторе нет порта для соединения концентраторов, то можно использовать обычный порт рабочей станции при условии, что два концентратора соединены витой парой.

Об управлении концентратором

Так как концентраторы довольно просты, управление ими ограничено. Впрочем, управляемые концентраторы способны составлять отчеты об использовании сети и статистике ошибок, а также могут осуществлять администрирование отдельных портов. Если не считать их функций, связанных с генерацией отчетов, почти все кон-

центраторы имеют очень скромный набор средств сообщения о своей активности — диагностические светодиоды на передней панели, которые бывают следующих типов.

- *Питание.* Обычно подключение концентратора к источнику питания и его нормальное функционирование обозначается постоянным зеленым светодиодом.
- *Активность.* Вид этого индикатора не является универсальным для всех концентраторов; на некоторых из них присутствует единственный индикатор активности, обозначающий наличие передачи в сети. Другие концентраторы имеют индикаторы активности процессов передачи на отдельных портах.
- *Связь.* На большинстве концентраторов есть светодиоды связи для каждого порта; они обозначают успешное установление соединения между концентратором и подключенным устройством. На некоторых концентраторах светодиоды связи одновременно являются индикаторами активности.
- *10/100.* На концентраторах, поддерживающих несколько скоростных режимов, могут присутствовать светодиоды, указывающие, на какой скорости работает порт.
- *Коллизии.* Единственным светодиодом на концентраторе, который привлекает внимание при работе устройства, является индикатор коллизий. Несистематическое мигание этого индикатора является нормальным, но заметное сокращение интервалов мигания может обозначать наличие неисправности в сети, связанной с передачей данных или производительностью.

Что касается интеллектуальных концентраторов с функциями управления, обращение к их статистическим данным и информации об ошибках чаще всего производится одним из нескольких нижеперечисленных способов.

- *Прямой консольный доступ.* Для этого необходимо, чтобы терминал или компьютер был подключен к последовательному коннектору концентратора — обычно это подключение производится с помощью последовательного нуль-модемного соединения, но для некоторых устройств может потребоваться кабель с прямым соединением пар или специализированный последовательный кабель. Как только соединение установлено, любая программа эмуляции терминала типа HyperTerm сможет обеспечить доступ к системе управления на базе командной строки. Несмотря на то, что настройки консоли различаются в зависимости от производителя, обычно 8 бит, отсутствие контроля по четности и один стоповый бит (или 8–N–1) на скорости порта 9600 бит/с с эмуляцией терминала VT100 способны обеспечить бесперебойное соединение с устройством. Команды также зависят от конкретного производителя, так что вам следует обязательно ознакомиться с руководством по эксплуатации коммутатора; для начала можно сразу после входа на терминал ввести с клавиатуры команду ?.
- *Удаленный доступ в командной строке средствами Telnet.* Чтобы обратиться к сетевой командной строке с помощью Telnet, сначала необходимо назначить концентратору, по меньшей мере, один IP-адрес и маску подсети. Обычно это можно сделать, предварительно подключившись к концентратору с помощью последовательного пульта оператора. После настройки IP-адреса обращение к нему с помощью Telnet должно обеспечить доступ к командной строке концентратора.
- *Доступ по графическому пользовательскому Web-интерфейсу.* Если вы предпочитаете графический интерфейс управления, на некоторых концентраторах с этой

целью встроены небольшие Web-серверы. Для обращения к этому интерфейсу управления устройство должно иметь хотя бы один IP-адрес и маску подсети, которые обычно назначаются посредством прямого консольного доступа. После проведения конфигурации доступ к графическому интерфейсу, как правило, осуществляется с помощью стандартного Web-браузера типа Microsoft Internet Explorer или Netscape Navigator. Некоторые устройства работают только со специальным графическим приложением, которое поставляется в комплекте с устройством на дискете или компакт-диске.

Примечание

При настройке управления концентратором и любым другим устройством необходимо изменить и сохранить принимаемый по умолчанию пароль администратора. Кроме того, при настройке устройства для организации сетевого доступа к нему имеет смысл назначать IP-адрес и маску подсети, но не адрес шлюза. Этим вы лишите сторонних пользователей прямого доступа к управляющим функциям концентратора. Убедитесь в том, что назначаемый IP-адрес доступен и не используется другим устройством.

Поиск и устранение неисправностей концентратора

Важным преимуществом звездообразной топологии, формируемой посредством концентраторов и витой пары, конечно же, является простота поиска и устранения неисправностей. В отличие от линейной шины, которая применяется в сетях 10Base2 и 10Base5, в звездообразной топологии неисправный сегмент кабеля влияет на работу лишь одного узла, тогда как в тех же условиях в шине сети 10Base2 из строя выйдут все узлы. Кроме того, учитывая, что в звездообразной топологии все узлы связываются через одну точку (концентратор), тестирование следует начинать именно с нее.

При локализации неисправностей соединения в первую очередь нужно проверить диагностические индикаторы концентратора и сетевого адаптера рабочей станции. Отсутствие сигнала светодиода связи на любом из этих устройств, вероятнее всего, указывает на наличие неисправности физического соединения. При этом нужно убедиться в том, что данный порт работает как на хосте, так и на концентраторе (если он является управляемым). Если связь присутствует на одном конце соединения, но отсутствует на другом, то либо соединение физически неисправно, либо одно из этих устройств не настроено на нужную скорость (10 или 100 Мбит/с). Несоответствие скоростей передачи приводит к невозможности установления связи, а некоторые устройства более ранних версий в этой ситуации могут вести себя непредсказуемым образом. Если подозрение падает на физическую неисправность, следует проверить, нет ли в кабеле физических повреждений и плохо закрепленных коннекторов. Если это возможно, воспользуйтесь тестером или сканером кабеля. Не забывайте о необходимости соблюдать ограничение расстояния (100 м) для витой пары.

Однако полностью доверять светодиоду связи при диагностике кабеля не стоит. Вполне возможно, что из строя вышли порт концентратора или сетевой адаптер. Чтобы проверить это предположение, просто перенаправьте данный сегмент кабеля на новый (заведомо исправный) порт концентратора и проверьте сигнал светодиода связи. Если отсутствие связи сохраняется, попытайтесь поменять местами сегменты кабеля на двух концах канала и проверьте сегмент кабеля с помощью тестера. Нако-

нец, если связь установить не удается, замените сетевой адаптер рабочей станции. Более подробно методы поиска неисправностей витой пары изложены в *гл. 8.*

Примечание

Всегда обращайте внимание на то, поддерживают ли сетевой адаптер и концентратор один и тот же скоростной режим Ethernet, т. к. сетевой адаптер 10BaseT не будет работать с концентратором, поддерживающим только 100BaseT или FastEthernet, и наоборот.

В процессе поиска неисправностей могут помочь и другие статусные и диагностические индикаторы концентратора. К примеру, если пользователи сообщают о низкой производительности сети, следует проверить состояние индикатора коллизий. Этот светодиод сигнализирует о периодических коллизиях, но большое количество коллизий не является нормальным и бывает вызвано либо сбоями в обмене информацией на одном или нескольких узлах, либо слишком высоким уровнем использования сети; в этом случае сеть следует сегментировать, чтобы создать дополнительные коллизионные домены.

Если неисправность заключается в ошибке передачи, конкретный узел или узлы, которые являются причиной ее появления, можно выявить визуально, сопоставляя синхронность сигнализирования светодиода коллизий и светодиода активности отдельных портов. Кроме того, выявить неисправный узел можно, последовательно отключая порты один за другим до тех пор, пока светодиод коллизий не возобновит нормальную частоту сигнализирования. Наконец, при использовании управляемого концентратора его командная строка или графический интерфейс, вероятно, смогут вывести статистику каждого отдельного порта — например, данные о коллизиях или ошибках передачи. Когда неисправный узел найден, необходимо проверить с помощью кабельного сканера, нет ли в соответствующем сегменте кабеля физических неисправностей и электромагнитных помех.

Иногда управляемый концентратор может внешне как бы исчезать из сети — т. е. прекращать отвечать на управляющие Telnet- или Web-запросы. Обычно это происходит, когда устройство поддерживает протоколы BOOTP или DHCP. При первой загрузке устройства с поддержкой BOOTP оно отсылает широковещательный запрос всем серверам BOOTP или DHCP на получение IP-адреса и сопутствующей информации. Если в локальной сети такой сервер существует, концентратору выделяется новый IP-адрес, который, скорее всего, не соответствует тому адресу, который был ему выделен при первоначальной конфигурации. Чтобы исключить такую ситуацию, подключитесь к порту консоли концентратора и убедитесь в том, что конфигурация BOOTP отключена. Обязательно присвойте устройству новый IP-адрес, и прежде чем выходить с пульта оператора, сохраните конфигурацию.

Модули доступа к среде

Подобно концентраторам в среде Ethernet, модули MAU выполняют функцию физического соединения рабочих станций в условиях звездообразной топологии с витой парой. В данном случае в качестве сетевой среды используется не Ethernet, а *маркерное кольцо* — технология, разработанная компанией IBM. Обе технологии физически формируют звездообразную топологию, но на этом их сходство заканчивается — модули доступа к среде маркерного кольца фактически организуют внутрен-

нюю шину, таким образом, формируя логическое кольцо из всех рабочих станций сети. Кроме того, в отличие от Ethernet, в кольцевой сети с маркерным доступом не возникает коллизий при передаче, т. к. устройство управления передачей, называемое *маркером*, позволяет всем рабочим станциям осуществлять передачи в рамках заданного временного промежутка. Впрочем, у сетей на основе маркерного кольца есть и недостаток — до последнего времени их скорость была ограничена 4 или 16 Мбит/с. В настоящее время доступны более скоростные варианты сетей с маркерным доступом, но в рамках локальных сетей технологии Fast Ethernet и Gigabit Ethernet стали более популярными.

Сеть на основе маркерного кольца работает посредством объединения всех рабочих станций в кольцо, организуемое с помощью модуля доступа к среде. Затем каждый хост ждет, пока к нему перейдет маркер, который позволит осуществить передачу. Располагая маркером, рабочая станция может осуществлять передачу, не опасаясь возникновения коллизий. После завершения передачи одной рабочей станцией маркер передается следующей рабочей станции в рамках кольца. Если у рабочей станции нет маркера, она не может осуществлять передачу.

Само кольцо формируется с помощью электрических реле в составе модуля MAU, которые соединяют передающую пару одного порта с принимающей парой другого порта. Это продолжается от порта к порту — до тех пор, пока все порты не сформируют одно кольцо. Если какой-то отдельный порт не используется, он переводится в режим обхода; таким образом, кольцо переходит к следующему активному порту.

При подключении к сети новой рабочей станции порт модуля MAU начинает работать в режиме обхода, обеспечивая кольцевую проверку новой рабочей станции. Чтобы стать участником кольца, эта рабочая станция подает на передающую пару низкое напряжение — тем самым она обозначает свою готовность войти в кольцо. Модуль MAU выявляет этот уровень напряжения, и принимающая пара данной рабочей станции подключается к передающей паре другого порта, а ее передающая пара подсоединяется к принимающей паре другого порта. Этот метод привлечения рабочей станции в кольцо называется *включением*. Если в какой-то момент напряжение порта понизится, MAU посчитает этот узел неисправным и удалит его из кольца, поместив этот порт в режим обхода.

Классы модулей MAU

Подобно своим Ethernet-собратьям, модули MAU подразделяются на три основных класса: пассивные, активные и управляемые. Пассивный MAU — это просто коробка с электрическими реле, предназначенными для организации внутреннего кольца из подключенных рабочих станций. Такие модули не обеспечивают усиления сигнала; следовательно, расстояния в сетях маркерного кольца на основе пассивных MAU до некоторой степени ограничены.

С другой стороны, активные MAU содержат усилители сигнала и способны увеличивать размеры сети с маркерным доступом до масштабов, значительно превосходящих сети на основе пассивных MAU. Как правило, количество портов в таких устройствах варьирует в диапазоне от 8 до 16 и более, но управляемых или интеллектуальных разновидностей активных MAU не существует.

Вместо управляемых MAU в сетях на основе маркерного кольца могут устанавливаться блоки CAU (Controlled Access Units — управляемые блоки доступа). Помимо

наличия функций управления, CAU отличаются от MAU тем, что они не позволяют рабочим станциям осуществлять с ними прямое соединение. Чтобы подключить к CAU рабочую станцию, необходим дополнительный модуль под названием абонентской приставки.

Поиск и устранение неисправностей MAU

Многие алгоритмы устранения неисправностей, имеющиеся в сетях на основе маркерного кольца, встроены в сетевые адаптеры рабочих станций; таким образом, многие ошибки, происходящие в сетях такого типа, остаются незамеченными. Впрочем, как и в любых других проводных инфраструктурах, из строя могут выходить и кабели, и аппаратное обеспечение. Поэтому поиск физических неисправностей в условиях маркерного кольца мало отличается от поиска неисправностей в среде Ethernet. На самом деле, светодиоды многих модулей доступа к среде очень напоминают индикаторы на коммутаторах Ethernet.

В сетях на основе маркерного доступа сбои соединения, как правило, обуславливаются неисправностями кабеля или аппаратной части. Поэтому в случае возникновения любых трудностей при подключении рабочей станции к кольцу в первую очередь следует тестировать кабель. Если эта проверка пройдет успешно, попробуйте подключить кабель к другому порту MAU. Наконец, причиной неисправности может быть сетевой адаптер рабочей станции; чтобы проверить эту возможность, на его место следует поставить другой адаптер. К счастью, некоторые адаптеры для маркерного кольца поставляются в комплекте с диагностическим программным обеспечением, которое сможет выявить ошибку или вывести данные о сбое связи.

Коммутаторы

Термин "коллизионные домены" встречался нам не один раз, но до настоящего момента мы не обсуждали устройства, способные обеспечить создание этих автономных виртуальных или физических сегментов сети. Коммутаторы могут формировать отдельные коллизионные домены как физически, так и виртуально, т. к. они работают на канальном уровне (или уровне 2 модели OSI), а в случае многоканальности — на более высоких уровнях.

При работе на уровне 2 устройство способно принимать интеллектуальные решения о том, как обрабатывать определенный пакет данных на основе MAC-адреса источника и назначения. MAC-адрес (Media Access Control address — адрес управления доступом к среде) представляет собой уникальный идентификатор, жестко закодированный в любом сетевом устройстве на этапе его производства.

В этой главе будут рассматриваться коммутаторы Ethernet — они передают кадры между портами. Существуют и другие сетевые коммутаторы — к примеру, коммутаторы ретрансляции кадров и коммутаторы ATM (Asynchronous Transfer Mode — асинхронный режим передачи) используются чаще всего владельцами сетей связи. Кроме того, коммутаторы ATM применяются на крупных сетях предприятий — они заметно отличаются от коммутаторов Ethernet тем, что осуществляют коммутацию в ячейках, а не в кадрах. Коммутаторы ATM намного дороже коммутаторов Ethernet, но они обладают значительными преимуществами в производительности, что оправдывает их высокую цену.

На первый взгляд коммутатор Ethernet напоминает концентратор, но коммутатор не просто принимает сигнал с одного порта и передает его на все остальные. Коммутатор, принимая пакет с одного из своих портов, сначала считывает информацию, которая содержится в заголовке этого пакета. С помощью этой информации коммутатор устанавливает, откуда пакет пришел и куда он должен направиться. В результате коммутатор передает кадр через порт назначения (и только через него), который соединяет его с предполагаемым получателем. Этот процесс осуществляется во всех случаях за исключением ситуации, когда рабочая станция отсылает широковещательный пакет, предназначенный для всех рабочих станций, который коммутатор передает через все свои порты.

Направление кадров только через порт, который соединяет коммутатор с предполагаемым получателем, имеет множество преимуществ, важнейшим из которых является производительность, т. к. множество узлов сети могут осуществлять передачи одновременно, не опасаясь возникновения коллизий. Другим преимуществом коммутируемой архитектуры является повышенная безопасность. В коллективных средах или средах, формируемых вокруг концентратора, весь трафик передается на все порты; следовательно, любая рабочая станция может перехватить сетевые сообщения другой рабочей станции. Напротив, в коммутируемых средах, поскольку трафик направляется только предполагаемому получателю, другие рабочие станции не могут перехватить сообщения, которые для них не предназначены. Есть и множество других преимуществ, таких как работа в дуплексном режиме, организация VLAN и расширенные возможности управления сетью.

Примечание

Коммутаторы предназначены не только для того, чтобы соединять рабочие станции; они также выполняют функцию объединения нескольких концентраторов. Этим они помогают сэкономить на пропускной способности и повысить производительность, т. к. коммутатор отсылает пакеты только тому подключенному к нему концентратору, который отвечает за принимающую пакет рабочую станцию.

Дуплексная передача

Значительное повышение производительности при использовании коммутаторов достигается благодаря тому, что рабочая станция получает возможность выполнять операции отправки и приема одновременно, т. е. она работает в дуплексном режиме. Этот режим отличается от обычного полудуплексного режима, при котором рабочая станция может передавать данные только тогда, когда она их не получает, и наоборот.

Чтобы понять, как это происходит, в первую очередь обратите внимание на то, что порт коммутатора и хост, к которому он подключен, образуют выделенную линию Ethernet (в противоположность совместному использованию канала несколькими портами коммутатора). Это позволяет коммутатору и хосту отправлять и получать сигналы одновременно, т. к. ограничений на передачу и пропускную способность в данном случае не существует. Коммутатор передает полученные пакеты конкретному получателю незамедлительно — ожидание возможно лишь в том случае, если через порт назначения уже передаются данные. В такой ситуации коммутатор помещает кадр в буфер и передает его после освобождения нужного порта. В результате коллизии и повторные передачи, обуславливаемые ими, исключаются.

Значительное повышение производительности достигается не только устранением коллизий и повторных передач — сетевым адаптерам серверов и рабочих станций больше не нужно выделять отдельное время на операции передачи и получения. В результате производительность увеличивается почти на 100%, т. е. вдвое по сравнению с коллективным полудуплексным режимом.

Технологии коммутации

Для коммутации данных между сетевыми портами коммутаторы Ethernet применяют два основных метода. У каждого из этих методов есть свои преимущества, и выбор в пользу одного из них в значительной степени обуславливается той средой, в которой он будет применяться. Вне зависимости от того, какой метод выбран, все коммутаторы пользуются базой данных переадресации портов (Port Forwarding Database, FDB), которая обеспечивает коммутацию с проводной скоростью, т. к. устройство хранит таблицу хостов и соответствующих им портов для последующего обращения к ней.

При использовании первого метода коммутации данные прибывают на коммутатор, а затем незамедлительно им обрабатываются — зачастую это происходит еще до завершения передачи. Коммутатор устанавливает, на какой порт следует перенаправить полученные кадры, и запускает процесс передачи. Этот быстродействующий метод называется *транзитной коммутацией*, т. к. коммутатор, не внося данные в буфер, начинает перенаправлять их в тот момент, когда узнает пункт их назначения из первого полученного кадра. Так как перенаправление данных происходит до завершения передачи всех кадров источником, коммутатор не может произвести никакие действия по исправлению ошибок. Несмотря на то, что во многих ситуациях этот метод оказывается наиболее быстрым из двух возможных, скорость его действия может быть значительно снижена, если данные повреждены, или если коммутатор загружает кадры в буфер при занятости принимающего порта.

Второй метод коммутации называется *коммутацией с буферизацией пакетов* — в соответствии с его названием данные, прибывающие на коммутатор, хранятся в буферах до получения всех кадров. При хранении данных коммутатор анализирует их в поисках информации о пункте их назначения. После занесения в буфер всего кадра коммутатор производит поиск ошибок в кадре с помощью кода CRC (Cyclic Redundancy Code — избыточный циклический код), а затем перенаправляет его на порт коммутатора получателя. Если порт получателя занят, коммутатор продолжает хранить кадр до тех пор, пока не получает возможность успешно перенаправить его. Зачастую этот метод является более предпочтительным, т. к. во многих случаях коммутатору приходится временно буферизовать исходящие данные, что обуславливается занятостью получателя; кроме того, коммутаторы с буферизацией пакетов производят дополнительный контроль ошибок, в то время как в транзитных коммутаторах он не выполняется. Среднее время ожидания или задержка передачи при транзитной коммутации составляет 45,6 микросекунд. Это менее чем на 6 микросекунд быстрее, чем соответствующий показатель коммутатора с буферизацией пакетов, который создает задержку продолжительностью в 51,5 микросекунд. Минимальное различие между двумя методами коммутации обуславливает выбор коммутации с буферизацией пакетов.

Применение коммутатора

При подключении коммутатора рекомендуется в первую очередь спланировать, где в сети он будет размещен. К примеру, несмотря на то, что коммутатор можно подключить напрямую к любой рабочей станции, в случае, если высокая производительность сети не столь важна, этот вариант слишком дорог. Вместо этого имеет смысл подключить к коммутатору серверы, а рабочим станциям выделить небольшие концентраторы, которые впоследствии будут объединены коммутатором.

Как показано на рис. 13.1, эта схема обеспечивает возможность прямого высокоскоростного дуплексного соединения с серверами и предусматривает наличие нескольких наборов групп рабочих станций или рабочих групп, каждая из которых находится в собственном коллизионном домене, что позволяет обращаться к серверам с минимальной возможностью возникновения коллизий. В результате производительность сети и стоимость ее ввода в эксплуатацию поддерживаются на оптимальном уровне.

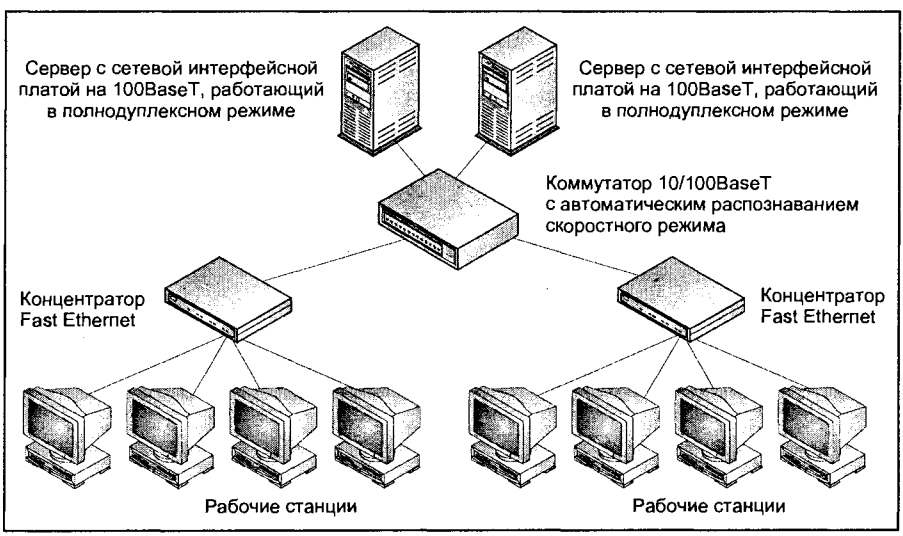


Рис. 13.1. На этом примере коммутаторы объединяют две рабочие группы, подключенные к концентраторам, и при этом обеспечивают серверам дуплексную передачу по стандарту 100BaseT

В подобной схеме коммутатор, как и концентратор, не требует проведения специальной конфигурации. Сразу после установки в сеть коммутатор автоматически определяет расположение портов всех рабочих станций и серверов и сохраняет эту информацию в своей базе данных переадресации портов. При желании обеспечить управление коммутатором ему необходимо назначить IP-адрес и маску подсети, что можно сделать через его последовательный консольный порт.

Связанные группы

Простые коммутаторы 2-го уровня, как правило, предусматривают средства сегментации (деления) портов коммутатора на логические группы меньшего размера, на-

зываемые *связанными (мостовыми) группами*. Эта функция полезна в том случае, если необходимо физически разделить две или несколько сетей. К примеру, предположим, что финансовый отдел занимает коммутационные порты 1—7, отдел маркетинга — порты 8—15, а отдел сбыта — порты 16—23.

Предположим, что каждый отдел располагает собственным сервером; тогда коммутатор можно настроить на три отдельные логические группы, что гарантирует обращение каждого отдела только к тем ресурсам, которые для него предназначены. Кроме того, сегментация коммутатора сокращает широковещание в рамках данного сетевого сегмента, т. к. в логических группах участвует меньше рабочих станций, а это, как и сокращение частоты коллизий, повышает производительность сети.

VLAN

С развитием коммутаторов усовершенствовались и наборы их функций. Одним из наиболее важных дополнений к функциям коммутаторов Ethernet является способность к созданию сетей VLAN, причем не только в рамках одного коммутатора, но и между несколькими коммутаторами. Сети VLAN обладают множеством преимуществ, включая возможности перенаправления трафика друг другу (когда эту функцию поддерживает коммутатор 3-го уровня) и физического перемещения пользователей между коммутаторами при сохранении их участия в определенной VLAN.

Вновь обращаясь к обсуждению логических групп, на рис. 13.2 мы видим три отдела, каждый из которых имеет собственный набор доступных сетевых ресурсов. Проблема заключается в том, что, если пользователю в финансовом отделе требуется получить доступ к серверу в отделе сбыта, он физически не может этого сделать. Если поместить каждую из этих групп в отдельные VLAN, появляется множество вариантов выхода из этого затруднительного положения. Имейте в виду, что коммутатор 3-го уровня может выполнять маршрутизацию между VLAN, но не между логическими группами. Большинство коммутаторов не поддерживают одновременно VLAN и контактные группы.

Один из вариантов — выбрать маршрутизацию между VLAN. Эта функция обеспечивается внешним маршрутизатором, который будет рассматриваться в *гл. 14*, или коммутатором 3-го уровня, который может работать как на канальном, так и на сетевом уровне. В нашем случае пользователь VLAN отдела сбыта (называемой VLAN 20) сможет обратиться к серверу в VLAN отдела финансов (VLAN 10) с помощью его IP-адреса. Коммутатор опознает этот IP-адрес как принадлежащий к VLAN 10 и при необходимости выполнит виртуальную маршрутизацию между двумя VLAN. Эта схема предусматривает создание более мелких широковещательных доменов, которые способны повысить производительность сети в целом.

Еще один пример преимущества VLAN показан на рис. 13.3, где мы видим четыре коммутатора, подключенных с помощью оптоволоконных каналов. Есть три различных VLAN, каждая из которых относится ко всем коммутаторам. С помощью протокола 802.1Q каждый коммутатор в группе способен тегировать каждый кадр с помощью идентификатора VLAN. В результате, когда данные перемещаются от коммутатора к коммутатору, принимающий коммутатор определяет идентификатор VLAN в теге 802.1Q кадра и на основе этой информации перенаправляет кадр в соответствующую VLAN и/или широковещательную группу. Эта функция дает возможность пользователям данной VLAN переходить от коммутатора к коммутатору, не теряя

соединения с VLAN своей рабочей группы, что, в свою очередь, разрешает некоторые довольно значительные трудности управления, связанные с перемещениями, добавлениями и изменениями.

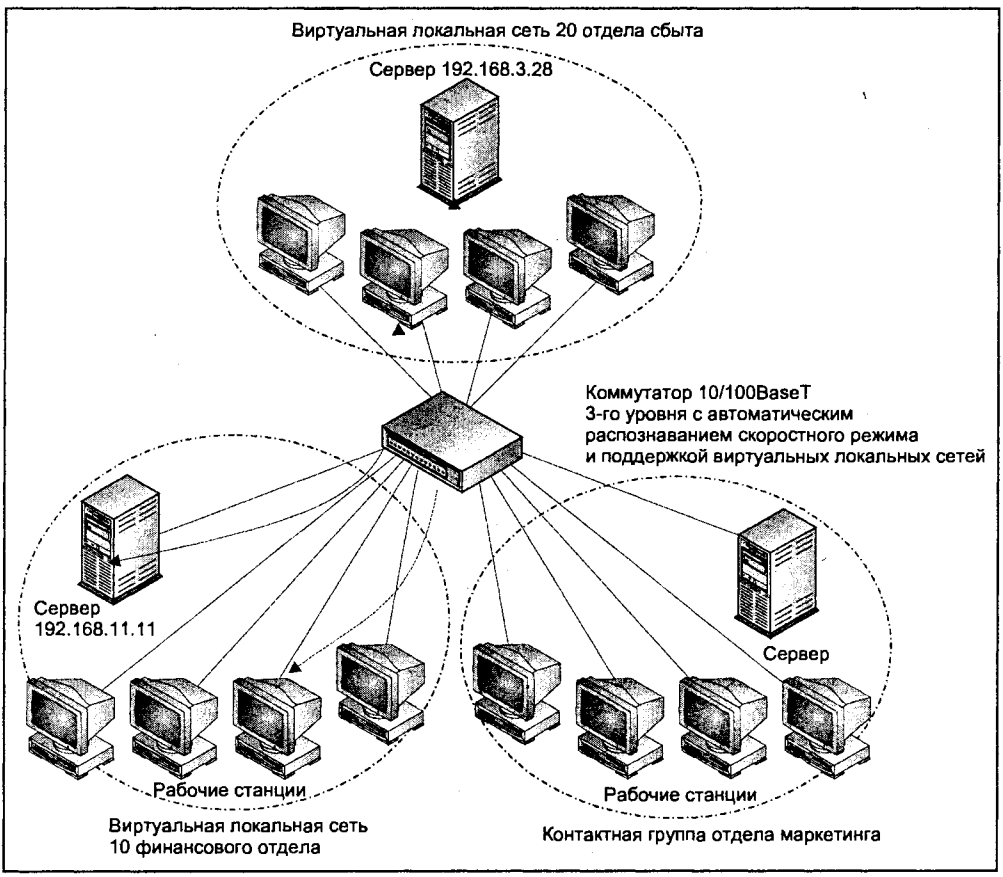


Рис. 13.2. Различие между логическими группами и VLAN в отношении разделения широковещательных доменов

Тег 802.1Q представляет собой 4 байта данных, которые добавляются к традиционному формату кадров Ethernet 802.3 и содержат не только информацию о принадлежности к VLAN, но и данные о приоритете кадра 802.1p. Тег состоит из четырех отдельных полей, представленных в табл. 13.1.

Процесс конфигурации VLAN в коммутаторе не представляет большой сложности — как правило, он выполняется несколькими командами. К примеру, чтобы на коммутаторе Extreme Summit Ethernet добавить порты 1, 2, 3, 5, 7, 23 и 24 к VLAN 10, можно воспользоваться следующей командой:

```
Switch-1: configure vlan 10 add ports 1,2,3,5,7,23,24
```

Примечание

Если коммутатор работает и на 3-м уровне, для подключения интерфейса виртуальной маршрутизации настроенной VLAN может потребоваться собственный IP-адрес. Без этого адреса маршрутизация между VLAN, вероятно, будет невозможна.

Таблица 13.1. *Поля тега 802.1Q*

Метка	Имя поля	Размер	Описание
TCI	Управляющие данные тега (Tag Control Info)	2 байта	Значение 8100 указывает на применение в кадре тегов 802.1Q и 802.1p
P	Приоритет (Priority)	3 бита	Обозначает уровень приоритета 802.1p от 0 до 7
C	Канонический индикатор (Canonical indicator)	1 бит	Указывает, имеют ли MAC-адреса канонический формат. Как правило, в кадрах стандарта Ethernet это значение устанавливается на 0
VLAN	Идентификатор VLAN (VLAN ID)	12 бит	Указывает, к какой VLAN принадлежит данный кадр

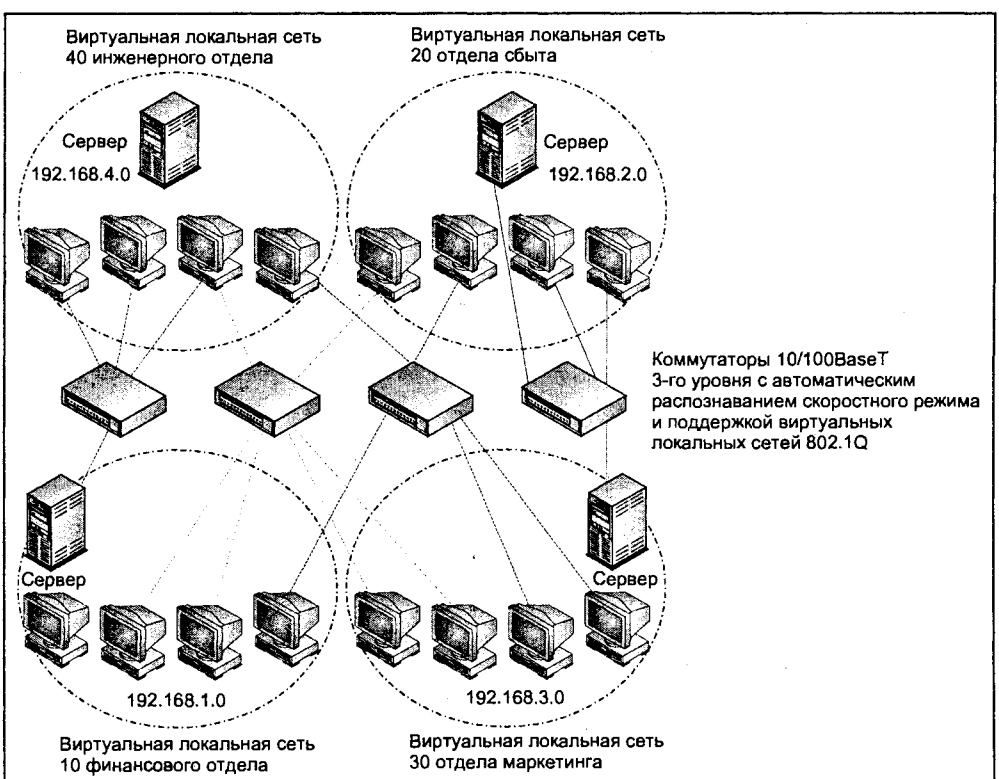


Рис. 13.3. Тегирование VLAN 802.1Q между коммутаторами

Зеркальное копирование в портах

Зачастую при возникновении масштабных сбоев в работе сети единственным средством их обнаружения является изучение данных, отсылаемых по сети, с помощью сетевого анализатора пакетов. В этом нет ничего сложного, если сеть состоит исключительно из концентраторов Ethernet — в этом случае через любой порт проходят все отсылаемые данные. Но предположим, что один из коммутаторов установлен специально для того, чтобы оградить порты от получения данных, которые для них не предназначены — как тогда исследовать все данные, проходящие по сети?

К счастью, многие производители коммутаторов учли эту ситуацию и разработали решение под названием *зеркального копирования (mirroring)*. С помощью этой функции коммутатор можно настроить так, чтобы он буквально копировал трафик, исходящий из одного порта или из группы портов коммутатора на любой другой порт, настроенный под эту функцию. Кроме того, для проведения тестирования коммутаторы можно настроить на зеркальное копирование одной или нескольких VLAN на один порт.

К примеру, чтобы активировать на коммутаторе Extreme Summit Ethernet зеркальное копирование из VLAN 1 в порт 48, следует ввести следующие команды:

```
Switch-1: enable mirroring to port 48
Switch-1: configure mirroring add VLAN 1
```

Примечание

Зачастую при активации зеркального копирования на одном из портов он может стать непригодным для выполнения нормальных сетевых передач.

Об управлении коммутатором

Так как коммутаторы — это довольно сложные устройства, которые могут считывать и анализировать передаваемые данные, они способны предоставить значительные объемы статистических данных, а также информацию о степени использования каждого порта и счетчики ошибок. Помимо этого, коммутатор должен показывать MAC-адреса и, если речь идет о коммутаторе 3-го уровня, IP-адреса рабочих станций, соответствующих каждому порту. Эта информация может оказаться полезной при попытке обнаружить причину ухудшения пропускной способности сети или рабочие станции, порождающие ошибки в сети.

Подобно простейшим концентраторам, почти все коммутаторы имеют набор диагностических светодиодов на передней панели, причем даже расположение этих индикаторов на коммутаторах и интеллектуальных концентраторах зачастую совпадает.

Интерфейсы управления коммутатором могут предоставить данные об уровне использования сети, частоте появления ошибок и другой статистической информации в режиме реального времени. Доступ к этой информации осуществляется с помощью командной строки или графического пользовательского Web-интерфейса, но, возможно, полезным для вас окажется способ обращения к ней посредством протокола SNMP. Он предполагает накопление и мониторинг группы сетевых устройств через центральное приложение. Некоторые устройства поддерживают возможность изменения конфигурации с помощью программного управления SNMP,

которое при наличии нескольких коммутаторов может снизить временные затраты на администрирование.

Примечание

При использовании SNMP в целях безопасности рекомендуется менять принимаемые по умолчанию частные и общие строки SNMP. Если такая возможность поддерживается конкретным устройством, следует определить доступ хостов на основе их IP-адресов либо через SNMP, либо через Telnet.

Поиск и устранение неисправностей коммутатора

Так как коммутаторы во многом похожи на концентраторы, процедуры поиска и устранения неисправностей в этих устройствах почти одинаковы, за исключением нескольких дополнений. Инструкции по основным принципам поиска неисправностей в сетях звездообразной топологии представлены в предыдущем разделе.

Общие принципы поиска и устранения неисправностей

Помимо знания общих принципов поиска и устранения неисправностей концентраторов, необходимо помнить, что коммутаторы (как и интеллектуальные концентраторы) обладают таким дополнительным преимуществом, как возможность мониторинга передач и ошибок для каждого отдельного порта. Поэтому в целях обнаружения рабочих станций, испытывающих трудности при передаче или получении данных, необходимо обращаться к интерфейсу управления коммутатором. Большое количество ошибок может свидетельствовать о физической неисправности кабеля, но в подобном случае нужно обязательно определить показатель приращения, т. к. текущее число ошибок могло накопиться за большой период времени.

При любой возможности следует пользоваться базой данных переадресации портов. К примеру, если каким-то образом один и тот же IP-адрес был присвоен двум компьютерам, Windows, как правило, сообщает об этом и приводит MAC-адрес рабочей станции-источника сбоя. Имея эту информацию, можно обратиться в базу данных переадресации портов, найти указанный MAC-адрес, определить местонахождение или, по крайней мере, номер физического порта соответствующей рабочей станции, и временно отключить ее — таким образом, одна из двух конфликтующих рабочих станций сможет нормально работать.

Примечание

При перемещении рабочей станции на новый порт необходимо очистить содержимое базы данных переадресации портов (а на коммутаторах 3-го уровня, и ARP-кэш), т. к. некоторые коммутаторы не могут определить устаревание записи для порта. Помните, что на время восстановления базы данных переадресации портов производительность коммутатора может понизиться. Вместо этого вы можете воспользоваться подготовительным и менее радикальным методом — после включения хоста и его подсоединения к сети попробуйте послать с него Ping-запрос на его же шлюз.

Другим распространенным источником сбоев в работе коммутаторов является недостаточная совместимость по функции автосогласования. При одновременном использовании сетевого адаптера и коммутатора с функцией автосогласования нужно

настроить оба устройства вручную — установить на них желаемые скорость порта и дуплексный режим. Очень часто автоматически устанавливается нежелательный полудуплексный режим, а в некоторых случаях режим в обоих устройствах периодически меняется, что обуславливает появление сбоев соединения между ними. Чаще всего это происходит тогда, когда одно из устройств настроено на дуплексный режим, а другое — на автосогласование. Настройки скорости и дуплексного режима сетевого адаптера можно задать на рабочей станции через свойства или настройки драйвера адаптера. Для получения информации о настройке этих параметров обратитесь к руководству по эксплуатации концентратора и сетевого адаптера.

Примечание

Проверьте, поддерживают ли коммутатор и сетевой адаптер один и тот же скоростной режим Ethernet — сетевой адаптер 10BaseT не будет работать с коммутатором, который поддерживает только стандарт 100BaseT или Fast Ethernet, и наоборот.

Поиск и устранение неисправностей в VLAN

Дополнительные преимущества VLAN являются источником потенциальных трудностей. Довольно часто, когда пользователи приписаны к одной VLAN, а на самом деле находятся в другой, они теряют доступ к сети. С помощью MAC-адреса соответствующей рабочей станции эта проблема устраняется довольно просто. Найдите в базе данных переадресации портов запись этого MAC-адреса и соответствующий ему номер порта. Затем определите, в какой VLAN находится этот порт — если она определена неверно, внесите изменения в настройки так, чтобы он находился в соответствующей VLAN.

Другой распространенный источник сбоев в работе VLAN — это внутренняя маршрутизация. Простым средством локализации сбоя передачи является утилита командной строки `traceroute` (`tracert`) — она есть в большинстве операционных систем и сетевых устройств. Чтобы воспользоваться этой утилитой, просто введите в командной строке `traceroute` (или эквивалентную команду), а вслед за ней укажите IP-адрес пункта назначения маршрутизации. В результате утилита Traceroute выводит список всех устройств (транзитов, хопов), через которые должно пройти сообщение, чтобы попасть в пункт назначения. В случае неудачи хопы обозначаются "***", что указывает на превышение лимита времени. Как правило, сбой при маршрутизации расположен между хопом, который блокируется по времени, и предшествующим хопом.

Если предшествующим хопом является коммутатор (предполагается, что это коммутатор 3-го уровня), проверьте его маршрут по умолчанию и любой другой его маршрут. Для осуществления маршрутизации между VLAN каждому коммутатору нужно присвоить IP-адрес в каждой подсети, где будут проходить маршруты.

Симптомы неисправностей

Многие сбои в соединении можно свести к физическим повреждениям кабеля, но зачастую причиной неисправности становится элементарная ошибка, допущенная во время конфигурации. Ниже представлены некоторые типичные ошибки конфигурации хостов и сетей.

Симптом 13.1. Соединение между коммутируемыми сегментами отсутствует

Если предположить, что оба сегмента качественно соединены с коммутатором, то причина неисправности, скорее всего, заключается в конфигурации этого коммутатора. Так как коммутаторы можно разделить на логические группы или VLAN, вполне возможно, что два данных сегмента находятся в разных логических группах или VLAN. Чтобы убедиться в этом, проверьте настройки коммутатора для каждого из подключенных портов и внесите в них необходимые изменения.

Симптом 13.2. Наличие постоянных широковещательных штормов

Одним из побочных эффектов применения Microsoft Windows является заметное усиление широковещательных штормов, которое происходит по мере добавления в сегмент локальной сети все большего количества узлов. Одним из методов уменьшения широковещания является создание нескольких мелких широковещательных доменов. Эта задача довольно легко выполнима с помощью коммутационных VLAN; в результате широковещательных штормов становится меньше, а все узлы сохраняют возможность взаимодействия.

Симптом 13.3. Низкая пропускная способность коммутатора

Часто причиной низкой пропускной способности является несоответствие настроек дуплексного режима. К примеру, если порт коммутатора сервера жестко закодирован на дуплексную передачу со скоростью 100 Мбит/с, а сам сервер настроен на автосогласование, то сервер будет осуществлять согласование в полудуплексном режиме со скоростью 100 Мбит/с. Чтобы устранить эту неисправность, нужно по возможности вручную настроить соответствующие порты коммутатора на скорость 100 Мбит/с и дуплексный режим. Кроме того, с помощью интерфейса управления сервером определите, на каких портах количество ошибок является избыточным. Эта информация поможет выявить другие порты, являющиеся источниками сбоев связи и работы в дуплексном режиме.

Симптом 13.4. Невозможно установить связь с коммутатором с помощью Telnet, SNMP или Web-браузера

Чтобы сделать коммутатор доступным в сети, ему необходимо присвоить IP-адрес и маску подсети. Если такая настройка уже выполнена, проверьте, находится ли рабочая станция, с которой осуществляется доступ к коммутатору, в одной локальной подсети с коммутатором. Если это не так, коммутатору должен быть присвоен адрес шлюза, с помощью которого он получит возможность обмена информацией вне локальной подсети. Наконец, вполне возможно, что настройки коммутатора позволяют ему устанавливать сетевые управляющие соединения только с определенными IP-адресами. Чтобы проверить, входит ли в их число ваш IP-адрес, подключитесь к коммутатору через консольный порт.

Если ни одно из перечисленных решений не привело к желаемому результату, можно предположить, что сервер BOOTP или DHCP произвел динамическую реконфигурацию коммутатора. Чтобы проверить, так ли это, подключитесь к порту коммутатора, и проверьте его IP-адрес. Если адрес изменился, убедитесь в том, что протоколы BOOTP и DHCP отключены, а если это не так, отключите их. Прежде чем выходить из интерфейса конфигурации, не забывайте сохранять внесенные в настройки изменения.

Симптом 13.5. Невозможно получить доступ к коммутатору через его последовательный порт

Для подключения к портам пульта оператора некоторых сетевых устройств требуются нуль-модемные соединения, для других нужны простые последовательные кабели, для третьих — специализированные кабели. Чтобы проверить выбор кабеля и настройки эмуляции терминала, обратитесь к руководству по эксплуатации коммутатора. Если неисправность не удалось устранить, замените кабель, т. к. он может быть неисправен. Редко из строя может выйти консольный порт. В устройстве может быть временно заблокирован интерфейс управления, его нормальную работу можно восстановить после перезагрузки.

Дополнительные ресурсы

Cisco — технология Ethernet:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm.

Cisco — поиск и устранение неисправностей в сетях Ethernet:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1904.htm.

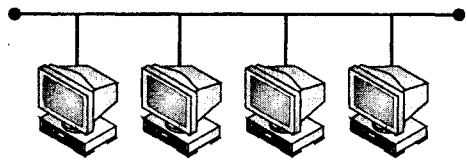
Web-сайт Чарльза Сперджена, посвященный технологии Ethenet:
http://www.ethermanage.com/ethernet/ethernet.html.

Технологический справочник Extreme Networks:
http://www.extremenetworks.com/technology/technology.asp.

Институт инженеров по электротехнике и электронике (IEEE):
http://grouper.ieee.org/groups/802/3/.

Lantronix Networking: **http://www.lantronix.com/learning/index.html**.

TechFest: **http://www.techfest.com/networking/**.



ГЛАВА 14

Мосты, маршрутизаторы и шлюзы

По мере перехода от локальных сетей к региональным и глобальным, сетевые устройства должны становиться все более и более интеллектуальными по способам передачи данных между сетями. Такой рост интеллекта необходим, поскольку, если в целях расширения сети или передачи данных между двумя или несколькими географически удаленными сетями понадобятся дополнительные коллизионные домены, простой ретрансляции всего трафика из одной сети в другую (как это делают концентратор или повторитель) окажется недостаточно — трудности начнут появляться уже в силу ограничений по пропускной способности.

Чтобы обеспечить эффективную передачу данных во все более сложных средах, сетевым устройствам приходится работать не только на физическом уровне, но и на канальном, сетевом, а иногда — и на более высоких уровнях. Устройства, функционирующие на этих уровнях — мосты, маршрутизаторы и шлюзы — чаще всего используются для решения задач, связанных с глобальными сетями. В этой главе мы рассмотрим такие устройства с точки зрения их функционирования, а также поиска и устранения неисправностей.

Мосты

Первым устройством этой группы является мост, который работает на уровне 2 модели OSI (канальном уровне). Мосты — это устройства с двумя или несколькими портами, которые используются как интеллектуальные повторители и предназначены для соединения двух или нескольких сетей в рамках одного общего широковещательного домена. В зависимости от типа моста, подобное соединение может происходить либо в локальной, либо в глобальной сети.

Различие между повторителем и мостом заключается в том, что мост — это более интеллектуальное устройство передачи данных между двумя сетями. Повторитель просто выполняет ретрансляцию данных, получаемых им с одного порта, на все остальные порты, а мост считывает получаемые кадры данных и на основе адреса назначения определяет, нужно ли перенаправлять кадр на один или несколько своих портов. Решение о перенаправлении принимается после сравнения пункта назначения кадра с таблицей подключенных хостов для всех портов моста. Если мост установит соответствие между пунктом назначения кадра и одним из своих портов, он

примет данный кадр и выполнит его передачу лишь через тот порт, на котором доступен получатель. Это позволяет сэкономить на пропускной способности и оптимизировать общий уровень использования всех подключенных сетей. Передача кадра на все порты происходит лишь в том случае, если пункт назначения этого кадра не найден в таблице.

Примечание

Может сложиться впечатление, что функции моста похожи на функции коммутатора, но не забывайте, что коммутатор 2-го уровня — это всего лишь многопортовый мост.

Использование в сети функций мостов дает ей множество преимуществ и возможностей. Вот некоторые из них:

- локализация распространенных сетевых неисправностей между двумя сегментами сети;
- общая фильтрация кадров между двумя сегментами локальной сети для оптимизации трафика и использования сети (т. е. разделение локальных сетей на более мелкие коллизионные домены);
- существенное расширение локальной сети в пределах здания путем организации мостов между двумя или несколькими сегментами с помощью медного или оптоволоконного кабеля при выделении отдельных коллизионных доменов и поддержке широковещательного домена;
- соединение двух географически удаленных сетей посредством арендуемой выделенной линии передачи данных при поддержке широковещательного домена.

Режимы работы моста

При ближайшем рассмотрении моста можно выделить четыре основных процесса, определяющих функционирование этого устройства. Первый процесс называется *прослушиванием* (listening) и является простой процедурой наблюдения за сетевым трафиком. В ходе этого процесса мост наблюдает за сетевым трафиком на всех интерфейсах и создает таблицу распределения хостов по портам. Чтобы обеспечить актуальность информации в этой таблице, мост удаляет ее записи по истечении определенного срока хранения, в течение которого хост не осуществляет обмен данными. Эти данные, содержащиеся в таблице, используются вторым процессом, который называется *продвижением* (данных) (Forwarding).

Когда мост получает кадр, он сравнивает его адрес назначения с таблицей адресов, которая создается в процессе наблюдения за трафиком. Если обнаруживается совпадение пункта назначения, мост перенаправляет данный пакет на соответствующий интерфейс. Если же соответствие не найдено, мост активизирует третий процесс, который называется *лавинной адресацией* (Flooding), при котором мост отправляет кадр на все порты, а затем ожидает получения ответа из пункта назначения кадра.

Заключительный процесс — *фильтрация* — предусматривает минимизацию ненужного трафика в рамках или между сетевыми сегментами. К примеру, на элементарном уровне мост активизирует фильтрацию для того, чтобы взаимодействие между двумя хостами, принадлежащими одному сегменту сети, не приводило к продвиже-

нию трафика на другие порты моста и их переполнению. В расширенной реализации фильтрация может применяться для ограничения обмена информацией между хостами, находящимися в различных сегментах сети.

Алгоритм покрывающего дерева

Если в сети установлен только один мост, он работает достаточно надежно, но если в одной сети используется два или несколько мостов, то возможно образование петель. Это происходит, когда хост в одной сети передает данные хосту в другой сети, причем эти две сети соединены двумя или несколькими мостами. Когда каждый из этих мостов получает кадры данных, он определяет местоположение получателя и соответственно продвигает данные. К сожалению, т. к. каждый мост получил и продвинул информацию, произошло дублирование всех кадров. Кроме того, при наблюдении за трафиком каждый мост приходит к заключению, что оба хоста находятся в одном и том же сегменте сети, поэтому, активизируя фильтрацию, мосты больше не будут пытаться продвигать кадры между этими двумя хостами, в результате чего возможность обмена информацией между ними исчезнет.

Чтобы избежать такой ситуации, а также воспользоваться избыточностью, которая обеспечивается наличием в заданной среде нескольких мостов, мост поддерживает функцию под названием *покрывающего дерева*, которая отвечает за привязку маршрутов к определенному сегменту сети. Алгоритм STA (Spanning Tree Algorithm — алгоритм связующего дерева) был изначально разработан компанией Digital Equipment Corporation (DEC), а впоследствии был изменен и опубликован в виде спецификации 802.1d комитетом IEEE 802.

В первую очередь алгоритм STA определяет, какой мост в данной среде является корневым (root bridge), выбирая для этого мост с наименьшим идентификатором моста или MAC-адресом. Затем, основываясь на сообщениях о конфигурации всех мостов в сети, алгоритм STA вычисляет лучший путь от любого заданного моста до корневого. После вычисления всех путей мост, путь которого к корневому мосту является оптимальным в заданном сегменте, становится для данного сегмента *назначенным мостом* (designated bridge). Все мосты, которые не входят в оптимальный путь (или обеспечивают дублирующий путь к данной сети), переводятся в режим ожидания или блокировки. В режиме блокировки порт моста не выполняет функции наблюдения, продвижения и лавинной адресации кадров; таким образом, при работающем алгоритме STA петель возникать не должно, т. к. все дублирующие порты мостов в любом заданном сегменте эффективно блокируются.

При использовании алгоритма STA все мосты в рамках сети обмениваются сообщениями об их конфигурации или BPDU (Bridge Protocol Data Unit — протокольный блок данных моста), чтобы определить, кто из них имеет доступ к определенным сегментам сети. Обмен этими сообщениями производится каждые несколько секунд, благодаря этому сетевая топология не теряет своей актуальности. Кроме того, если один из мостов не отправляет BPDU всем остальным, считается, что он больше не является действующим путем ни к одному из сегментов сети и исключается из топологии. Каждый раз, когда обнаруживается изменение топологии сети (т. е. когда какой-то мост перестает отсылать сообщения BPDU), каждый из мостов перезапускает алгоритм STA, который в очередной раз решает, через какие порты следует обращаться к сетям.

Типы мостов

Так как существуют разнообразные варианты практического применения мостов, есть три основных типа этих устройств: локальный мост, удаленный мост и транслирующий мост, каждый из которых обладает определенным набором функций. Поскольку мосты наблюдают за всем сетевым трафиком (неразборчивый режим), они могут повторять данные для всех подключенных сетевых сегментов; хотя очень часто они пользуются фильтрацией на уровне MAC-адресов источника и/или назначения, чтобы выполнять повторную передачу только тех данных, которые нужно отослать в другую сеть. Степень фильтрации зависит от среды, в которой работает мост, и от пропускной способности между двумя и более сетями, соединенными мостом.

Локальный мост

Как правило, такой мост содержит два или несколько портов одного типа (например, только порты Ethernet, только порты маркерного кольца и т. д.) и соединяет два или более однородных сегмента локальной сети в рамках заданного пространства, например, в пределах здания. Первый наиболее распространенный способ применения *локального моста* связан с необходимостью разделения одного крупного сегмента локальной сети на два или несколько более мелких сегментов с целью создания дополнительных коллизионных доменов и повышения производительности сети. При этом между концентраторами, модулями MAU или сегментами сети 10Base2/10Base5 устанавливается один двухпортовый или многопортовый мост, который по необходимости осуществляет передачу трафика между сегментами и тем самым ограничивает коллизии и обеспечивает эффективное взаимодействие всех сегментов сети. По выполняемым функциям мост этого типа больше всего напоминает коммутатор 2-го уровня, поэтому для решения подобных задач можно применять оба этих устройства.

Удаленный мост

При необходимости соединения двух или нескольких географически удаленных локальных сетей оптимальным решением, как правило, является использование *удаленного моста.* Мост такого типа обычно имеет в своем составе порты локальной и глобальной сети, что обеспечивает возможность одновременного подключения к этому мосту локальной сети и глобальной сети (например, T-1). Кроме того, удаленные мосты проводят адресную фильтрацию данных, предназначенных для передачи в удаленные сети; благодаря этому обеспечивается эффективное использование пропускной способности глобальной сети, которая, как правило, намного ниже аналогичного показателя в локальной сети.

Пример использования удаленного моста показан на рис. 14.1. Имеется две локальные сети Ethernet, одна из которых находится в Нью-Йорке, а другая — в Денвере. Чтобы соединить эти две сети в одну группу с помощью моста, необходимы два удаленных моста — по одному на каждую локальную сеть. В каждой локальной сети порт моста локальной сети осуществляет соединение с локальной сетью, а порт моста глобальной сети соединяет с арендуемой линией T-1 между этими двумя мостами. Когда кадр данных, предназначенный к отправке на рабочую станцию в Денвере, создается в сети в Нью-Йорке, мост анализирует этот кадр и сравнивает его с адресной таблицей хостов. Так как адрес назначения этого кадра относится к сети, расположенной в Денвере, мост передает его по каналу T-1 другому удаленному

мосту, который, в свою очередь, перенаправляет кадр в локальную сеть в Денвере. Широковещательные кадры также передаются по каналу Т-1 для их ретрансляции в удаленную сеть, если в сети не установлен маршрутизатор или не изменены настройки мостов.

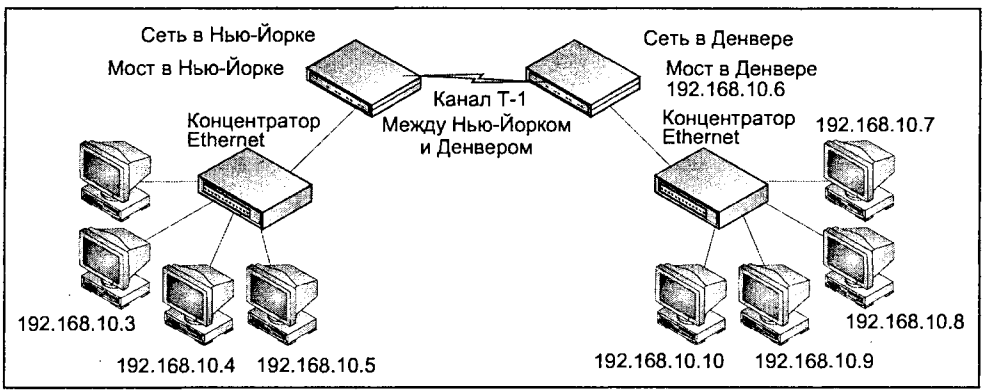


Рис. 14.1. Две географически удаленные сети, соединенные с помощью мостов Ethernet

Транслирующий мост

При необходимости соединения двух разнородных сетей (например, сети Ethernet и маркерного кольца) используется *транслирующий мост*. Эта задача выполняется путем преобразования данных с учетом типа сети назначения; при этом изменениям подвергаются структура кадра и скорость передачи между двумя соединенными сетями. К транслирующим мостам относятся и некоторые типы беспроводных мостов, т. к. они тоже сталкиваются с различиями в структуре кадров и скорости между сетями на основе беспроводных технологий и локальной сетью. Важно заметить, что настройки некоторых маршрутизаторов также предусматривают возможность выполнения ими функций транслирующего моста; следовательно, для решения подобных задач можно применять оба этих устройства.

Об управлении мостами

Как и маршрутизаторы, мосты не требуют больших усилий по настройке или управлению. После установки и включения питания моста он запускает собственный процесс изучения подключенных к нему сетей. При появлении в сети кадра с неизвестным адресом назначения мост пытается обнаружить хост назначения, передавая этот кадр на все порты или сегменты, за исключением того порта, с которого он поступил. Если какой-то хост отвечает на кадр, посланный мостом, в базу данных моста заносится новая запись, и все последующие кадры, отсылаемые на этот адрес, автоматически перенаправляются на соответствующий порт.

Учитывая наличие этого автоматического процесса сетевой идентификации, во многих случаях конфигурации локального моста, принимаемой по умолчанию, вполне достаточно. Однако при необходимости установить ограничения на широковещание или продвижение кадров следует изменить конфигурацию. Настройки фильтрации

такого типа основываются на фильтрации по MAC-адресам (источника или назначения) и имеют возможность статического (не динамического и не прозрачного) продвижения или даже исключения кадров.

Примечание

Обычно для нормальной работы локального моста нет необходимости в его конфигурировании, однако важно изменить информацию о регистрации, принятую для него по умолчанию. Это предотвратит возможные проблемы, связанные с эксплуатацией и безопасностью.

Функции прозрачного моста, присущие удаленным мостам, могут обеспечить успешное создание базы данных перенаправления по портам без какой-либо дополнительной настройки, но очень часто порты, подключенные к глобальным сетям, требуют проведения предварительного конфигурирования. Это обусловливается разнообразием настроек портов, которые могут применяться в глобальных сетях. Кроме того, в случае применения в глобальной сети каналов T-1 некоторые мосты комплектуются последовательными портами V.35 (вместо внутренних устройств обслуживания канала), и при этом для внешних устройств обслуживания канала каждого устройства требуется отдельная конфигурация. Подобную настройку иногда нужно выполнять и на беспроводных мостах, т. к. в целях безопасности их работа с настройками по умолчанию крайне не желательна.

Так как по умолчанию мосты осуществляют ретрансляцию всех широковещательных сообщений (кадров, предназначенных для всех хостов) в каждый подключенный к ним сегмент, важно следить за уровнем широковещания в рамках всей сети. Производительность сети может быть значительно снижена из-за слишком большого количества широковещательных передач или наличия широковещательных штормов. Если это произойдет, нужно либо ввести ограничение на количество широковещательных сообщений, которые обрабатывает порт моста, или заменить мосты маршрутизаторами, т. к. маршрутизаторы формируют независимые широковещательные домены, которые не осуществляют повторение широковещательных сообщений из одного сегмента в другой.

Чтобы упростить управление сегментами, соединенными мостами, большинство мостов поддерживают режим командной строки или графический пользовательский Web-интерфейс, которые способны в реальном времени выводить статистику кадров и широковещательных сообщений, переданных в каждый сегмент. Кроме того, именно с помощью такого интерфейса можно задать фильтрацию, ограничивающую прохождение отдельных кадров между различными сегментами сети. Доступ к этому интерфейсу, как правило, осуществляется непосредственно с консоли (как и на коммутаторе), а также через сеть посредством Telnet/SSH или графического пользовательского Web-интерфейса. Некоторые мосты с расширенными функциональными возможностями, кроме того, обеспечивают поддержку протокола SNMP, с помощью которого выполняется сложный мониторинг и составление отчетов об уровне использования сети и статистике ошибок, которые передаются на центральную консоль управления SNMP.

Если речь идет о современных мостах, всегда рекомендуется пользоваться последними версиями микропрограммного обеспечения. Различные изменения в микропрограммном обеспечении позволяют более эффективно и безопасно выполнять некоторые задачи, а применение последней версии способствует уменьшению по-

тенциальных сбоев. Обязательно сохраняйте копию текущей конфигурации, поскольку в случае выхода моста из строя такая резервная копия существенно снизит временные затраты по установке и настройке нового устройства. Эту операцию можно выполнить с помощью протокола TFTP (Trivial File Transfer Protocol — простейший протокол передачи файлов) или FTP.

Примечание

В более крупных средах разумно устанавливать такие вспомогательные службы, как TFTP-сервер (для загрузки конфигурации), NTP-сервер (для централизованной временной синхронизации) и SYSLOG-сервер (для централизованной регистрации ошибок устройств). Эти службы помогут диагностировать сетевые неисправности и выявить потенциальные сбои.

Поиск и устранение неисправностей мостов

Как правило, неисправности мостов локализуются в пределах одной из подключенных сетей, хотя в некоторых случаях они обуславливаются ошибками, допущенными при конфигурировании. Процесс обнаружения источника неисправности лучше всего начинать с того, чтобы исключить возможность неисправности самого моста (т. к. ее легче диагностировать). Одной из основных ошибок настройки, приводящей к сбоям, является неправильная установка скорости порта или дуплексного режима не только самого моста, но и того устройства, к которому он подключен. Убедитесь в том, что на обоих концах соединения между мостом и сетью заданы правильные настройки порта. Кроме того, обязательно проверьте статистику уровня использования моста и ошибок и выделите все завышенные значения. Нередко высокий уровень использования сети обуславливает переполнение буфера моста, особенно в том случае, если в сети в больших объемах передаются широковещательные сообщения. Если дело обстоит именно так, попробуйте установить причину широковещательного шторма с помощью сетевого анализатора пакетов.

При использовании удаленного моста не забывайте проверять наличие ошибок, а также среднестатистический и максимальный уровень использования подключенного канала глобальной сети. К сожалению, т. к. пропускная способность в большинстве глобальных сетей составляет лишь малую долю пропускной способности локальных сетей, вполне возможно, что существующий канал глобальной сети либо слишком мал для текущего режима его эксплуатации, либо перенасыщен. В этом случае постарайтесь перейти к оптимальным средствам соединения с глобальной сетью, или поищите способы сокращения межсетевого трафика. Общераспространенным способом уменьшения межсетевого трафика является создание локальных серверов для каждого из удаленных офисов; таким образом, при выполнении большинства своих функций локальным рабочим станциям не нужно пользоваться каналом глобальной сети с ограниченной пропускной способностью.

Примечание

Резервное копирование данных удаленного сервера через удаленный мост необходимо планировать на ночное время, когда уровень использования сети минимален. Кроме того, имеет смысл выполнять резервирование изменений (в противоположность полному), чтобы ограничить объем данных, передающихся по каналу глобальной сети с ограниченной пропускной способностью.

Устойчиво низкая пропускная способность сети

Как отмечалось ранее, многие причины снижения производительности чаще всего вызваны одной из подключенных сетей. В этом отношении сложно переоценить значение хорошего сетевого анализатора пакетов. Комплекты программ наподобие SnifferPro являются оптимальными средствами исследования текущего состояния сети с точки зрения соотношения затрат и эффективности, т. к. они позволяют проводить анализ не только сетевого трафика в целом, но и отдельных сообщений между двумя или несколькими устройствами. Кроме того, они превосходно справляются с идентификацией многих обычных и менее распространенных неисправностей, ухудшающих производительность, и зачастую способны выявить аппаратные средства или MAC-адрес неисправного устройства. Помните, что высокая частота коллизий и других ошибок может значительно снизить производительность, а сообщения о таких ошибках, как правило, можно найти на коммутаторе или мосте в сети.

Потеря кадров

Кадры не могут просто исчезнуть из сети, но они могут быть неправильно продвинуты, отфильтрованы или просто выброшены из межсоединения из-за высокого уровня его использования. Если создается впечатление, что кадры не пребывают в пункт назначения, для начала проверьте, не слишком ли высок уровень использования моста, т. к. переполнение его буферов может приводить к отбрасыванию пакетов. Если уровень использования нормальный, убедитесь в наличии всех специальных фильтров и корректной фильтрации мостом всех кадров. Кроме того, проверьте правильность статических записей продвижения, т. к. неправильные записи могут привести к перенаправлению кадра в неверный сегмент сети. Если это не помогает, проверьте, нет ли в текущей динамической или адресной базе данных перенаправления неверных записей. При этом следует обратить особое внимание на адреса источника и назначения и их соответствие нужному порту моста. Если и здесь ошибку выявить не удается, то может помочь очистка базы данных перенаправления.

Образование петель из-за одновременного использования нескольких мостов

В условиях, когда в сети установлено более одного моста, настройка алгоритма STA на обоих мостах является обязательной. Без покрывающего дерева не избежать образования петель, а они, в свою очередь, будут приводить к появлению ошибочного сетевого трафика и потерянных кадров. С помощью алгоритма STA один из мостов блокирует свой избыточный порт до тех пор, пока не появится необходимость в нем. Это сводит к минимуму образование петель.

Трудности при соединении сетей разных типов

Сбои в работе сети могут существенно снизить производительность многосетевого моста; следовательно, если взаимодействие обеих сетей не согласовано, сбои, скорее всего, возникать будут. В этом случае сначала проверьте, нет ли сбоев в обоих сегментах сети, а также посмотрите статистику по уровню использования и ошибкам, что может помочь локализовать неисправность в одной из двух сетей. Если сбои не прекращаются, то, вероятно, для той же цели следует воспользоваться маршрутизатором — как известно, при выполнении такого рода задач они демонстрируют более высокую степень надежности.

Маршрутизаторы и шлюзы

До сих пор в данной главе и в *гл. 13* мы обсуждали только те сетевые устройства, которые работают на первом и втором уровнях модели OSI. Эти устройства хорошо справляются с задачами, связанными с повторением, организацией мостов и коммутацией в пределах сети; в то же время они не могут передавать данные между двумя или несколькими сетями.

Этот пробел заполняет устройство, работающее на сетевом (3-м) уровне модели OSI и способное выполнять маршрутизацию данных между двумя или несколькими однородными или разнородными сетями с учетом информации об источнике, пункте назначения или их обоих. В ранний период развития Интернета это устройство называли *шлюзом*, т. к. первоначально оно объединяло высокопроизводительные машины в рамках глобальной сети. Позже такие устройства начали выполнять функцию связывания локальных сетей, и теперь, в соответствии со своей основной функцией, они называются *маршрутизаторами.*

Понятие маршрутизатора

Маршрутизатор представляет собой сетевое устройство с двумя или несколькими интерфейсами, которые обычно подсоединяются к локальным сетям или каналам глобальных сетей (т. е. ISDN, DSL, T-1, T-3 и т. д.). Маршрутизатор выполняет функцию направления данных из одной сети в другую. Отличие маршрутизатора от моста заключается в том, что маршрутизатор передает данные на сетевом уровне; следовательно, маршрутизаторы способны передавать данные через различные сети, которые могут относиться к одному или разным типам канального уровня (Ethernet, маркерное кольцо, FDDI, ATM, ретрансляция кадров). Кроме того, сетевые широковещательные сообщения, как правило, не циркулируют между маршрутизированными сетями, хотя некоторые маршрутизаторы и обеспечивают широковещательную ретрансляцию или функцию прокси в отношении протоколов, подобных BOOTP и DHCP. Процесс маршрутизации можно представить следующим образом.

1. При получении кадра информация о нем удаляется, и дейтаграмма анализируется в поисках ошибок. При возможности все ошибки исправляются, и кадр перенаправляется по стеку.
2. Сетевой уровень определяет адрес назначения, указанный в заголовке, выявляет сетевую часть этого адреса и на ее основе проводит поиск в таблице маршрутов.
3. В таблице маршрутов выполняется поиск сети назначения, проводится выбор наиболее точного из доступных маршрутов (например, с участием 192.168.4.0 вместо 192.168.0.0). Если маршрут не найден, на адрес источника отправляется сообщение ICMP "Network Unreachable" ("Сеть недостижима").
4. В поле Time To Live (время жизни, TTL) маршрута кадра вносятся все необходимые изменения. Это поле является средством выявления петель. Когда показатель счетчика TTL равен нулю, кадр отбрасывается, и происходит отправка сообщения ICMP "TTL Expired" ("Время жизни маршрута истекло").
5. Проводится подготовка к перенаправлению кадра на следующий транзит (хоп), который определяется по таблице маршрутов. Проверяется показатель MTU (Maximum Transmit Unit — максимальная единица передачи данных) сети сле-

дующего транзита (к примеру, в сети Ethernet MTU равна 1514 байт/кадр); при необходимости кадр фрагментируется в соответствии с этим параметром.

6. Готовый к отправке пакет данных ставится в нужную очередь выходного интерфейса, после чего происходит перенаправление пакета на следующий хоп. Если очередь переполнена или маршрут стал недействительным, пакет отбрасывается, о чем нужно по возможности оповестить его источник.

Так как маршрутизаторы передают данные на сетевом уровне, для упаковки данных в маршрутизируемую форму необходим протокол сетевого уровня. В качестве примеров основных маршрутизируемых протоколов сетевого уровня выступают протоколы IP и IPX, хотя первый из них в современных сетях получил значительно большее распространение, и в настоящее время именно он используется в качестве единственного протокола сетевого уровня в сети Интернет.

Протокол IP обращается к хостам посредством 32-битового или 4-октетного адреса, с помощью которого маршрутизатор определяет источник и пункт назначения пакета. Поэтому каждый хост имеет IP-адрес типа "192.168.4.28". Хосты выделяются в логические сети с помощью *маски сети*, которая сообщает хосту и маршрутизатору, в какой подсети они находятся. Маска сети определяет, какая часть IP-адреса идентифицирует сеть, а какая — хост. К примеру, IP-адрес 192.168.6.7 с маской сети 255.255.255.0 обозначает хост 7 в сети 192.168.6, а IP-адрес 10.20.4.13 с маской сети 255.255.0.0 — хост 4.13 в сети 10.20. Это средство адресации очень напоминает телефонную сеть, в которой код региона и префикс указывают на районную АТС (или, в нашей терминологии, сеть), а последние четыре цифры обозначают конкретную телефонную линию (или, в нашей терминологии, хост) в районной АТС.

Чтобы маршрутизатор имел возможность передавать трафик между двумя различными сетями, он не только должен быть подключен к каждой из них, но и должен обладать IP-адресом в каждой из этих логических сетей. К примеру, на рис. 14.2 изображены две сети с адресами 192.168.11.0 и 192.168.4.0, каждой из которой соответствует маска сети 255.255.255.0. Эти сети подключены к маршрутизатору с адресами 192.168.11.1 и 192.168.4.1, соответственно; при этом для каждого хоста в сети настроены IP-адрес, маска сети и шлюз (локальный маршрутизатор). Предположим, что хост 192.168.11.46 передает пакет данных хосту 192.168.11.18. Так как оба этих хоста находятся в одной IP-сети, данные перемещаются между двумя рабочими станциями, не проходя ни через маршрутизатор, ни через шлюз. Затем хост 192.168.11.46 передает пакет данных хосту 192.168.4.13, который находится в другой IP-сети. В этом случае рабочая станция сначала отсылает пакет своему шлюзу или маршрутизатору 192.168.11.1. Маршрутизатор исследует заголовок пакета и считывает IP-адрес пункта назначения. Затем он сравнивает этот адрес со своей таблицей маршрутов и вычисляет подходящий маршрут. В нашем случае сеть назначения напрямую подсоединена к сети источника, так что маршрутизатор, зная, как достичь сети 192.168.4.0, передает пакет напрямую подсоединенному интерфейсу сети 192.168.4.0. Наконец, пакет прибывает на адрес назначения 192.168.4.13.

Примечание

Хосты и сетевые устройства, расположенные в пределах одной IP-сети, на канальном уровне пользуются MAC-адресацией и формируют собственную таблицу преобразования IP-адресов в MAC-адреса, пользуясь для этого протоколом APR (Address Resolution Protocol — протокол разрешения адресов). Чтобы просмотреть таблицу ARP хоста, следует ввести команду `arp -a` (в системе на базе Windows) или `show ip arp` (на маршрутизаторе Cisco).

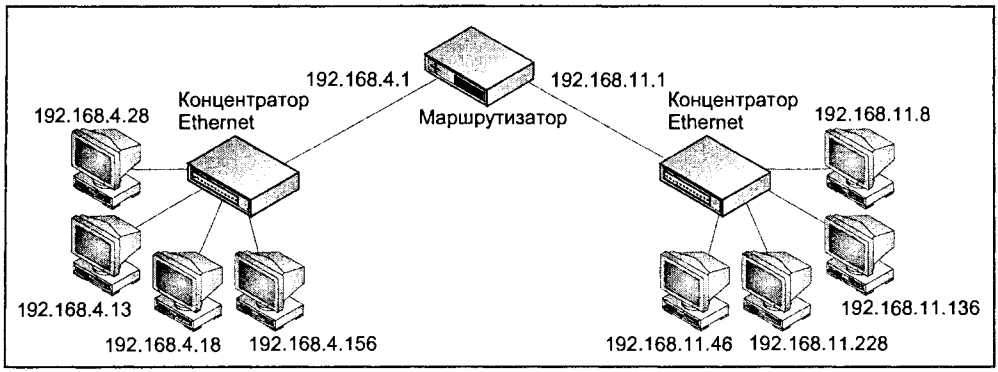


Рис. 14.2. Две сети в рамках различных IP-подсетей, соединенные одним маршрутизатором

После рассмотрения процесса маршрутизации между напрямую соединенными сетями возникает вопрос: "Если маршрутизатор может осуществлять маршрутизацию только между двумя непосредственно связанными сетями, как он вычисляет маршрут к **www.yahoo.com**?" Действительно, отдельные маршрутизаторы могут осуществлять маршрутизацию только между сетями, соединенными напрямую; но маршрутизаторы могут работать совместно, показывая друг другу пути из точки A в точку B. Этот процесс называется прохождением транзитов (хопов) в сетях.

Вычисление маршрутов

Чтобы один маршрутизатор осуществлял трафик через бесчисленное множество других маршрутизаторов, он должен знать, по какому пути отсылать пакет — по-другому это называется следующим хопом пакета. Данные о путях используются маршрутизаторами совместно, а обмен ими производится с помощью одного или нескольких протоколов маршрутизации, таких как RIP, OSPF и BGP.

Есть три типа маршрутов — связанные (с указанием адреса непосредственно подключенных сетей), статические и динамические. Примеры связанных маршрутов в этой главе уже приводились — они создаются, когда маршрутизатор имеет прямое физическое соединение с сетью. Статические маршруты необходимо вводить вручную с указанием следующего хопа для данной сети назначения. Кроме того, любые маршруты содержат данные о маршрутных затратах (метрику), которые применяются маршрутизатором для выбора маршрута. Практически, чем ниже маршрутные затраты или метрика, тем более предпочтительным является маршрут.

Замечательным примером статического маршрута является крайне важный маршрут по умолчанию. Маршрут по умолчанию сообщает маршрутизатору о том, куда необходимо отсылать данные, если в таблице перенаправления по адресам не задан путь в сеть назначения. В конфигурационном файле маршрутизатора Cisco маршрут по умолчанию выглядел бы так:

```
ip route (Сеть назначения) (Маска сети назначения) Метрика_след._хопа
```

или

```
ip route 0.0.0.0 0.0.0.0 192.168.100.1 0
```

Сеть назначения 0.0.0.0 и маска сети 0.0.0.0 определяют любую сеть; таким образом, если маршрутизатор не может найти в таблице перенаправления по адресам более точного совпадения, он последует этому маршруту и отошлет данные этого маршрута на следующий хоп 192.168.100.1. Так работают многие выделенные интернет-соединения, когда маршрутизатор клиента располагает лишь одним маршрутом по умолчанию, который пересылает все данные подключенному провайдеру. Маршрутизация данных и их направление предполагаемому получателю происходит далее через сеть поставщика услуг Интернета.

Примечание

Маршруты по умолчанию могут также распространяться через протоколы динамической маршрутизации, но более разумно задать статический маршрут по умолчанию как наихудший, с высокой метрикой или затратами, на случай отказа динамической маршрутизации.

Динамический маршрут вычисляется на основе одного из множества различных протоколов динамической маршрутизации. "Динамическими" такие маршруты называются потому, что они динамически изменяются при изменении пути к данной сети. При этом маршрутизатор должен быть настроен только на отслеживание трафика или участие в данном протоколе динамической маршрутизации с указанием других маршрутизаторов (их называют соседями маршрутизатора), от которых он будет получать маршруты.

Протоколы динамической маршрутизации подразделяются на две основные группы в зависимости от того, в какой области сети они применяются; называются они *внутренними* и *внешними* протоколами маршрутизации. Внутренние протоколы можно охарактеризовать как средство обмена маршрутной информацией с данной группой внутренних сетей или автономной системой (Autonomous System, AS). *Автономная система* представляет собой совокупность сетей одной организации или группу, управляемую центральной организацией. Обычно собственную автономную систему имеет поставщик услуг Интернета, и в ее рамках находятся все его клиенты. Как правило, в автономной системе существует несколько методов доступа или подключения к другим внешним сетям, поэтому многие организации с единственным средством установления соединения не имеют собственной автономной системы.

Наиболее распространенными внутренними протоколами маршрутизации являются протокол RIP (Routing Information Protocol — протокол маршрутной информации) и протокол OSPF (Open Shortest Path First Protocol — протокол первоочередного открытия кратчайших маршрутов). Во многих сетях протокол RIP используется до сих пор, а в крупных сетевых средах широко применяется протокол OSPF, т. к. он выполняет маршрутные обновления значительно эффективнее.

Однако основное различие между протоколами RIP и OSPF заключается в том, как каждый из них определяет оптимальный путь к пункту назначения. К примеру, протокол RIP применяет *дистанционно-векторный метод маршрутизации*, при котором решения о маршрутизации принимаются на основе расстояния или количества хопов и вектора (направления), в котором пакет должен следовать к пункту назначения. После того как протокол RIP соберет информацию о направлениях и расстояниях для данной сети, алгоритм Беллмана-Форда анализирует эту информацию и определяет, какой путь является наилучшим.

Протокол OSPF отличается от RIP тем, что использует основанный на состоянии связей метод маршрутизации, который собирает маршрутную информацию на общесетевом топографическом уровне. Затем эта информация анализируется алгоритмом Дийкстра, и составляется текущая таблица перенаправления по адресам. Протокол OSPF превосходит RIP во многих отношениях, но особенно это проявляется в крупных сетевых средах, когда быстрые и эффективные маршрутные обновления, выполняемые OSPF, в значительной степени обуславливают стабильность сетей при изменении маршрутов. При использовании протокола OSPF всякий раз, когда маршрутизатору нужно обновить доступные пути к другим маршрутизаторам, он отправляет всем ближайшим соседям-маршрутизаторам короткий служебный пакет LSA (Link-State Advertisement — объявление состояния связи) для определения состояния линии связи. Этот служебный трафик затем анализируется и встраивается в таблицу перенаправления соседних маршрутизаторов, которые, в свою очередь, отсылают собственные служебные пакеты LSA другим соседним маршрутизаторам и т. д. Этот процесс происходит лишь в том случае, если из-за изменения маршрута или состояния линии связи таблица перенаправления маршрутизатора подверглась изменениям — этим протокол OSPF отличается от RIP, который отсылает маршрутные обновления вне зависимости от изменения маршрутов.

Другой важной функцией протокола OSPF, которая обеспечивает минимальное время конвергенции маршрутов и контролирует поток служебных сообщений, является применение областей в рамках маршрутной иерархии. Крупную сеть можно разбить на несколько более мелких областей маршрутизации OSPF, каждая из которых имеет собственную базу данных состояния связей и поток служебных сообщений LSA. Для объединения последовательности областей OSPF существует магистральная область или область 0, в которую все остальные области OSPF передают информацию о состоянии связей для агрегирования маршрутов между сетями.

Общая схема работы протокола маршрутизации OSPF выглядит следующим образом.

1. Выполняется настройка OSPF на каждом маршрутизаторе в рамках данной области. В ходе конфигурации маршрутизатору автоматически или вручную присваивается уникальный идентификатор, в роли которого выступает старший IP-адрес интерфейса.
2. Затем OSPF пытается создать *смежности* (adjacencies) или каналы связи для передачи информации о маршрутизации. Соседи OSPF могут находиться по другую сторону двухточечных каналов (T-1, T-3 и т. д.), широковещательных каналов (сети Ethernet) и даже каналов NBMA (Nonbroadcast Multiple Access Link — нешироковещательная сеть с множественным доступом) типа ATM или ретрансляции кадров.
   - Чтобы ограничить количество смежностей в рамках данной сети, протокол OSPF распределяет маршрутизаторы по типам. К примеру, в некоторых сетевых реализациях OSPF *назначенный маршрутизатор* (Designated Router, DR) назначается на роль ведущего сервера маршрутов (master route server); таким образом, все маршрутизаторы в пределах этой сети OSPF отсылают свои служебные пакеты LSA только ведущему серверу маршрутов. При использовании областей OSPF в каждой из них присутствует один или несколько *пригранич-ных маршрутизаторов* (Area Border Router, ABR), которые передают маршрутную информацию между собственными областями и магистральной областью.

3. Обмен информацией в OSPF состоит из трех основных процессов:
   - Сначала маршрутизатор запускает OSPF со специальным коротким *приветственным сообщением* (HELLO) для установления связи с соседним маршрутизатором OSPF. Сообщение HELLO также используется для задания в сети назначенного маршрутизатора.
   - После установления смежностей маршрутизатор задействует процесс "обмена", с помощью которого он делится информацией о своих связях с соседями. Дополнительно, в ходе этого процесса маршрутизатор получает от своих соседей информацию о других связях. Все данные, полученные в результате обмена, хранятся в базе данных состояния связей, синхронизация которой между всеми маршрутизаторами данной сети OSPF производится посредством процессов обмена и лавинной адресации.
   - После завершения процесса обмена маршрутизаторы OSPF оповещают своих соседей о состоянии связей с помощью процесса лавинной адресации. При этом сообщения LSA издаются или отсылаются методом лавинной адресации всем активным интерфейсам OSPF данного маршрутизатора. Сообщения LSA анализируются принимающими маршрутизаторами и при необходимости заносятся в базу данных состояния связей.
4. База данных состояния связей фактически не предоставляет маршруты или таблицы перенаправления по адресам: вместо этого к содержимому базы применяется алгоритм Дийкстра с целью анализа и установления кратчайшего пути к заданной сети, который затем вносится в таблицу перенаправления по адресам маршрутизатора.

В то время как внутренние протоколы маршрутизации обеспечивают динамическую маршрутизацию в рамках автономной системы, внешние протоколы маршрутизации отвечают за маршрутизацию между автономными системами. Одним из наиболее часто применяемых внешних протоколов маршрутизации является протокол BGP (Border Gateway Protocol — пограничный межсетевой протокол). Как правило, этот протокол работает на одном или нескольких приграничных маршрутизаторах (border router), которые выполняют функцию шлюза из одной автономной системы, или группы сетей, в другую автономную систему.

Типичным примером использования протокола BGP могут быть поставщики услуг Интернета. Они применяют BGP для обмена маршрутной информацией друг с другом. Поставщики услуг довольно редко применяют BGP для обеспечения клиентской маршрутизации, но если клиент располагает многоканальной системой или подключением к нескольким поставщикам услуг, то это необходимо. Протокол BGP предусматривает маршрутизацию между крупными сетями; таким образом, этот протокол способен обрабатывать более 100 000 маршрутов, которые используются каждым приграничным маршрутизатором поставщика услуг для эффективного перенаправления данных через сеть Интернет. Ниже приводится пример таблицы маршрутизации поставщика услуг, в которой после обозначения сетей назначения указывается их текущий оптимальный следующие хоп:

```
Gateway of last resort is 10.0.1.1 to network 0.0.0.0
B  208.221.13.0/24 [20/0] via 10.26.199.239, 1w4d
B  206.51.253.0/24 [20/0] via 10.26.199.239, 1w4d
B  205.204.1.0/24 [20/0] via 10.26.199.239, 1w4d
```

```
B  204.255.51.0/24 [20/0] via 10.26.1.236, 3d11h
B  200.68.140.0/24 [20/0] via 10.26.199.239, 1w4d
B  199.221.26.0/24 [20/0] via 10.26.29.249, 1w0d
B  199.0.199.0/24 [20/0] via 10.26.196.111, 1w4d
B  192.68.132.0/24 [20/0] via 10.26.17.244, 11:23:10
   170.170.0.0/16 is variably subnetted, 3 subnets, 3 masks
B    170.170.0.0/19 [20/0] via 10.26.199.239, 1w4d
B    170.170.224.0/20 [20/0] via 10.26.199.239, 1w4d
B    170.170.254.0/24 [20/0] via 10.26.33.249, 1w4d
B  216.239.54.0/24 [20/0] via 10.26.17.244, 4d14h
```

Примечание

Обсуждению OSPF, BGP и других протоколов маршрутизации можно посвятить целую книгу, поэтому если вы хотите получить более подробную информацию о протоколах маршрутизации, обратитесь к дополнительным источникам, приведенным в конце главы.

Установка и настройка маршрутизаторов

Установить маршрутизатор довольно просто, т. к. в корпоративной среде большинство маршрутизаторов ограничивается тремя или четырьмя сетевыми интерфейсами. Чтобы пояснить процессы установки и конфигурирования, мы рассмотрим установку маршрутизатора в окружении, изображенном на рис. 14.3.

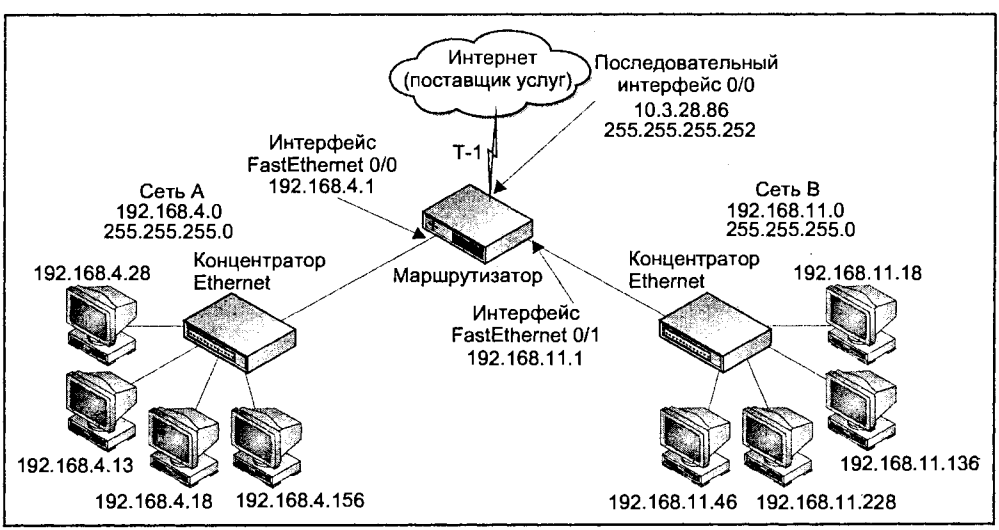


Рис. 14.3. Пример сети, в которой осуществляется конфигурация маршрутизатора

Среда нашего примера состоит из двух локальных сетей (A и B), у каждой из которых есть собственная подсеть IP. Кроме того, есть одно соединение T-1 с поставщиком услуг. Адресация локальных сетей производится с помощью 192.168.4.0 и

192.168.11.0, соответственно; при этом маршрутизатор имеет интерфейсы 192.168.4.1 и 192.168.11.1 для локальных сетей; 10.3.28.86 соответствует интерфейсу T-1. Так как в подобных средах маршрутизаторы Cisco используются довольно часто, в этом примере мы также будем иметь дело с маршрутизатором Cisco 3640. Принимая во внимание вышеприведенные данные, маршрутизатор будет оснащен тремя интерфейсами: двумя Fast Ethernet и одним последовательным (T-1) интерфейсом со встроенным устройством CSU (Channel Service Unit — устройство обслуживания канала).

Установку маршрутизатора следует начинать с подключения к нему силового кабеля. После этого подключите маршрутизатор к каждой локальной сети с помощью кабеля Ethernet. Порты Fast Ethernet маршрутизатора следует маркировать Fast Eth 0 и Fast Eth 1. В нашем примере необходимо подключить сеть A к Fast Eth 0, а сеть B — к Fast Eth 1. Наконец, пользуясь кабелем T-1, подключите канал T-1 к порту RJ-45 с маркировкой Serial 0.

Примечание

В некоторых сборках могут потребоваться перекрестные кабели. По этой причине всегда следует иметь в запасе несколько таких кабелей, тогда при появлении трудностей в установлении связи вы сможете воспользоваться кабелем другого типа. Кроме того, будьте внимательны: не подключите сеть Ethernet к последовательному порту, и наоборот — их гнезда на маршрутизаторе идентичны.

Имейте в виду, что межсетевая операционная система Cisco различает сетевые интерфейсы типа `Тип_интерфейса Номер_слота/Номер_порта`. Таким образом, если все интерфейсы примера, которые нам следует настроить, установлены на слот 0, при настройке порты Fast Ethernet будут обозначены как FastEthernet 0/0 и FastEthernet 0/1, а интерфейс T-1 — как Serial 0/0.

Прежде чем в первый раз включать питание маршрутизатора, имеет смысл сначала подключиться к консоли устройства. Это позволит вам просматривать загрузочные диагностические данные и цикл загрузки маршрутизатора, что может привлечь внимание к возможным аппаратным неисправностям. Чтобы подключить консоль, в первую очередь найдите синий или черный консольный кабель, входящий в комплект маршрутизатора. На большинстве современных моделей маршрутизаторов Cisco есть последовательный консольный порт RJ-45 с маркировкой "Console" или "CON". Подключите конец кабеля с разъемом RJ-45 к консольному порту маршрутизатора, а конец кабеля с DB9 (возможно, потребуется адаптер последовательного порта) — к терминалу VT100 или рабочей станции с программным обеспечением для эмуляции терминала. После этого терминалу или программе эмуляции терминала следует задать следующие настройки: 9600 бод, 8 бит данных, отсутствие контроля по четности, 1 стоповый бит. Выполнив эту задачу, включите питание маршрутизатора; в результате должно появиться следующее сообщение:

```
System Bootstrap, Version 12.0(3)T, RELEASE SOFTWARE (fc1)
Copyright © 1999 by cisco Systems, Inc.
```

После этого маршрутизатор запускает свои диагностические средства и начинает загружать межсетевую операционную систему (Internetwork Operating System, IOS). Кроме того, маршрутизатор проводит идентификацию интерфейсов и запоминаю-

щих систем, которые он способен обнаружить, и выводит сообщение, подобное следующему:

```
cisco 3640 (R4700) processor (revision 0x00) with 44032K/5120K
bytes of memory.
Processor board ID 28351804
R4700 CPU at 100Mhz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)
16384K bytes of processor board PCMCIA Slot0 flash (Read/Write)
```

После завершения процесса загрузки маршрутизатора выводится сообщение "Router con0 is now available, Press RETURN to get started" ("Маршрутизатор con0 готов к работе, для запуска нажмите <RETURN>"). Чтобы приступить к конфигурированию, просто нажмите клавишу <Enter> на клавиатуре терминала. Вероятно, маршрутизатор обнаружит, что его загрузка происходит впервые, и спросит, не хотите ли вы запустить программу настройки. В нашем примере выберите вариант "NO", после чего появится приглашение маршрутизатора `Router>`.

Для того чтобы конфигурирование стало возможным, сеанс консоли необходимо перевести в разрешающий режим или назначить ему уровень привилегий 15. Для этого следует вести в командной строке `enable`. При обычных обстоятельствах для входа в разрешающий режим требуется ввод пароля, но, поскольку пока что пароль не установлен, маршрутизатор выведет новое приглашение `Router#`, которое обозначает, что был активирован разрешающий режим.

Прежде чем приступить к настройкам, мы настоятельно рекомендуем установить системные часы, т. к. диагностика неисправностей с неправильно датированными записями в журнале может оказаться довольно трудоемким занятием. Чтобы установить часы маршрутизатора, введите команду по шаблону

```
clock set ЧЧ:ММ:СС МЕСЯЦ ДЕНЬ ГОД,
```

например,

```
clock set 09:00:00 June 07 2002.
```

Подтверждать ввод маршрутизатор не будет — если установка прошла успешно, он просто возвратится к командной строке.

При первой загрузке маршрутизатор создает элементарную конфигурацию, в соответствии с которой он и продолжает работать. Чтобы просмотреть текущую рабочую конфигурацию, введите `show running-config` или `show run`. В результате рабочая конфигурация на терминале будет отображаться поэкранно.

Чтобы начать настройку для нашего примера, маршрутизатор необходимо перевести в режим конфигурирования. Для этого введите `configure terminal` или `config t`, в результате чего должно появиться новое приглашение `Router(conf)#`, обозначающее режим настройки.

Примечание

В режиме конфигурирования будьте предельно осторожны, потому что все без исключения изменения вступают в силу немедленно и могут неблагоприятно сказаться на работе сети, если вы по невнимательности введете неверные конфигурационные команды.

Как обычно, чтобы получить список возможных команд в ответ на любой запрос устройства, просто введите `?`. Чтобы получить список возможных завершений команды, введите имя этой команды и `?`. Функция вывода завершений команд есть во всех режимах (включая режим настройки) и может оказаться полезной при изучении функций, которые можно настроить на данном маршрутизаторе. Как правило, команды конфигурирования можно инвертировать или отменить, если перед именем команды ввести `no`. К примеру, если в процессе настройки интерфейса администратор вводит команду `shut`, интерфейс входит в состояние административного отключения. Чтобы отменить эту команду или блокировку интерфейса, следует ввести команду `no shut` — в результате ранее введенная команда будет удалена из конфигурации.

При настройке маршрутизатора можно пользоваться нижеперечисленными командами. Имейте в виду, что они обеспечивают лишь базовую конфигурацию, и для достижения желаемых функциональных возможностей маршрутизатора вам, вероятно, потребуются дополнительные команды.

- `hostname`. С помощью этой команды осуществляется настройка имени хоста маршрутизатора. После настройки она заменяет приглашение `Router>` введенным текстом.
- `aaa new-model`. Сообщает маршрутизатору о том, что мы будем настраивать функции учетной записи, аутентификации и авторизации с помощью нового набора команд — таким образом, старые команды отключаются.
- `aaa authentication`. Активизирует аутентификацию каждого пользователя маршрутизатора.
- `username USER PASSWORD`. Включает пользователя и его пароль в локальную базу данных пользователей.
- `enable secret`. Устанавливает пароль разрешающего режима с помощью более развитого алгоритма шифрования, чем старая команда `enable password`.
- `clock timezone`. Устанавливает часовой пояс для той географической зоны, в которой работает маршрутизатор.
- `ip subnet-zero`. Разрешает нулевую подсеть как тип подсети.
- `ip domain-name`. Задает доменное имя маршрутизатора.
- `ip name-server`. Указывает маршрутизатору на необходимость применения определенного сервера имен для разрешения DNS.
- `interface Serial | FastEthernetX/X`. Подготавливает маршрутизатор к принятию конфигурационных команд для указанного интерфейса.
- `ip address ADDRESS NETMASK`. Устанавливает IP-адрес и маску сети для настраиваемого интерфейса.
- `speed 100`. Устанавливает скорость порта Ethernet, равную 100 Мбит/с.

- `full-duplex`. Переводит порт Ethernet в полнодуплексный режим, что ограничивает неисправности, вызванные автосогласованием.
- `ip classes`. Указывает маршрутизатору на необходимость разрешения классов подсетей в целях маршрутизации.
- `ip route NETWORK NETMASK INTERFACE` или `NEXT-HOP METRIC`. Настраивает маршрут для указанной сети. В настоящем примере мы будем настраивать только маршрут по умолчанию, так что маршрутизатор будет перенаправлять весь нелокальный трафик поставщику услуг Интернета, подключенному к интерфейсу Serial 0/0. Кроме того, вместо оператора интерфейса `Serial 0/0` можно указать IP-адрес следующего хопа.
- `line con | aux | vty`. Подготавливает маршрутизатор к принятию конфигурационных команд для определенного терминального устройства.

Принимая во внимание эти команды, а также то, что маршрутизатор находится в режиме конфигурирования, для его настройки (в нашем примере) необходимо ввести следующее:

```
hostname ExampleRouter

aaa new-model
aaa authentication login default local enable
username jdoe password hound
enable secret AgoodPassword

clock timezone EST -5
ip subnet-zero
ip domain-name sampledomain.com
ip name-server 10.99.99.28

interface Serial0/0
 ip address 10.3.28.86 255.255.255.252
 encapsulation ppp
 no fair-queue
 service-module t1 timeslots 1-24

interface FastEthernet0/0
 ip address 192.168.4.1 255.255.255.0
 speed 100
 full-duplex

interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 speed 100
 full-duplex

ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0 0
no ip http server
```

```
line con 0
 password пароль_для_консоли
 transport input none
line aux 0
 password auxpasswordhere
line vty 0 4
 password telnetpasswordhere
```

Примечание

Не забудьте правильно изменить все имена пользователей и пароли. После настройки полномочий для доступа к маршрутизатору нужно будет пользоваться именно ими.

Если конфигурация проведена правильно, маршрутизатор должен снова отобразить свою командную строку, но теперь ее приглашением должно стать `ExampleRouter#`. Чтобы проверить конфигурацию интерфейсов, следует ввести

```
show ip interfaces brief;
```

в результате будет выведена таблица с перечислением трех настроенных интерфейсов; она будет выглядеть примерно так:

```
Interface      IP-Address    OK? Method Status  Protocol
FastEthernet0/0  192.168.4.1   YES manual up    up
Serial0/0      10.3.28.86    YES manual up    up
FastEthernet0/1  192.168.11.1  YES manual up    up
```

После проверки настроек интерфейсов не забудьте сохранить текущую рабочую конфигурацию с помощью команды `copy running-config startup-config` или (сокращенно) `copy ru st`. Кроме того, можно вводить устаревшую команду `write memory`, хотя она вышла из употребления и в ближайшем будущем, видимо, будет удалена из межсетевой операционной системы Cisco. Если команду `copy` не ввести, конфигурация будет потеряна после первой же перезагрузки маршрутизатора. После сохранения конфигурации выйти из консоли можно с помощью команды `logout`. Теперь маршрутизатор готов к работе.

Об управлении маршрутизатором

Маршрутизаторы являются высокоинтеллектуальными устройствами и при этом обладают довольно простыми интерфейсами управления. Ранее в этой главе уже говорилось о существовании нескольких различных методов обращения к управляющим функциям маршрутизатора: прямой консольный доступ, доступ с помощью Telnet, протокола SNMP, а в некоторых случаях — доступ с помощью графического пользовательского Web-интерфейса средствами HTTP.

Практически все маршрутизаторы поддерживают метод консольного доступа, который, как правило, осуществляется через последовательный порт RJ-45 или DB-9. Для некоторых маршрутизаторов обязательно использовать специальный (фирменный) консольный кабель, поставляемый в комплекте, поэтому если вы не применяете этот кабель в данный момент, не потеряйте его. В большинстве случаев про-

грамма эмуляции терминала с настройками 8-N-1 предоставляет доступ к текстовому интерфейсу командной строки. В интерфейсах управления различных производителей применяются разнообразные команды, но большинство интерфейсов предусматривает функцию вывода возможных команд. Поэтому начинайте работу с ввода команды `?` или `help` — это поможет вам выбрать нужную команду или параметр настройки.

Многие маршрутизаторы поддерживают доступ к командной строке с помощью сетевой службы Telnet. Маршрутизатор использует клиента Telnet для подключения к одному из IP-адресов интерфейса. В маршрутизаторах Cisco эти соединения называются сеансами VTY; их настройка производится в разделе конфигурации "Line VTY". Этот метод доступа к функциям управления маршрутизатором практически не отличается от метода доступа консольного доступа, однако будьте внимательны и не внесите никакие изменения в настройку, которая может помешать осуществлению доступа или завершить текущий сеанс Telnet с маршрутизатора. Это особенно важно, если администратор не находится непосредственно рядом с устройством.

Многие администраторы пользуются командой Cisco `reload in XX`, обеспечивающей проведение плановых перезагрузок при внесении в конфигурацию существенных изменений, которые могут случайно повлиять на доступ. После настройки перезагрузки (если она не была отменена) маршрутизатор повторно загружает ранее сохраненную конфигурацию и вновь становится доступным. Естественно, при этом предполагается, что администратор не сохранил последние изменения в конфигурации. Учтите, что с начала перезагрузки маршрутизатора и до ее завершения устройство не осуществляет перенаправление трафика.

Некоторые маршрутизаторы также поддерживают доступ к своим управляющим функциям с помощью графического пользовательского Web-интерфейса. Такие интерфейсы, несомненно, значительно упрощают операции управления, но во многих современных маршрутизаторах для установки некоторых настроек нужно использовать интерфейс командной строки (Command-Line Interface, CLI). Применяя графический пользовательский интерфейс, не забудьте сделать все необходимое, чтобы обеспечить его защиту — с помощью списков доступа по IP или другого способа контроля доступа.

Для обеспечения активного управления маршрутизатором многие организации используют протокол SNMP. Этот протокол позволяет консоли управления (типа HP OpenView или SNMP-C) опрашивать сетевые устройства для получения важных статистических данных, например, о пропускной способности интерфейса или показаниях счетчика ошибок. Кроме того, протокол SNMP позволяет устройству передавать аварийные сигналы при возникновении ошибки, например, нарушения электропитания или чрезмерном повышении температуры. Дополнительно, свободно распространяемые программы типа MRTG с помощью протокола SNMP способны запрашивать у маршрутизатора такую информацию, как уровень использования пропускной способности, и создавать сравнительно достоверные графики, помогающие проводить анализ изменения любого показателя.

Примечание

При использовании протокола SNMP мы настоятельно рекомендуем присвоить частной и общей строкам сообщества необычные значения. Кроме того, если маршру-

тизатор поддерживает режим фильтрации IP-адресов для доступа средствами SNMP, советуем активировать эту функцию для повышения уровня безопасности устройства.

Если в сети установлено более одного маршрутизатора, управление ими можно немного упростить, если ввести в данную среду SYSLOG-сервера. SYSLOG представляет собой централизованное средство регистрации, которому все сетевые устройства могут отсылать свои журналы. В результате значительно облегчается диагностика сетевых сбоев, т. к. все регистрационные данные находятся в одном месте. Кроме того, имейте в виду, что некоторые сетевые устройства при перезагрузке избавляются от своих регистрационных файлов; таким образом, если маршрутизатор внезапно перезагрузится, вам вряд ли удастся узнать, почему это произошло.

Многие производители регулярно выпускают новые версии микропрограммного обеспечения. Настоятельно рекомендуем пользоваться именно последними версиями микропрограммных средств. Помимо добавления новых функций и изменения существующих, эти версии часто содержат заплаты на слабые места в системе защиты. Это не значит, что на маршрутизатор следует устанавливать каждую новую версию; напротив, при появлении новых выпусков микропрограммного обеспечения вам следует в первую очередь ознакомиться с сопровождающей их информацией и решить, стоит ли устанавливать эту версию. По возможности протестируйте новую версию микропрограммного обеспечения на неиспользуемом устройстве и только затем загружайте его на рабочий маршрутизатор.

Что касается безопасности, многие маршрутизаторы поддерживают фильтрацию пакетов на основе любой комбинации источника, пункта назначения и номера порта. В межсетевой операционной системе Cisco эта функция называется списками доступа (Access Lists), установка которых производится в режиме конфигурирования. Эта функция особенно полезна при обеспечении безопасности сети в отсутствие брандмауэра. Кроме того, ее можно использовать для запрета доступа определенных хостов или сетей во внутреннюю сеть на основании IP-адреса назначения или номера порта. Чтобы ознакомиться с этой функции более подробно, воспользуйтесь руководством по эксплуатации маршрутизатора или свяжитесь с его производителем.

Примечание

При работе со списками доступа следует соблюдать осторожность, чтобы не отключить административный или легальный пользовательский доступ к маршрутизатору. Если у вас есть сомнения по поводу конфигурации, сначала лучше всего проверить команды или хотя бы запланировать перезагрузку на случай, если доступ к маршрутизатору будет потерян.

Одна из самых полезных функций маршрутизации называется *трансляцией сетевых адресов* (Network Address Translation, NAT). Эта функция предусматривает обращение к локальной сети посредством частного или зарезервированного пространства IP-адресов. Когда хост или устройство с частным IP-адресом пытается отправить данные через маршрутизатор, последний перехватывает пакет и устанавливает соответствие между частным IP-адресом отправителя и общедоступным IP-адресом с возможностью маршрутизации; только после этого пакет выходит за пределы данной сети. Когда хост назначения отсылает данные обратно, маршрутизатор вспоминает (с помощью трансляции и таблицы сеансов), какой хост во внутренней сети запрашивал входящие данные и выполняет их маршрутизацию.

В большинстве случаев эта функция работает без осложнений, но когда внешний отправитель меняет ранее использовавшиеся номера портов источника или пункта назначения, маршрутизатору сложно определить, какому хосту в рамках частной сети нужно послать эти данные. В таких случаях требуется однозначное соответствие трансляции сетевых адресов; таким образом, IP-адресу X данных, прибывающих на маршрутизатор, ставится в соответствие внутренний или частный IP-адрес Y.

Примечание

Важно заметить, что в некоторых приложениях функция трансляции сетевых адресов не работает.

Некоторые управляющие команды

В разных маршрутизаторах наборы команд отличаются, но все же существует несколько базовых команд, которые необходимо иметь в виду при администрировании таких устройств. Команды, перечисленные ниже, относятся к межсетевой операционной системе Cisco, но и у многих других производителей есть аналогичные команды.

- `show ip arp`. Извлекает текущую таблицу ARP (Address Resolution Protocol — протокол разрешения адресов) данного маршрутизатора. Таблица ARP содержит данные о соответствии IP-адресов MAC-адресам хостов. Эта информация может оказаться полезной при выявлении дублирования IP-адреса.
- `show ip route`. Выводит таблицу текущего IP-маршрута или таблицу перенаправления по адресам. Во многих небольших сетях в нее входит лишь маршрут по умолчанию (0.0.0.0, 0.0.0.0) и маршруты ко всем напрямую подключенным интерфейсам. В крупных сетях такая таблица может быть значительно более объемной. Чтобы извлечь или проверить текущий маршрут до определенного пункта назначения, можно не просматривать таблицу целиком, а воспользоваться командой `show ip route IP-адрес_назначения`.
- `show ip interface brief`. Как указывалось ранее в этой главе, команда отображает сводку всех настроенных интерфейсов на маршрутизаторе. В состав сводки входят такие данные, как IP-адрес интерфейса и его текущее состояние. Помимо этого, командой `show ip interface INTERFACE` можно воспользоваться для получения подробной информации об указанном интерфейсе маршрутизатора (например, об уровне использования, ошибках или отброшенных пакетах).
- `show interface INTERFACE`. Как и предыдущая, эта команда выводит подробную информацию об интерфейсе, но она относится к аппаратному уровню (а не к IP и не к уровню протокола).
- `show process cpu | memory`. Если маршрутизатор работает медленно, эта команда помогает локализовать причину низкой производительности. В зависимости от установки, команда выводит либо текущую информацию о загрузке центрального процессора, соответствующую предысторию и различные процессы, исполняющиеся в центральном процессоре, либо данные об использовании памяти по отдельным процессам.
- `copy running-config tftp`. Всегда сохраняйте копию настроек маршрутизатора. С помощью этой команды можно перенести текущую конфигурацию маршрути-

затора на внешний сервер типа TFTP-сервера (или на FTP-сервер, если маршрутизатор должным образом настроен). Кроме того, эта команда с другими опциями позволяет при необходимости скопировать конфигурацию на новый маршрутизатор.

Поиск и устранение неисправностей маршрутизаторов и шлюзов

Так как маршрутизаторы работают на уровне 3, большинство неисправностей происходит на сетевом уровне. Как правило, это неисправности логического, а не физического характера. Учитывая этот принцип, многие неисправности можно локализовать с помощью нескольких команд, причем даже если неисправность имеет физический характер, вполне вероятно, что ее можно будет выявить очень быстро.

Администраторы чаще всего сталкиваются с жалобами на отсутствие связи. В таких случаях лучше всего запустить на неисправном хосте утилиту Traceroute или Ping. Traceroute отправляет ряд ICMP-пакетов в указанный пункт назначения; она должна отчитываться о времени отклика каждого хопа, через который пакет проходит на пути к цели. После завершения тестирования очевидным станет одно из следующих обстоятельств.

- Связь с пунктом назначения исправна, тогда, скорее всего, проблема локализуется на прикладном уровне неисправного хоста. Это нередко встречается в системах на базе Windows; чтобы устранить неисправность, достаточно перезагрузить компьютер. Иногда в таких случаях бывает полезно выполнить операцию Traceroute извне; если пункт назначения доступен из сети Интернет, это можно сделать с помощью сайтов типа **http://www.traceroute.org**.
- Утилита Traceroute достигает пункта назначения, но отчитывается о слишком длительном времени обращения или избыточным временем ожидания при прохождении хопа X или после него. Эта информация указывает на сетевую неисправность, которая расположена между последним нормально пройденным хопом и хопом с избыточным временем ожидания или в худшем случае с полной блокировкой по превышению времени. Если неисправный хоп находится вне локальной сети и маршрутизатора, сделать что-либо практически невозможно. Если хоп находится в сети поставщика услуг Интернета, сообщите ему о неисправности. Если же неисправный хоп расположен в локальной сети, проверьте, нет ли между ним и предыдущим нормальным транзитом физических дефектов. Если один из рассматриваемых хопов находится в пределах маршрутизатора, проверьте с маршрутизатора все интерфейсы на высокий уровень использования, наличие большого количества ошибок или отброшенных пакетов. Любой из этих показателей служит признаком либо физической неисправности (например, дефект в локальной сети или повреждение канала T-1), либо высокого уровня использования. Если источником проблемы является канал глобальной сети, немедленно сообщите об этом провайдеру.
- После прохождения хопа X Traceroute начинает непрерывно курсировать между двумя хопами. Эта ситуация служит признаком возникновения петли; следует проверить, нет ли между этими двумя маршрутизаторами конфликтующих маршрутов. Если петля расположена между локальным интерфейсом глобальной сети и ее удаленным интерфейсом или между локальной сетью и Интернетом, то

для устранения этой неисправности можно привлечь поставщика услуг Интернета. Наконец, убедитесь в том, что в таблице перенаправления по адресам маршрутизатора есть действующий маршрут к данному пункту назначения.

- Traceroute вообще не сообщает о достижимых хопах или блокировка по времени происходит на первом же хопе. Из этого следует, что либо в локальной сети есть физическая неисправность, либо на неисправном хосте присутствует ошибка конфигурации. Если потеря связи зарегистрирована на всех хостах, возможно, вышел из строя маршрутизатор или его интерфейс. Убедитесь в том, что локальный шлюз данной рабочей станции правильно настроен на Ethernet-интерфейс маршрутизатора. Наконец, возможно, что список управления доступом (Access Control List, ACL) на маршрутизаторе первого транзита не допускает передачи сообщений Traceroute или данных вообще; следовательно, нужно проверить, нет ли на данном маршрутизаторе такого списка.

Если маршрутизатор работает медленно или с большим временем ожидания, которое выявляет утилита Ping, проверьте уровень использования по статистике маршрутизатора. Если этот показатель действительно высок, то маршрутизатор будет пытаться буферизовать исходящие пакеты до тех пор, пока буферы не переполнятся, а затем он будет просто отбрасывать пакеты. Кроме того, проверьте уровень использования ресурсов центрального процессора и памяти маршрутизатора, возможно, источником неисправности является процесс, истощающий ресурсы маршрутизатора. Чрезмерная нагрузка на процессор и память иногда обусловлена отказом в обслуживании (Denial of Service, DoS). Об этом нужно поставить в известность поставщика услуг Интернета. Наконец, никогда не сбрасывайте со счетов регистрационные файлы маршрутизатора, т. к. могут помочь разобраться в неисправностях маршрутизатора.

Если связь периодически пропадает, но физические неисправности выявить не удается, обязательно проверьте настройки значений MTU и MRU (Maximum Receive Unit — максимальный размер принимаемого блока) каждого интерфейса (если это возможно). При неправильных настройках этих значений периодическое понижение производительности обуславливается высокой частотой фрагментации пакетов.

Если время от времени возникают сбои при выполнении некоторых приложений, вполне возможно, что порты, через которые соответствующие приложения проводят обмен информацией, блокируются списками контроля доступа. Убедитесь в том, что ни один из настроенных списков контроля доступа не блокирует порты TCP или UDP. Кроме того, если вы пользуетесь трансляцией сетевых адресов, помните, что не все сетевые приложения полностью поддерживают эту функцию, для правильной работы некоторых приложений может потребоваться установление однозначных соответствий.

Симптомы неисправностей

Мосты и маршрутизаторы — довольно сложные устройства, поэтому найти и устранить их неисправности иногда бывает непросто. Но поскольку оба этих устройства работают логично и последовательно, существенную помощь могут оказать хорошее понимание настройки этих устройств, а также сетевые графики. Ниже приводится список наиболее распространенных симптомов неисправности и способов устранения неисправностей.

Симптом 14.1. Не удается получить доступ к кабельному/DSL-маршрутизатору

Если Ping-запрос, отправленный на локальный интерфейс маршрутизатора, ни к чему не приводит, проверьте исправность кабеля на обоих концах соединения. Кроме того, убедитесь в том, что настройка IP-адресов и масок подсети обоих устройств выполнена верно. Наконец, при необходимости зайдите на маршрутизатор с помощью консольного кабеля и, проверив все прочие сетевые настройки, попытайтесь очистить ARP-кэш этого устройства.

Симптом 14.2. Диагностические светодиоды маршрутизатора не отражают корректную последовательность загрузки

Это может служить признаком существующей или потенциальной неисправности устройства. Ознакомьтесь с разделом руководства по эксплуатации маршрутизатора, посвященным кодам светодиода для последовательности загрузки. При загрузке маршрутизатора проверьте, нет ли на консоли маршрутизатора каких-либо сообщений.

Симптом 14.3. Светодиод связи или активности маршрутизатора не работает

Скорее всего, дело в неисправности кабеля между маршрутизатором и подключенным устройством. Проверьте кабель, а при необходимости замените его. Кроме того, убедитесь в том, что используется нужный тип кабеля, т. е. кабель прямого соединения, а не перекрестный, или наоборот. Что касается конфигурации, проверьте, не отключены ли интерфейсы маршрутизатора. Если интерфейсы обоих устройств настроены на автосогласование, имеет смысл провести их настройку вручную.

Симптом 14.4. Ваш широкополосный маршрутизатор прекращает работу

Широкополосные маршрутизаторы подвержены отказам в обслуживании и поскольку они постоянно включены, это может заметно повлиять на их работу. Такая ситуация может возникнуть, когда на один административный порт устройства направлен большой объем трафика. Зачастую простейшим способом избавиться от этой проблемы является перезагрузка устройства. Если сбои в работе устройства продолжаются, проверьте, нет ли в его регистрационных журналах информации о конфликтах при распределении ресурсов или о большом количестве ошибок на отдельном интерфейсе. Кроме того, узнайте, не выпускал ли производитель устройства новой версии микропрограммного обеспечения, которое предназначено для устранения этой неисправности.

Симптом 14.5. Не удается установить связь с другими компьютерами через маршрутизатор

Проверьте настройки рабочей станции, в особенности IP-маску подсети и все определенные на этой станции статические маршруты. Если компьютеры, с которыми не удается установить связь, находятся в другой подсети IP, проверьте правильность настройки на рабочей станции шлюза по умолчанию, а также наличие действующего маршрута к компьютеру назначения на маршрутизаторе. Кроме того, убедитесь в наличии действующей конфигурации IP на самом компьютере назначения.

Симптом 14.6. Не удается перемещаться по сети Интернет с помощью маршрутизатора

Проверьте статистику ошибок связи с глобальной сетью на интерфейсе управления маршрутизатором. Если для связи используется линия SDSL или кабельный канал, попробуйте перезагрузить маршрутизатор, чтобы он вновь вошел в сеть. Если через маршрутизатор успешно проходят Ping-запросы с IP-адресацией, а именованным URL-адресам этого сделать не удается, проверьте, настроены ли на данной рабочей станции один или несколько действующих DNS-серверов.

Симптом 14.7. Ваша Web-страница зависает, а загруженные данные оказываются поврежденными

Такая ситуация может свидетельствовать о неполадках при дуплексной передаче между рабочей станцией и концентратором/коммутатором, или между концентратором/коммутатором и маршрутизатором. Также проверьте, нет ли в статистике интерфейса маршрутизатора признаков частого появления ошибок в локальной сети или в каналах глобальной сети, подключенных к маршрутизатору.

Симптом 14.8. Не удается получить IP-адрес с использованием кабельного модема или DSL-маршрутизатора

Некоторые широкополосные модемы фиксируются на MAC-адресе подключенного устройства; таким образом, если вы недавно поменяли местами два устройства, то вам, возможно, не удастся получить IP-адрес с помощью протокола DHCP. Попробуйте очистить таблицу MAC или ARP маршрутизатора, отключив его буквально на пару секунд. Также убедитесь в отсутствии включенных персональных брандмауэров, т. к. иногда именно они являются причиной сбоев при назначении адресов протоколом DHCP.

Если неисправность вызвана DSL-маршрутизатором, убедитесь в том, что маршрутизатор настроен на обслуживание IP-адресов посредством протокола DHCP. Проверьте, достаточно ли в адресном пуле IP-адресов для всех хостов локальной сети.

Симптом 14.9. Почтовая программа не получает электронную почту через маршрутизатор

Если ваш почтовый клиент испытывает трудности при получении электронной почты, убедитесь в том, что порт 110 (обеспечивающий передачу по протоколу POP3) не заблокирован. Если вы используете другой почтовый протокол, удостоверьтесь в отсутствии блокировки его порта. Помимо этого, некоторые почтовые серверы не принимают и не отправляют почту на хосты с IP-адресами, которые не имеют соответствующих обратных DNS-записей. На специальном сайте, например, **http://www.samspade.com**, вы можете проверить наличие такой записи, выполнив поиск имени для вашего текущего IP-адреса. Если необходимая обратная DNS-запись отсутствует, обратитесь к вашему поставщику услуг Интернета.

Симптом 14.10. Маршрутизатор отказывается работать с NetMeeting

Если маршрутизатор настроен с использованием трансляции сетевых адресов или списком контроля доступа, вы можете применять NetMeeting на хосте со статическими соответствиями адресов и отсутствием списков контроля доступа, которые могли бы ограничить работу NetMeeting. Для исполнения своих разнообразных под-

программ это приложение пользуется множеством портов, ни один из которых не должен блокироваться списком контроля доступа.

Симптом 14.11. Маршрутизатор отказывается подключаться к вашему поставщику интернет-услуг

Проверьте все настройки интерфейса. В случае применения T-1 проверьте правильность установки настроек типа кадра и синхронизации. Маршрутизатор должен показывать состояние интерфейса и протокола как рабочее (Up), а если это не так, попробуйте сверить все настройки конфигурации с поставщиком услуг Интернета. Наконец попросите поставщика услуг Интернета провести удаленный тест для кольцевой проверки вашего маршрутизатора, чтобы проверить рабочее состояние канала T-1, а также провести проверку схемы с точки зрения передачи.

Симптом 14.12. Невозможно получить доступ к маршрутизатору через Web-страницу

Проверьте рабочий порт Web-сервера маршрутизатора. Если порт изменился, его нужно указать в составе URL-адреса в виде **http://1.2.3.4:8000** (конкретные цифры должны соответствовать текущему номеру порта). Если ранее использовались неверные аутентификационные данные, перед повторной попыткой обращения к устройству вам, вероятно, придется закрыть все окна Web-браузеров.

Дополнительные ресурсы

Bridge Functions Consortium (Консорциум по функциям мостов) на UNH IOL: **http://www.iol.unh.edu/consortiums**.

Cisco, "Основы организации мостов и коммутации": **http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/bridging.htm**.

Cisco,"OSPF": **http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ospf.htm**.

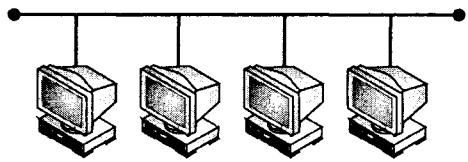
Cisco, "Поиск неисправностей в прозрачных мостовых средах": **http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1920.htm**.

Маршрутизация Cisco: **http://www.cisco.com/warp/public/732/Tech/routing.shtml**.

IEEE: **http://grouper.ieee.org/groups/802/3/**.

Juniper Networks: **http://www.juniper.net/techcenter**.

Руководство по маршрутизации средствами TCP/IP и IPX: **http://www.sangoma.com/fguide.htm**.



ГЛАВА 15

Брандмауэры и прокси-серверы

Брандмауэры и прокси-серверы являются двумя наиболее распространенными и важными средствами защиты сетей. Основная функция брандмауэров заключается в фильтрации сетевого трафика с целью предотвращения несанкционированного доступа в компьютерную сеть или из нее. Прокси-серверы выполняют запросы от имени внутренних пользователей при обращении к ненадежным (т. е. внешним) объектам. Прокси-службы могут предоставляться напрямую брандмауэром, но они могут располагаться и на отдельном хосте, работающем совместно с брандмауэром.

Введение в брандмауэры

Организация брандмауэров может быть очень разнообразна, и иногда брандмауэром фактически является совокупность нескольких компьютеров. В этой главе *брандмауэром* мы будем называть компьютер или компьютеры, расположенные между надежными (например, внутренними) и ненадежными (например, Интернет) сетями и контролирующие весь трафик, который между ними проходит. Эффективность брандмауэров обуславливается их следующими свойствами:

- все сообщения проходят через брандмауэр;
- брандмауэр пропускает только санкционированный трафик;
- брандмауэр способен выдерживать атаки на самого себя.

Эффективность брандмауэра значительно снижается в случае наличия альтернативного пути сетевой маршрутизации. Несанкционированный трафик можно провести в обход брандмауэра (это все равно, что охранять парадный вход, но черный ход оставлять открытым). Кроме того, если в вопросе дифференциации санкционированного и несанкционированного трафика на брандмауэр рассчитывать нельзя, или он настроен на пропуск опасных или ненужных сообщений, то он практически бесполезен. Наконец, т. к. брандмауэр призван противостоять атакам, но нет ничего, что оградило бы от них его самого, он должен быть способен отражать атаки на самого себя.

Брандмауэром может быть маршрутизатор, персональный компьютер, хост или совокупность хостов, специально настроенная на защиту частной сети от протоколов и служб, которые злонамеренно запускаются с хостов, находящихся вне надежной

сети. Как правило, брандмауэр устанавливается по периметру сети, т. е. находится между сетью и любыми внешними соединениями. При необходимости дополнительной защиты брандмауэры можно и нужно устанавливать внутри сетевого периметра, чтобы обеспечить защиту определенной группы хостов.

То, как брандмауэр обеспечивает защиту, зависит от его настроек и от настроек, заданных пользователем. В настоящее время существует четыре основных категории брандмауэрных технологий:

- фильтры пакетов;
- прикладные шлюзы;
- шлюзы уровня схем;
- механизмы с запоминанием состояния пакетов.

Брандмауэры и TCP/IP

Для того чтобы полностью разобраться в различиях и функциях брандмауэров, необходимо иметь представление о стеке протоколов TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/протокол Интернета). Мы уже рассмотрели вопросы организации сетей, теперь обратимся к свойствам TCP/IP, которые являются важной составляющей работы брандмауэров. Основное назначение TCP/IP заключается в том, чтобы предоставить компьютерам способ передачи данных другим компьютерам по сети. Функцией брандмауэра является контроль над прохождением трафика TCP/IP между хостами и сетями.

TCP/IP — это набор протоколов и приложений, которые выполняют функции, соответствующие определенным уровням модели OSI (Open Systems Interconnection — взаимодействие открытых систем). Передача информации в TCP/IP осуществляется путем независимых передач по сети блоков данных в форме пакетов. На каждом уровне модели TCP/IP к такому пакету добавляется очередной заголовок. В зависимости от применяемой технологии брандмауэра он использует информацию из заголовков, чтобы принимать решения, связанные с контролем доступа.

Порты

Эффективность передачи данных обуславливается тем, что большая часть хорошо известных служб работает через порты. Почти все брандмауэры принимают некоторые или все решения, связанные с контролем доступа, на основе информации о портах, содержащейся в заголовках пакетов.

Если бы поставщики услуг не использовали эти порты, они должны были бы извещать своих пользователей о том, какие порты им следует задействовать. К примеру, протоколу HTTP соответствует хорошо известный порт 80, и почти все Web-серверы в сети Интернет настроены на обслуживание HTTP-запросов именно через порт 80. Подключение к любому другому порту привело бы к ошибке. Если бы администратор решил, что его Web-сервер будет обслуживать запросы с помощью порта 81, ему пришлось бы сообщить всем пользователям о необходимости подключения через порт 81 (обычно порт указывается в браузере после URL-адреса, например, **http://www.somewebserver.com:81**). Порт 80 (или как в другом нашем примере порт 81) считается портом назначения TCP, и эта информация хранится в заголовке пакета TCP.

Примечание

Степень защищенности Web-сервера не увеличится, если он будет работать через нестандартный порт. Такие попытки обеспечить безопасность почти во всех случаях обречены на неудачу. Хакеры тратят много времени на сканирование портов. Именно так называется процесс систематического подключения к каждому порту в системе и определения наличия или отсутствия отклика. Следовательно, то, что ваш Web-сервер работает через порт 37244, очень скоро будет обнаружено!

В дополнение к портам назначения, пакеты TCP (и UDP) содержат данные о порте источника. *Порт источника* — этот порт, который применяется пользовательским стеком протоколов TCP/IP для подключения его к порту сервера. Кроме того, для пакетов, которые проходят от сервера к пользователю, он становится портом назначения. Обычно порт источника полупроизвольно назначается процессом TCP (или UDP) на хосте источника и, как правило, находится в диапазоне от 1023 до 65 535, хотя это и не требуется. На рис. 15.1 показано, как номера портов используются в пакетах TCP/IP.

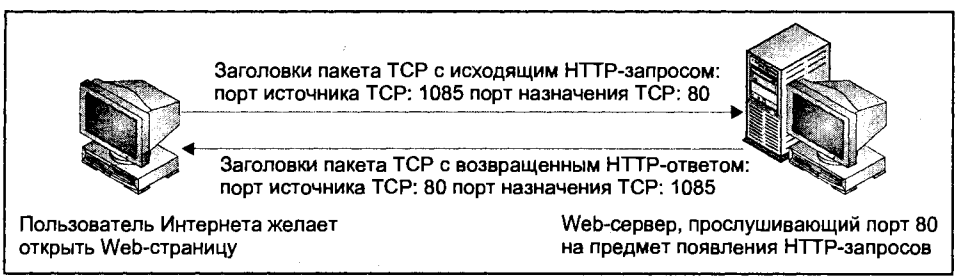


Рис. 15.1. Номера портов TCP в ходе HTTP-запроса

Список номеров портов TCP и приложений, с которыми они связаны, приводится в документе RFC 1700, "Assigned Numbers" ("Назначенные номера"). Полный перечень назначенных номеров портов TCP и UDP опубликован по адресу **http://www.iana.org/assignments/port-numbers**. В табл. 15.1 приведен небольшой список наиболее популярных служб и связанных с ними портов.

Таблица 15.1. *Краткий перечень наиболее распространенных номеров портов протоколов TCP и UDP*

Служба	Протокол	Порт
FTP FTP-данные	TCP	21 20
Протокол SSH	TCP	22
Telnet	TCP	23
SMTP	TCP	25
DNS (Передача зон)	TCP	53
DNS (Запросы)	UDP	53

Таблица 15.1 (окончание)

Служба	Протокол	Порт
HTTP	TCP	80
NetBIOS	TCP UDP	137—139
POP3	TCP	110
Протокол IMAP (Internet Message Access Protocol — протокол доступа к сообщениям в Интернете)	TCP	143
Протокол SNMP (Simple Network Management Protocol — простой протокол сетевого управления)	UDP	161
Захваты SNMP	UDP	162
HTTPS	TCP	443
X Windows	TCP	6000

Брандмауэры с фильтрацией пакетов

Брандмауэры с фильтрацией пакетов обеспечивают защиту сети путем фильтрации сетевых сообщений на основе информации, содержащейся в заголовках TCP/IP каждого пакета. Брандмауэр анализирует заголовок пакета и использует содержащиеся в нем данные для принятия решения относительно того, следует ли признать и маршрутизировать данный пакет в пункт его назначения, отказаться от пакета и без объявления отбросить его или отклонить пакет (т. е. отбросить его и оповестить об этом отправителя).

Фильтры пакетов принимают решения исходя из следующих данных заголовка:

- IP-адрес источника;
- IP-адрес назначения;
- применяемый сетевой протокол (TCP, UDP или ICMP);
- порт источника TCP или UDP;
- порт назначения TCP или UDP;
- тип сообщения ICMP (Internet Control Message Protocol — протокол управляющих сообщений в сети Интернет), если применяется протокол ICMP.

Кроме этой информации, для принятия решения хороший фильтр пакетов пользуется данными, которые не содержатся непосредственно в заголовке пакета — к примеру, информацией о том, через какой интерфейс был получен данный пакет.

У фильтра пакетов есть вход, набор фильтров и выход. На входе на брандмауэр заходит трафик из ненадежной сети. После этого пакеты обрабатываются в соответствии с тем набором фильтров, который использует брандмауэр (часто эти фильтры называются правилами). От этих фильтров зависит, будут ли пакеты признаны и через выход отправлены в пункт назначения, или без объявления отброшены или отклонены. Пример фильтра пакетов приводится в следующем разделе.

Пример фильтрации пакетов

Рассмотрим сеть, в которой содержится один Web-сервер и один почтовый сервер, доступные из сети Интернет. Кроме того, есть возможность администрирования этих серверов из Интернета посредством протокола SSH (Secure Shell Protocol — протокол сетевой оболочки); при этом использование этого протокола ограничено сетью источника с адресом 128.5.6.0/24. Описанная конфигурация показана на рис. 15.2. Разрешение входящих сообщений, поступающих через фильтр пакетов, предполагает принятие правил, приведенных в табл. 15.2.

Таблица 15.2. *Пример набора правил для фильтра входящих пакетов*

Правило	Протокол	Адрес источника	Адрес назначения	Порт источника	Порт назначения	Действие
1	TCP	128.5.6.0/24	129.1.5.155 128.1.5.154	>1023	22	Разрешить (Permit)
2	TCP	Любой	129.1.5.154	>1023	80	Разрешить (Permit)
3	TCP	Любой	129.1.5.155	>1023	25	Разрешить (Permit)
4	Любой	Любой	Любой	Любой	Любой	Запретить (Deny)

Иными словами, правило 1 разрешает хостам, находящимся в сети 128.5.6.0/24 (т. е. хостам 128.5.6.0—128.5.6.255), отправлять пакеты Web- или почтовому серверу, если номер их порта источника превышает 1023, а портом назначения является 22. Не забывайте, что фильтр пакетов воспринимает не SSH, а свойства заголовков TCP/IP. Если свойства пакета не полностью соответствуют правилу 1, они сравниваются со следующим правилом. Правило 2 разрешает любой сети отправлять пакеты Web-серверу, указывая порт назначения 80 (хорошо известный порт HTTP) и порт источника не ниже 1023. Если свойства пакета не соответствуют этому правилу, они сравниваются с правилом 3. Если пакет не отвечает требованиям и этого правила, он обрабатывается в соответствии с правилом 4, которое предполагает исключение любого трафика, не разрешенного ни одним из предыдущих правил. Помните, что брандмауэры должны пропускать только санкционированный трафик, а следовательно, в соответствии с оптимальными методами их настройки, последнее правило каждого набора должно предполагать отбрасывание любого трафика, который не был явно разрешен вышеприведенными правилами.

С набором правил, описанным в табл. 15.2, связано несколько существенных замечаний. Во-первых, правила обрабатываются сверху вниз, и при установлении соответствия обработка прекращается. Во-вторых, этот набор правил следует рассматривать как набор для его входящего трафика — не только потому, что он применяется к пакетам, поступающим на вход брандмауэра, но и потому, что сообщения TCP в действительности являются двусторонними. Для того чтобы обмен информацией стал возможен, необходим совместимый набор исходящих фильтров, применяемых к обратному трафику, также проходящему через брандмауэр. Если разрешается лю-

бой исходящий трафик, это необязательно. Но чаще всего организации предпочитают фильтровать исходящий трафик, чтобы не допустить утечки информации в ненадежную сеть.

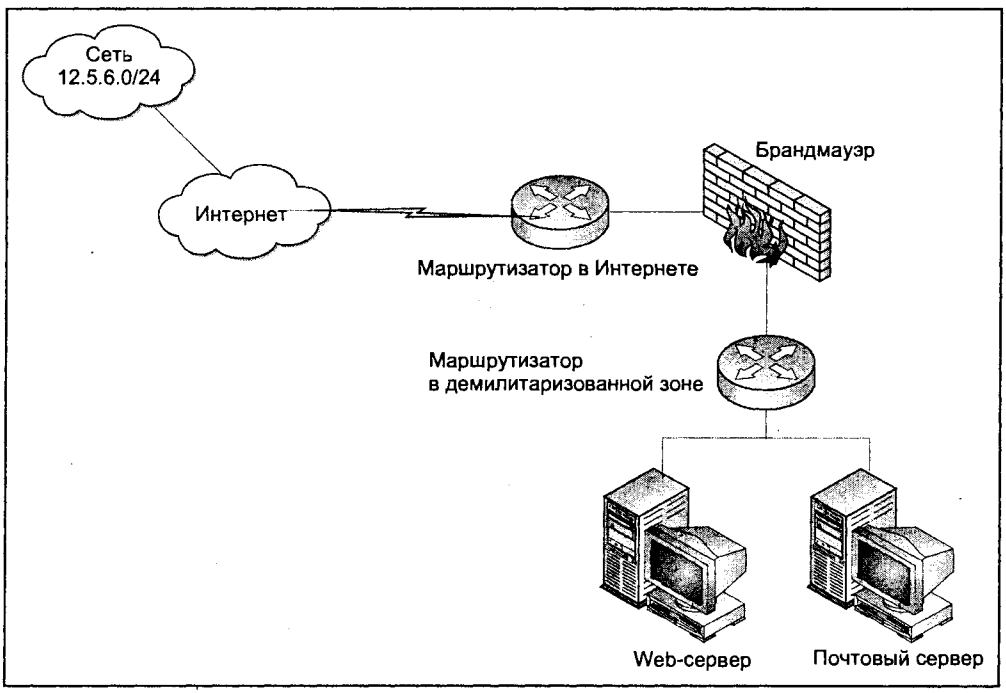


Рис. 15.2. Схема сети

Чтобы определить набор исходящих правил, поменяйте местами адреса и порты источника и назначения. К примеру, обратному трафику для нашего правила 2 соответствует адрес : порт источника 129.1.5.154 : 80 и адрес : порт назначения "любой": > 1023. Чтобы определять такое правило не приходилось, большинство фильтров пакетов располагают функцией разрешения прохода через интерфейс "установившихся" соединений. Для этого фильтр анализирует заголовок пакета TCP и определяет, является ли он частью действующего диалога. При этом он смотрит, очищен ли бит SYN TCP-заголовка. Учтите, что фильтр не отслеживает фактические соединения и при принятии решения основывается на состоянии этого бита. Развитием идеи фильтрации "установившихся" соединений являются фильтры пакетов с запоминанием состояния. Мы рассмотрим их далее в *разд. "Брандмауэры с запоминанием состояния пакетов"*.

Обратите внимание на то, что есть различные стратегии реализации фильтров пакетов; наиболее популярными среди специалистов по обеспечению защиты являются две следующих.

- Правила формулируются от самых частных к самым общим так, чтобы общее правило не перекрывало частное правило, противоречащее общему, но относящееся к его области действия.

- Правила упорядочиваются таким образом, чтобы наиболее часто используемые из них находились во главе списка. Это сделано для повышения эффективности: при нахождении полного соответствия устройство фильтрации прекращает обработку списка.

Преимущества и недостатки фильтрации пакетов

Определение точных правил фильтрации пакетов может стать очень сложной задачей. Если вы хотите использовать фильтр пакетов, вам следует оценить все преимущества и недостатки этого подхода. К преимуществам фильтров пакетов можно отнести следующее.

- Производительность. При использовании современных процессоров фильтрация производится на скорости, близкой к скорости передачи данных.
- Экономическая эффективность. Фильтры пакетов относительно недороги или вообще бесплатны. Они встроены в операционные системы большинства маршрутизаторов.
- Хороший способ управления трафиком. Простые фильтры пакетов можно использовать для отбрасывания нежелательного трафика на сетевых периметрах и между различными внутренними подсетями.
- Прозрачность. Фильтр пакетов не влияет на поведение пользователей.

Основные недостатки фильтров пакетов обуславливаются следующими факторами.

- Между надежными и ненадежными хостами допускаются прямые соединения.
- Фильтры пакетов плохо масштабируются. Когда наборы правил становятся громоздкими, предотвратить непредусмотренные сообщения становится очень трудно. Кроме того, из-за динамического характера некоторых протоколов для их нормального функционирования может потребоваться открытие большого количества портов. Наихудшим примером в этом смысле является FTP. Протокол FTP предполагает наличие входящих сообщений от сервера к клиенту, для того чтобы их передача стала возможной, фильтрам пакетов потребуется большое количество открытых портов.
- Фильтры пакетов подвержены несанкционированному доступу. Такие атаки обычно предполагают отсылку ложной информации в составе заголовков TCP/IP. Среди распространенных атак встречается использование ложных адресов источника и создание впечатления о том, что эти пакеты являются частью установившихся соединений.

Шлюзы прикладного уровня

Термин *шлюз прикладного уровня* имеет несколько значений. Он стал синонимом терминов бастионный (барьерный) хост, прокси-шлюз и прокси-сервер. Как упоминалось ранее, прокси-службы можно запустить либо непосредственно на брандмауэре, либо на отдельном сервере, работающем совместно с брандмауэром.

Шлюз прикладного уровня принимает решения о доступе на основе информации, содержащейся в пакете и относящейся ко всем семи уровням модели OSI. Из-за этого прикладные шлюзы иногда считаются "осведомленными о применении".

Степень защиты, которую обеспечивает прикладной шлюз, выше аналогичного показателя фильтра пакетов, но достигается это за счет потери прозрачности по отношению к службам, чьим агентом этот шлюз выступает. Прикладной шлюз зачастую играет роль посредника для приложений типа электронной почты, FTP, Telnet, HTTP и т. п. В частности, прикладной шлюз исполняет роль сервера по отношению к клиенту и роль клиента по отношению к настоящему серверу — фактически он обрабатывает запросы от имени пользователей, которых защищает.

То, что такой брандмауэр является осведомленным о применении, позволяет ему осуществлять дополнительную проверку сообщений, которую простой фильтр пакетов не предусматривает. Прикладной шлюз способен контролировать формат прикладных данных. Более того, он может выполнять дополнительную аутентификацию и регистрацию информации; он может осуществлять функции преобразования данных (если это необходимо и если он на это способен). К примеру, прикладной шлюз можно настроить так, чтобы он разрешал команду `GET` службы FTP, но запрещал ее команду `PUT`. Это может оказаться полезным, если вы хотите предоставить пользователям возможность загружать файлы на их компьютеры, но при этом обеспечить дополнительный уровень защиты против размещения файлов на FTP-сервере. В следующем разделе рассматривается процесс, применяемый прикладным шлюзом для представления внутренних пользовательских запросов Telnet.

Пример шлюза прикладного уровня

В нашем примере некая компания решает разместить Telnet-сервер, чтобы работающие в удаленном режиме администраторы могли выполнять определенные функции на хосте. При этом они объявляют шлюз Telnet, а не настоящее имя хоста сервера, скрывая его настоящее имя от ненадежных сетей. Процесс подключения к хосту осуществляется следующим образом:

1. Пользователь отсылает шлюзу прикладного уровня Telnet-запрос через порт 23. Это устройство фильтрации сверяет IP-адрес источника со списком допустимых источников. Если сообщения, отсылаемые с данного IP-адреса источника, разрешены, начинается следующий этап процесса соединения. В противном случае соединение разрывается.
2. Пользователь получает приглашение пройти аутентификацию. Дополнительно в процессе аутентификации пользователь может указать имя основного хоста.
3. Если аутентификация прошла успешно, пользователь получает в свое распоряжение командную строку или меню систем, к которым он может подключаться. Получить доступ к IP-адресам, которые им соответствуют, напрямую из сети Интернет невозможно — они принимают обращения исключительно через шлюз.
4. Пользователь выбирает систему, к которой желает подключиться. Этот выбор приводит к установлению нового TCP-соединения с хостом назначения, исходящего от шлюза прикладного уровня.
5. При необходимости пользователь приглашается к вводу дополнительной аутентификационной информации.

Примечание

Приложение типа proxy daemon — это усиленное приложение, которое еще в большей степени усложняет компрометацию и предусматривает единый источник обновления в случае обнаружения нового уязвимого места.

Недостатки шлюзов прикладного уровня

За уровень защиты, который обеспечивают шлюзы прикладного уровня, приходится платить. Ниже следует список общих недостатков, связанных с их применением.

- Ухудшение производительности. Каждый новый пользовательский запрос фактически предполагает открытие двух отдельных соединений: одного — между пользователем и шлюзом, и еще одного — между шлюзом и реальным хостом назначения. Для этого требуется удвоение количества соединений и объема обработки по сравнению с аналогичным показателем фильтра пакетов. Кроме того, дополнительные проверки на прикладном уровне также требуют большего количества случаев обработки и увеличения их продолжительности. Для современных потоковых приложений с высокой пропускной способностью (например, приложения видеоконференц-связи) задержка прокси-сервера является непозволительной роскошью.
- Нехватка прозрачности. Большинство прокси-серверов требуют изменений в поведении клиентов и/или пользователей. Временами клиентское программное обеспечение теряет возможность пользоваться прокси-серверами для установления своих соединений. Кроме того, прокси-серверы зависят от возможности помещения агента между конечным пользователем и реальным сервером.
- Необходимость в агентах для каждого приложения. Несмотря на то, что прокси-серверы для популярных служб широко распространены, найти агентов для более новых или реже используемых служб довольно сложно. В большинстве шлюзов прикладного уровня для передачи трафика через шлюз нужно использовать "контактного" агента, принимаемого по умолчанию, который, однако, не является осведомленным о применении и низводит шлюз до положения дорогостоящего фильтра пакетов.
- Ограничения осведомленности о применении. Шлюз должен быть способен различать безопасные функции приложения и его опасные функции. Если агент не может отличить одних от других или отбросить все нежелательное, не нарушая предполагаемые операции, степень его полезности значительно снижается.

Шлюзы канального уровня

Шлюзы канального уровня аналогичны шлюзам прикладного уровня, но они не являются осведомленными о применении. *Шлюз канального уровня* передает соединения TCP из надежной сети в ненадежную. Но прямого соединения между клиентом и сервером ни при каких обстоятельствах не происходит. Из-за того, что шлюз канального уровня не распознает прикладной протокол, он должен иметь данные о соединении. Эти данные предоставляются шлюзу клиентами, которые распознают прикладной протокол и настроены на его использование. Вообще, прикладные шлюзы используют модифицированные процедуры, а шлюзы уровня схем — модифицированных клиентов.

Основное преимущество шлюза канального уровня заключается в том, что он предоставляет службы для множества различных протоколов и может быть адаптирован в расчете на обслуживание еще большего количества передач. Впрочем, протоколы, требующие некоторой осведомленности о применении (например, протокол FTP, осуществляющий динамическую передачу данных портов), лучше приспособлены

к прикладным шлюзам, нежели к шлюзам канального уровня. Типичным примером шлюза канального уровня является агент SOCKS.

Примечание

SOCKS выходит за предметные рамки этой главы. Комплексное рассмотрение SOCKS содержится в документе RFC 1928.

Пример шлюза канального уровня

В нашем примере некая компания разрешает своим внутренним пользователям выходить в сеть Интернет. Но представители компании обеспокоены тем, следует ли допускать прямые соединения между пользователями и ненадежными Web-серверами в Интернете. Чтобы снизить риск, они решают использовать шлюз канального уровня, который предназначается для контроля над таким трафиком. Когда пользователь открывает Web-страницу, происходит следующее (как мы отмечали ранее, при использовании шлюзов канального уровня требуется специальная конфигурация или специализированное программное обеспечение). Этот процесс показан на рис. 15.3.

1. При открытии Web-страниц компьютер пользователя знает лишь о существовании сеанса между собой и шлюзом. Пользователь открывает браузер и пытается установить связь с URL-адресом назначения. Браузер специально настроен на использование прокси-сервера и отсылает запрос непосредственно на Web-сервер.
2. Прокси-сервер получает запрос пользователя, проверяет свои настройки, выясняя, разрешен ли обмен информацией, нужна ли для него аутентификация или же обмен информацией запрещен. Если аутентификация необходима, запускается соответствующий процесс. Если обмен информацией запрещен, шлюз обычно переадресует запрос на страницу "запрещено", на которой пользователю сообщается о том, что запрошенная информация ему предоставлена не будет.
3. После успешного завершения процесса аутентификации шлюз выполняет все дополнительные задачи типа сверки URL-адреса со списком разрешенных или запрещенных адресов.
4. Шлюз отправляет независимый запрос Web-серверу с целью извлечения информации.
5. После извлечения информации она предоставляется клиенту.

Примечание

Основным преимуществом HTTP-агентов, связанным с производительностью, является их способность кэшировать результаты пользовательских запросов. Вместо повторного извлечения данных Web-сайтов при очередном запросе пользователя HTTP-агент, один раз выполнив кэширование запроса, впоследствии обслуживает этот запрос с помощью кэша. В результате происходит экономия на пропускной способности, а производительность повышается благодаря тому, что пользовательские запросы могут быть выполнены локально, без обращения к сети Интернет.

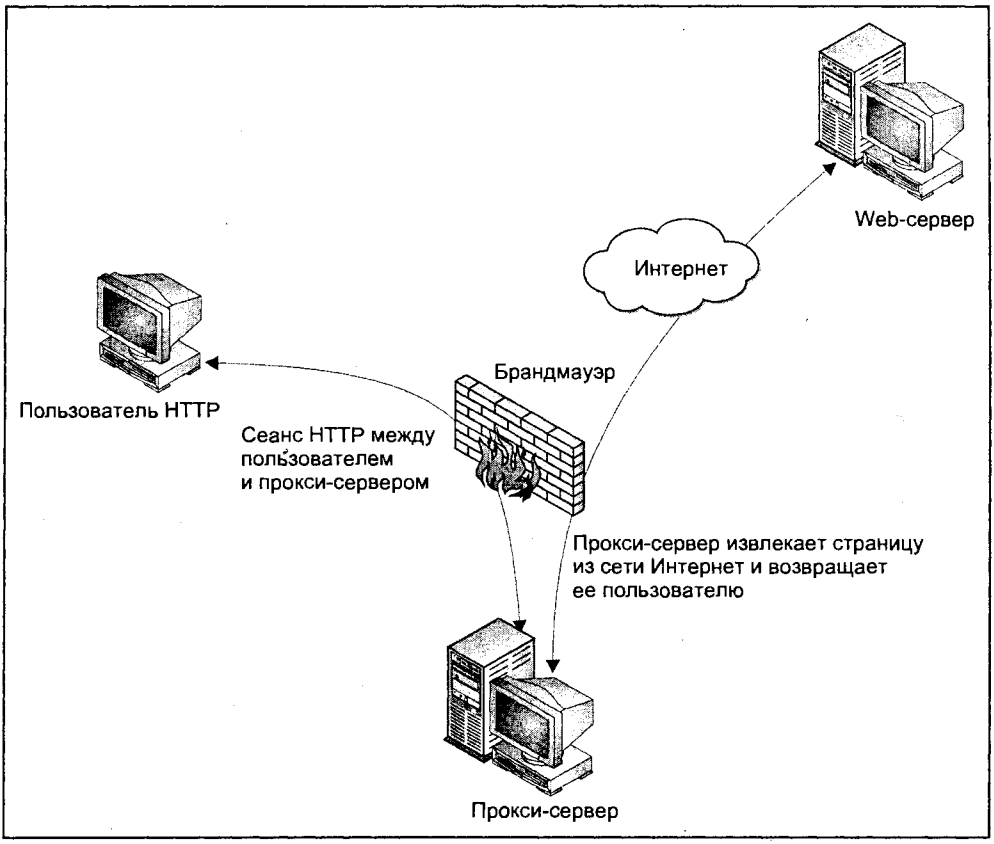


Рис. 15.3. Пользователь открывает Web-страницу через прокси-сервер

Недостатки шлюзов канального уровня

С применением шлюза канального уровня в качестве единственного средства защиты сети связано несколько недостатков. Некоторые из них приводятся ниже.

- Необходимы клиенты, которые могут использовать именно шлюзы канального уровня. Некоторые клиентские приложения нельзя модифицировать таким образом, чтобы они поддерживали шлюз канального уровня, что ограничивает их возможности по обращению к внешним ресурсам. Также использование приложений, поддерживающих шлюз канального уровня, связано со значительными расходами; в результате количество приложений, которые могут обращаться к внешним ресурсам, или область их применения уменьшаются.
- Шлюзы канального уровня не допускают контроль на прикладном уровне. Это позволяет приложениям использовать порты TCP, которые были открыты для выполнения других, легальных, задач. Некоторые одноранговые приложения можно настроить на работу на произвольных портах, таких как TCP 80 и TCP 443 (часто открывается для работы пользователя в сети Интернет). В резуль-

тате появляется возможность злоупотреблений и обнаруживаются слабые места, присутствующие в таких приложениях.

Брандмауэры с запоминанием состояния пакетов

Брандмауэр с запоминанием состояния пакетов (SPI, Stateful Packet Inspection) пропускает или запрещает пакеты, руководствуясь набором правил, очень схожим с правилами фильтрации пакетов. Когда брандмауэр осведомлен о состоянии, он принимает решения о доступе на основе не только IP-адресов и портов, но и SYN, ACK, порядковых номеров и других данных, содержащихся в заголовке TCP. Фильтры пакетов пропускают или запрещают отдельные пакеты; для осуществления двусторонних передач в них требуются правила разрешения, а брандмауэры с запоминанием состояния пакетов отслеживают состояние каждого сеанса и имеют возможность динамически открывать и закрывать порты в зависимости от требований отдельных сеансов.

Брандмауэры с запоминанием состояния пакетов сочетают в себе скорость и гибкость фильтров пакетов, с одной стороны, и безопасность прикладного уровня, обеспечиваемую прикладными агентами, с другой. Поэтому этот тип брандмауэра представляет собой компромисс между брандмауэром с фильтрацией пакетов и прикладным протоколом с осведомленностью о применении, но он уступает первому в быстродействии, а второму — в уровне защиты. При этом брандмауэр с запоминанием состояния пакетов очень эффективен при обеспечении безопасности сети.

Когда пакет поступает на брандмауэр, в механизме проверки происходит несколько действий.

1. Когда пакет поступает на брандмауэр, в первую очередь проверяется, является ли он частью существующего, установившегося потока информации. Брандмауэр с фильтрацией пакетов способен делать выводы о том, что пакет является (или не является) частью существующего диалога TCP, лишь на основе состояния бита SYN (он может быть установлен или очищен). Брандмауэр с запоминанием состояния пакетов с той же целью сравнивает характеристики пакета с таблицей существующих действительных соединений и определяет, есть ли между ними соответствие. На брандмауэре ведется таблица соединений, состоящая (как минимум) из IP-адресов источника и назначения, а также портов источника и назначения транспортного уровня. Отследить можно практически всю информацию, содержащуюся в заголовке пакета, включая порядковые номера TCP, которые и помогают брандмауэру определить пакет как часть действующего диалога.
2. Проверка пакета может продолжиться или прекратиться в зависимости от протокола. В некоторых распространенных протоколах, включая FTP и SMTP, есть несколько уязвимых мест, которые хорошо известны и часто используются. Производители брандмауэров добавили функции, расширяющие возможности этих устройств, связанные с защитой хостов от злоумышленников. Если брандмауэр имеет подобные функции, предназначенные для работы с тем протоколом, к которому относится пакет, он интерпретирует информационную часть пакета. Затем он, руководствуясь этими данными, принимает решение о перенаправлении.
3. Если в таблице соединений нет записи, соответствующей пакету, брандмауэр анализирует его на основе своего установленного набора правил. В большинстве брандмауэров с запоминанием состояния пакетов набор правил аналогичен пра-

вилам, используемым в фильтрах пакетов, и состоит из IP-адресов и портов источника, IP-адресов и портов назначения и протокола. Как упоминалось выше, набор правил фильтрации пакетов можно факультативно расширить, включив в него анализ данных.

4. Если на основе источника, пункта назначения, протокола и содержимого пакета пакет признан разрешенным, брандмауэр перенаправляет его в окончательный пункт назначения, а также создает или обновляет запись в таблице соединения, фиксируя диалог. Впоследствии эта запись соединения будет задействована в качестве метода проверки достоверности обратного пакета вместо определения специального правила.
5. Как правило, чтобы узнать, когда запись соединения следует удалить из таблицы соединения, брандмауэры пользуются таймерами и идентификацией пакета TCP, осуществляемой с помощью битов FIN или RST.

Преимущества и недостатки брандмауэра с запоминанием состояния пакетов

Технология запоминания состояния пакетов выгодно отличается от технологии фильтрации пакетов. Таблица соединений значительно снижает шансы спуфинга пакета, т. е. его представления как части действующего соединения. Так как брандмауэры с фильтрацией пакетов не фиксируют продолжающиеся сообщения, при выявлении участия пакета в ранее проверенном диалоге они вынуждены полагаться на формат этого пакета — в частности, на состояние бита SYN в пакете TCP. Следовательно, появляется возможность спуфинга пакетов TCP и отсутствует метод определения состояния пакетов UDP и ICMP. При наличии таблицы соединений брандмауэр получает намного большее количество информации, которой он может воспользоваться, решая, следует ли пропустить каждый отдельно взятый пакет.

Вторым преимуществом брандмауэров с запоминанием состояния пакетов по сравнению с фильтрами пакетов является их способность анализировать данные определенных типов пакетов. Эта функция оказалась очень ценной благодаря ряду хорошо известных и полностью документированных слабых общераспространенных протоколов. В качестве примера можно привести протокол FTP, применительно к которому проводится анализ команд для определения правильности направления их передачи. Принимая во внимание данные о порте TCP, брандмауэр получает возможность определять, на какой стороне диалога представлен клиент, а на какой — сервер. Затем брандмауэр ожидает отправки команд с обеих сторон и убеждается в том, что сервер не отсылает клиенту неверные команды, и наоборот.

Основным недостатком брандмауэра с запоминанием состояния пакетов является то, что он допускает прямые соединения между ненадежным и надежным хостами. Таким образом, надеяться следует не на усиленную прокси-службу, а на принимающий процесс.

Основы сетевой безопасности

Завершив обзор отдельных технологий брандмауэров, существующих в настоящее время, мы имеем полное право задаться вопросом: а зачем вообще нужен брандмауэр? Почему бы просто не усилить отдельные системы, чтобы они могли противосто-

ять атакам? Простейший ответ заключается в том, что брандмауэр предназначен для выполнения только одной задачи — классификации сообщений на санкционированные и несанкционированные. В результате отпадает необходимость в компромиссах между безопасностью, удобством использования и функциональностью.

Не будь брандмауэра, системы остались бы один на один со своими собственными устройствами организации защиты. Возможно, на этих системах работают службы, которые повышают функциональность или упрощают администрирование, но при этом они небезопасны, ненадежны или не всегда доступны. Брандмауэры используются как раз для того, чтобы реализовать этот уровень контроля доступа.

Если в конфигурации нет брандмауэра, обеспечение безопасности становится задачей хостов. Таким образом, защита зависит от возможностей самого слабого из хостов. Чем крупнее сеть, тем сложнее становится поддерживать все хосты на одинаково высоком уровне безопасности. Результатом допущенных недочетов (например, установки заплат в системы защиты 14 из 15 Web-серверов) могут стать случаи проникновения из-за простых ошибок, допущенных в конфигурации, или недостаточного обеспечения заплатами систем безопасности.

Брандмауэр выступает в качестве единственной точки соприкосновения с ненадежными сетями. Вместо того чтобы стараться обеспечить максимальную безопасность большого количества компьютеров, администраторы могут сосредоточиться на сопровождении одного брандмауэра. Это не отменяет необходимости повышения уровня защиты систем, обращение к которым осуществляется через брандмауэр; просто в данном случае формируется дополнительная степень защиты от ошибок.

Брандмауэры являются прекрасными средствами контроля. Так как через них проходит весь трафик, то и информация, содержащаяся в их журналах регистрации, может пригодиться при необходимости восстановления событий в случае появления бреши в системе защиты.

В общем, брандмауэры снижают риск использования систем для выполнения несанкционированных или непредусмотренных задач (например, хакерских атак). От каких именно рисков охраняют систему брандмауэры? В корпоративных системах и данных есть три основных параметра, сохранность которых обеспечивается брандмауэром.

- *Конфиденциальность.* Риск доступа к секретным данным лиц, не имеющих на это полномочий, или преждевременного разглашения этих данных. Предприятие может потерять миллионы долларов из-за разглашения своего бизнес-плана, коммерческой тайны или финансовой информации.
- *Целостность данных.* Риск несанкционированного изменения данных типа финансовой информации, технических характеристик изделий или цен товаров, выставленных на продажу на Web-сайте. Это связано с общими вопросами конфиденциальности, целостности и доступности. При использовании брандмауэров данный аспект подразумевает действия злонамеренных пользователей и/или манипулирование данными.
- *Доступность.* Доступность системы предполагает ее устойчивость и работоспособность по требованию пользователя (т. е. она должна функционировать тогда, когда к ней обращаются пользователи). Неработоспособные системы причиняют компаниям большие материальные убытки в виде потери рабочего времени и прибыли, и нематериальные — потерю доверия клиентов и плохую репутацию.

Распространенные типы атак

В предыдущей главе мы обсуждали причины, по которым частные лица и предприятия решаются на применение брандмауэров. Теперь вопрос в другом: как именно хакеры получают несанкционированный доступ в системы? Мотивы осуществления атак многочисленны: от "чтобы посмотреть, смогу ли" до применения скомпрометированных систем для атаки других систем, экономического шпионажа и даже деструктивных действий, предполагающих подрыв работоспособности и/или повреждение систем.

Существуют десятки различных способов получения незаконного доступа в системы. Ниже приводится краткий список наиболее распространенных атак.

- *Использование людских ресурсов.* Человек, планирующий атаку (инициатор атаки), обманом склоняет администратора или другого уполномоченного пользователя системы к разглашению его регистрационных данных или подробностей работы системы.
- *Ошибки в программах.* Атакующий использует программный дефект и заставляет приложение или службу запускать неразрешенные или непредусмотренные команды. Степень опасности таких атак повышается, если программа предоставляет дополнительные или административные полномочия. Подобные дефекты обычно являются причиной атак, связанных с переполнением буфера или с уязвимостью форматирующей строки.

Примечание

Информацию об атаках, связанных с переполнением буфера и форматирующей строкой, можно получить на сайтах: **http://www.insecure.org/stf/smashstack.txt**, **http://www.insecure.org/stf/mudge_buffer_overflow_tutorial.html**, **http://julianor.tripod.com/teso-fs1-1.pdf**.

- *Вирусы и/или троянские кони.* Инициатор атаки обманом заставляет легального пользователя запустить программу. Наиболее распространенным способом проведения такой атаки является маскировка программы под безобидное электронное письмо или включение ее в вирус. После запуска программа способна выполнять самые разнообразные действия, включая установку потайных программ, хищение файлов и/или полномочий и даже удаление файлов.
- *Неверная конфигурация системы.* Инициатор атаки может воспользоваться ошибками, допущенными при конфигурации системы, с помощью доступных служб и/или учетных записей. Очень часто допускаются ошибки, связанные с сохранением старых паролей в учетных записях, принимаемых по умолчанию (как на системном, так и на прикладном уровнях), а также с отсутствием ограничения доступа к прикладным программам администрирования или сохранение активного состояния посторонних или неиспользуемых служб.

Злоумышленники могут не только осуществлять попытки несанкционированного доступа к системам, но и стараться нарушить их работу. Это может нанести большой ущерб компаниям, если атаке подверглись важные для работы приложения. Такие атаки называются *отказом в обслуживании* (DoS, Denial of Service). Атака DoS предполагает лишение пользователя, сети или организации их ресурса или службы. Потеря обслуживания обычно связывается с невозможностью работы отдельной се-

тевой службы, такой как электронная почта или доступ к Интернету, или временной потерей всех сетевых подключений и служб.

Методы обеспечения безопасности

Обсуждение способов настройки и управления брандмауэрами выходит за тематические рамки этой главы (этой теме посвящено много книг), мы представим лишь ряд важных принципов, которые смогут повысить общий уровень защиты брандмауэра. Эти принципы применимы как к самому брандмауэру, так и к системам, которые он защищает. Отметим, что приведенные методы не являются взаимоисключающими, и при их совместном использовании они позволяют достичь высоких уровней безопасности.

Предоставьте вашему компьютеру возможность позаботиться о самом себе

За исключением некоторых очень редких ситуаций, настройки систем и приложений являются не самыми лучшими с точки зрения их безопасности. Также часто по умолчанию устанавливаются и активируются те службы, которые ухудшают функциональность системы или приложения. Поэтому лучше оставить в системе минимум служб и учетных записей, необходимых для ее нормального функционирования. Бесчисленные случаи проникновения обуславливаются именно компрометацией тех неиспользуемых служб или учетных записей, которые не требуются для обеспечения нормальной работы системы. Практика отключения ненужных служб и перенастройки других служб для достижения более высокого уровня защиты часто называется усилением хоста. Ниже представлен небольшой контрольный список, которого следует придерживаться при осуществлении усиления хоста.

1. Отключите все ненужные и лишние службы.
2. Удалите ненужные учетные записи и группы. Измените пароли и/или отключите прикладные и системные учетные записи, принятые по умолчанию. Отключите учетные записи, не требующие интерактивной регистрации.
3. Перенастройте оставшиеся службы с расчетом на повышение уровня безопасности.
4. Защитите абсолютно все административные функции.
5. Используйте устойчивые пароли. Так называются пароли, длина которых превышает семь символов и которые представляют собой сочетание букв в верхнем и нижнем регистрах, цифр и других буквенно-цифровых знаков.

Примечание

Институт SANS (**www.sans.org**) публикует руководства по "оптимальным методам" защиты операционных систем.

Заплаты! Заплаты! Заплаты!

Постоянная установка все большего и большего количества заплат, выпускаемых в настоящее время, — процесс, которому не уделяют достаточно внимания. Посто-

янно обнаруживаются все новые слабые места в системах. Система, которая только что была безопасной, через минуту может стать совершенно беззащитной. Для постоянной поддержки уровня защиты вашей системы следует подписаться на несколько почтовых рассылок о новых дефектах, а также на рассылки производителей о новом программном обеспечении. Популярные службы оповещения о слабых местах в системах защиты предоставляются следующими организациями:

- Internet Security Systems ведет базу данных и список рассылки xforce по адресу **http://www.iss.net/xforce**;
- SecurityFocus рассылает копию архива Bugtraq по адресу **http://www.securityfocus.com**;
- группа компьютерной "скорой помощи" (CERT, Computer Incident Emergency Response Team) на сайте **http://www.cert.org**;
- база данных распространенных слабых мест и дефектов (CVE, The Common Vulnerabilities and Exposures database) находится по адресу **http://www.cve.mitre.org**.

Примечание

После установки заплат убедитесь в том, что уровень защиты системы не понизился. К примеру, кластерные заплаты для Solaris компании Sun печально известны своим свойством реактивировать службы.

Устройства и операционные системы

Брандмауэры обычно устанавливаются поверх универсальных операционных систем типа Windows NT и UNIX. Они изменяют системное ядро и стек TCP/IP, чтобы сделать возможным мониторинг трафика. Следовательно, брандмауэры могут оказаться зависимыми от неполадок, характерных для той операционной системы, поверх которой они установлены. Чтобы достичь высокого уровня защиты, необходимо усиливать, латать и обслуживать операционную систему (об этом говорилось в предыдущем разделе). Эта задача может потребовать большого количества времени и сил, особенно в условиях недостатка опыта или времени на обеспечение защиты и поддержание полностью функциональной операционной системы. Некоторые производители предлагают альтернативу, реализуя брандмауэры в виде отдельных устройств.

В таких устройствах интегрированы операционная система и программное обеспечение брандмауэра, в результате чего получается полностью усиленная, специализированная защитная аппаратура. В процессе интеграции отбрасываются абсолютно все функции, не имеющие отношения к задачам фильтрации и ограждения пакетов. Кроме того, полностью функциональный интерфейс управления еще в большей степени упрощает задачи конфигурирования и обслуживания брандмауэра. При использовании аппаратных брандмауэров дополнительного усиления защиты не требуется (обычно достаточно просто изменить пароли, принятые по умолчанию). Вместо того чтобы перенастраивать и латать универсальную операционную систему, администраторы получают возможность сосредоточиться на разработке наборов правил. По сравнению с брандмауэрами на основе операционных систем аппаратные брандмауэры значительно сокращают эксплуатационные расходы и издержки, связанные с сопровождением. Среди популярных аппаратных брандмауэров следует отметить Cisco PIX, Netscreen, SonicWall и Check Point FireWall-1 на платформе Nokia IPSO.

Многоуровневая защита

Брандмауэр — это хорошее средство обеспечения безопасности, но полностью полагаться на него нельзя. Как отмечалось выше, брандмауэры не имеют возможности защищать от того, что санкционировано. Что произойдет, если злоумышленник сможет обойти брандмауэр? Рассмотрим ситуацию, в которой злоумышленник получает возможность средствами HTTP эксплуатировать Web-сервер, получая доступ к системе через оболочку. Брандмауэр разрешит прохождение такого трафика, т. к. обращения протокола HTTP к Web-серверу допускаются, и инициатор атаки сможет воспользоваться этим как каналом атаки других серверов и систем в данной сети, которые в таком случае остаются без защиты брандмауэра. Если эти системы не настроены на обеспечение безопасности, значит, ждать компрометации всей инфраструктуры осталось недолго.

При проектировании систем полезно использовать резервные средства контроля, которые могут ограничить или предотвратить повреждение системы в случае выхода из строя основных средств контроля. (Это все равно, что блокировать руль в машине при закрытых дверях.) Среди многоуровневых средств контроля необходимо выделить следующие.

- Усиление внутренних хостов, чтобы они могли противостоять атакам в случае выхода из строя брандмауэра или его обхода злоумышленником.
- Запуск служб в ограниченных средах (к примеру, с помощью команды `chroot` в UNIX) и с минимальными полномочиями, чтобы компрометация отдельной службы не приводила к немедленной компрометации целой системы.
- Использование нескольких брандмауэров от разных производителей или установка фильтров пакетов на сетевых маршрутизаторах. В результате уменьшается подверженность самого брандмауэра воздействию отдельных дефектов.
- Использование средств контроля людских ресурсов типа образования персонала, отслеживание данных журналов регистрации и предупреждения.
- Установка систем, способных автоматически обнаруживать и оповещать администраторов о несанкционированных или злонамеренных действиях. Они называются *системами обнаружения вторжений* (IDS, Intrusion Detection Systems).

Создание политики безопасности

Политика безопасности корпоративной информации рассматривает данные как имущество, которое нуждается в охране. Она определяет чувствительность организации к риску и возможные последствия возникновения бреши в системе защиты. Кроме того, политика безопасности устанавливает способы защиты данных; брандмауэр является реализацией такой политики.

Для небольших организаций, не имеющих обширной базы формализованных политик, очень важными задачами являются документирование назначения сети и применение брандмауэра для ограничения использования сети.

Политика безопасности предоставляет администраторам право отклонять множество запросов на обращение к брандмауэру, а такие запросы подаются постоянно. Без четкого определения того, что можно пропускать через брандмауэр, а что нельзя, его эффективность с течением времени уменьшается, т. к. разрешение распространяется на все большее количество служб.

Мониторинг и регистрация

Проникнуть можно в любую систему — для этого нужны лишь деньги и время. Но о попытках проникновения свидетельствуют улики в форме записей в журналах и т. п. Если за системами ведется постоянное наблюдение, вероятность обнаружения атаки значительно возрастает. Таким образом, чрезвычайно важным является мониторинг системной активности. Приложения должны регистрировать как успешные, так и неуспешные системные события. Расширенная регистрация и своевременный анализ журналов могут сообщить администраторам о подозрительной активности еще до возникновения серьезной бреши в системе защиты.

Примечание

Свидетельства испытаний и попыток атак могут быть разбросаны по разным журналам регистрации на множестве различных серверов. При обнаружении некоторых атак сведение воедино этих фрагментов информации может играть очень важную роль. Если временные метки этих записей в журналах на разных серверах различаются, коррелирование событий усложняется еще в большей степени. Чтобы системные часы на разных серверах оставались синхронизированными, рекомендуется пользоваться синхронизирующим сетевым протоколом (NTP, Network Time Protocol).

Проверка и тестирование

После настройки брандмауэра важно обеспечить соответствие запланированного уровня защиты фактическому, убедиться в отсутствии недочетов. Существует несколько бесплатных и коммерческих инструментальных средств, предназначенных для тестирования защиты брандмауэра и систем, находящихся под его защитой. Одним из лучших таких бесплатных средств является Nessus; загрузить его можно по адресу **www.nessus.org**.

Обнаружение вторжений и реагирование

Обнаружение вторжений — это процесс мониторинга сетевой и системной активности с целью выявления и предупреждения персонала о несанкционированных действиях. Реагирование на происшествия — это процесс, посредством которого организации отвечают на неисправности и аварии, включая обнаруженные вторжения. Комплексное рассмотрение обнаружения вторжений и реагирования на происшествия выходит за предметные рамки этой главы, но обозначить эту тему необходимо.

Системы обнаружения вторжений (IDS) отличаются от брандмауэров тем, что не проводят активного взаимодействия с сетевым трафиком (хотя некоторые из них способны предпринимать отдельные действия, руководствуясь настроенными аварийными сигналами). Системы IDS обеспечивают пассивный мониторинг ресурсов с целью обнаружения признаков злоумышленных действий, а при срабатывании аварийных сигналов оповещают об опасности соответствующий персонал. На сегодняшний день существует два основных типа IDS: сетевые и хостовые. Сетевые IDS следят за исключением из сети злоумышленных пакетов, а хостовые IDS обеспечивают мониторинг отдельных хостов на предмет несанкционированной деятельности.

Прежде чем устанавливать коммерческую IDS или аналогичную систему с открытым исходным кодом, организация должна составить план реагирования на происшест-

вия, призванный отвечать на вопрос: что делать с предполагаемыми атаками в рамках данной инфраструктуры. Хорошо продуманные и заранее запланированные способы реагирования на предполагаемые вторжения помогают предотвратить панику и дорогостоящие ошибки. Кроме того, создание и рецензирование процедур реагирования помогает выявить слабые места и недоработки в возможностях организации по обнаружению, реагированию и восстановлению, причем сделать это нужно до того, как станет слишком поздно. Конечной целью любого плана реагирования на происшествия является максимально оперативное и безболезненное возобновление нормального режима работы.

Первой трудностью на пути к эффективному реагированию на происшествия является обнаружение самого вторжения. Самой большой ошибкой в процессе использования системы IDS является неправильная настройка аварийных сигналов. Если система порождает слишком много ошибочных результатов анализа, люди прекращают реагировать на аварийные сигналы. (Вспомните сказку о мальчике, который кричал, что на него нападают волки!) С другой стороны, если аварийные сигналы системы не срабатывают во время настоящей атаки, эта система также бесполезна. Чтобы достичь равновесия между этими крайностями, потребуются многие часы работы и значительное мастерство.

Прежде чем устанавливать систему IDS, обязательно выполните усиление всех возможностей существующей инфраструктуры. Брандмауэры и серверы способны составлять журналы регистрации с большими объемами информации о проходящем через них трафике. При предварительных испытаниях и попытках взлома в этих журналах регистрации почти всегда фиксируются соответствующие свидетельства — это происходит еще до того, как инициатор атаки добьется успеха. Администраторам следует настроить свои системы в расчете на составление журналов регистрации в достаточных объемах, а затем своевременно проверять их содержимое.

Очередным этапом реагирования на происшествия после обнаружения бреши в системе защиты является оповещение. В зависимости от масштаба организации возможно обучение и содержание целой команды, ответственной за реагирование на происшествия. Для оповещения специального персонала о предполагаемом инциденте должен существовать понятный и простой механизм. При быстром реагировании нужно учитывать различие между малозначительным происшествием и серьезной брешью в системе защиты.

После оповещения специального персонала следует выполнить оценку. Непосредственной целью оценки должно быть определение положения дел и выявление действий, направленных на сдерживание и предотвращение последующего повреждения систем. Необходимо как можно быстрее ответить на два вопроса.

- Смог ли инициатор атаки проникнуть в ваши системы?
- Продолжается ли атака до сих пор?

Если атака в данный момент не находится в активном состоянии или не является очевидно успешной, то команда реагирования получает дополнительное время. Если атака успешна или находится в процессе осуществления, то решительные действия со стороны команды должны быть предприняты немедленно.

Конкретные действия обуславливаются конечными целями организации. Если она желает предъявить злоумышленнику иск, в планах реагирования должны предусмат-

риваться методы сохранения и сбора улик. Есть ряд юридических требований, которые нужно соблюсти, чтобы доказательства были приняты судом. Если организация не заинтересована в судебном преследовании, но ставит задачу восстановления, то отключение задействованных в атаке систем/сетевых соединений будет наиболее приемлемым ответным действием.

Примечание

Постарайтесь не ухудшить ситуацию — не регистрируйтесь и не давайте команды, особенно как администратор. Возможно, чтобы завершить атаку, злоумышленники только этого и ждут!

Решение о первоначальной реакции должно приниматься аварийной командой. Если команда полагает, что брешь в системе защиты не ограничится одним хостом, оптимальным выходом является отключение всех внешних соединений. В этом случае присутствует опасность отсоединения производственных систем (т. е. причинения еще большего ущерба, чем в случае продолжения атаки). Представьте, что произойдет, если Yahoo! или eBay будут отключаться при каждой обнаруженной атаке. Важнейшими факторами, обуславливающими принятие решения об оптимальном реагировании, являются качественное планирование и учет особенностей инфраструктуры. К примеру, неразумно отключать все сетевые соединения, если издержки от простоя предприятия составляют $100 000 в час, а предполагаемый ущерб от атаки — всего лишь $10 000.

После того, как команде реагирования удалось остановить первоначальную атаку, ей следует перейти в режим восстановления. Он может заключаться в передаче функций обработки резервным компьютерам, в проверке достаточности изоляции бреши в системе защиты, в восстановлении систем с помощью надежных резервных копий, в латании систем, оповещении специального персонала и т. п.

Примечание

Лучшим средством восстановления после вторжения является полное воссоздание неисправных систем с чистого листа или с надежной резервной магнитной ленты (созданной до проникновения, причем необязательно накануне атаки). Злоумышленники могут и будут устанавливать программы, в том числе потайные, чтобы закрепить за собой возможность доступа. К примеру, они могут заменить Telnet другой его версией, которая предусматривает соединение без предъявления паролей. Кроме того, они могут запускать троянских коней в распространенных бинарных файлах типа who и ps, чтобы их присутствие в системе оставалось незамеченным.

Последним и наиболее важным этапом является экспертиза. Необходимость ее проведения обуславливается множеством причин. Среди них есть и следующие.

- Оценка ущерба. Если атака потерпела неудачу, то значительного объема работ не потребуется. Впрочем, даже если атака оказалась неуспешной, организация может принять решение об усилении мониторинга — особенно если злоумышленник вел себя агрессивно и настойчиво.
- Выявление механизма вторжения.
- Проверка достаточности действий, предпринятых для закрытия бреши в системе защиты.

- Анализ источника возникновения бреши в системе защиты (т. е. неустановленная заплата, неверная настройка устройства, несанкционированное изменение настройки и т. д.).
- Если планируется судебное разбирательство, необходимо должным образом собрать, классифицировать и сохранить все доказательства.
- Наконец, необходимо выполнить анализ того, как организация обнаружила аварийную ситуацию и отреагировала на нее. Путем критического пересмотра реакции организация может усовершенствовать и наладить этот процесс.

Поиск и устранение неисправностей брандмауэров

В сбоях соединений в сети, как правило, виновен брандмауэр. Ниже приводится ряд предложений и советов, которые призваны помочь администраторам локализовать неисправности соединения и выяснять, действительно ли данная неисправность связана с брандмауэром.

Как отмечалось ранее, для обнаружения потенциальных брешей в системе защиты необходимо надлежащее ведение журналов регистрации. Они не менее полезны для выявления сбоев соединений в сети. Если пользователь не может установить соединение с определенным узлом с помощью определенной службы, в первую очередь следует проверить, регистрирует ли брандмауэр причины, по которым он отказывает в соединении.

Кроме того, полезно задаться несколькими вопросами, например: "Работало ли раньше то, что теперь остановилось?". Если раньше это действительно работало, администратору предстоит выяснить, что изменилось в конфигурации. Довольно часто виновниками "таинственного" прекращения работы являются изменения в маршрутизации сети и хостов, а также сбои в системе DNS.

Если все предположения несостоятельны, неоценимую помощь администратору окажут сетевые анализаторы пакетов. С помощью анализатора можно проследить прохождение пакетов по сети, чтобы выявить точную область локализации сбоя связности. Достигают ли брандмауэра пакеты, отправленные хостом? Фиксируются ли они в удаленной точке брандмауэра? Если пакеты не проходят через брандмауэр, проверьте свои наборы правил.

Симптомы неисправностей

Ниже приводится небольшой список возможных неисправностей, а также полезные советы по их устранению.

Симптом 15.1. Рабочая станция в локальной сети не может подключиться к сети Интернет

Практически во всех случаях причиной является неверная настройка свойств TCP/IP этой локальной рабочей станции. Проверьте правильность настройки маски подсети и шлюза по умолчанию рабочей станции. Попробуйте послать на ее шлюз

по умолчанию Ping-запрос. Кроме того, проверьте, могут ли другие рабочие станции, расположенные в той же подсети, получить доступ к Интернету. Если проблема не ограничивается одной рабочей станцией, в первую очередь проверьте правильность записей маршрутов в сетевых шлюзах и убедитесь в том, что такой доступ разрешен набором правил маршрутизатора.

Симптом 15.2. Сервер DMZ недоступен из сети Интернет

Причин может быть несколько. Убедитесь в правильности настройки маршрутизации и стека TCP/IP между всеми хостами и маршрутизаторами. При использовании трансляции сетевых адресов (NAT) следует проверить наличие записей трансляции и правильность записей в таблицах ARP. Как обычно, нужно убедиться в том, что набор правил брандмауэра разрешает подобные сообщения.

Симптом 15.3. Сбои при отправке электронной почты из локальной сети на почтовый сервер поставщика интернет-услуг

Для начала проверьте, чтобы поставщик услуг Интернета не установил фильтры, которые могли бы препятствовать применению его почтового сервера. После этого проверьте, допускает ли брандмауэр прохождение трафика SMTP через порт 25. Учтите, что загрузка почты с сервера происходит через различные порты (в IMAP — через порт 143, в POP3 — через порт 110). Кроме того, если вы отправляете почту посредством доменного имени, проверьте работоспособность системы DNS. Происходит ли отправка почты, если вы указываете IP-адрес? Если соединение через IP-адрес проходит успешно, а через доменное имя — нет, значит, скорее всего, проблема связана с DNS.

Симптом 15.4. Журнал регистрации брандмауэра сообщает о "переполнении диска"

Очевидно, эта неисправность связана с нехваткой пространства на диске. После высвобождения достаточного объема дискового пространства займитесь вопросами автоматического сжатия и архивирования регистрационных файлов. Лучше всего сохранять журналы регистрации на удаленном хосте — в таком случае переполнение диска не приведет к простою.

Симптом 15.5. Пароль администратора изменен или потерян

К сожалению, процедура восстановления пароля зависит от конкретного производителя. Чтобы узнать, существует ли возможность восстановления пароля, вам следует связаться с производителем. Впрочем, на случай, если когда-нибудь пароль нужно будет восстанавливать, лучше создавать резервные копии всех конфигурационных файлов. Кроме того, имеет смысл выяснить, как именно пароль был изменен, т. к. это может быть признаком сетевого вторжения.

Симптом 15.6. Выясняется, что соединения "auth"[1] блокируются

Если возможность соединения с определенной службой отсутствует, проверьте набор правил брандмауэра, чтобы узнать, разрешен ли ее трафик. Если он запрещен, следует обновить набор правил.

---

[1] "auth" — сокращение от "authentic" (подлинный). — *Ред.*

Симптом 15.7. Одна из подсетей не может подключиться к сети Интернет через брандмауэр

Для начала следует проверить таблицы маршрутов сети и брандмауэра. Если выяснится, что с маршрутизацией все в порядке и другие сети не испытывают трудностей при подключении к сети Интернет, проверьте набор правил — возможно, он запрещает доступ в Интернет для данной подсети.

Дополнительные ресурсы

Firewalls: The Complete Reference, Strassberg, Gondek, Rollie, et al., Osborne McGraw-Hill, 2002.

Check Point: **http://www.checkpoint.com**.

Cisco: **http://www.cisco.com/go/pix**.

NetScreen: **http://www.netscreen.com**.

SonicWALL: **http://www.sonicwall.com**.

Netfilter: **http://www.iptables.org/**.

Squid Web Proxy Cache: **http://www.squid-cache.org**.

SecurityFocus: **http://www.securityfocus.com**.

NTSecurity.com: **http://www.ntsecurity.com.**

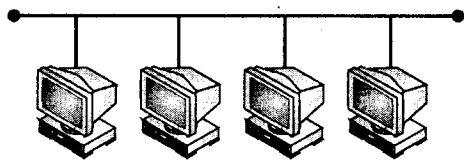
Координационный центр группы компьютерной "скорой помощи" (CERT) в Университете Carnegie Mellon: **http://www.cert.org**.

Internet Security Systems: **http://www.iss.net**.

Snort — сетевая система обнаружения вторжений с открытым исходным кодом: **http://www.snort.org**.

Руководство по защите узлов от Сетевой Рабочей Группы: **http://www.ietf.org/rfc/rfc2196.txt**.

Материалы по входящей фильтрации в сетях от Сетевой Рабочей Группы: **http://www.ietf.org/rfc/rfc2827.txt**.



ГЛАВА 16

Серверы печати

В перечень оборудования, с которым приходится иметь дело сетевым администраторам, входят и принтеры. Часто бывает, что отдельные принтеры получают недостаточную нагрузку, а наличие большого количества различных моделей принтеров в сети может иногда существенно осложнять работу технических специалистов. При включении принтеров в сеть администраторы получают возможность достичь более высокой загруженности меньшего количества принтеров; при этом деятельность, связанная с печатью, централизуется в рамках рабочей группы или отдела. Чем меньше принтеров, которые требуют технической поддержки, тем меньше комплектующих и расходных материалов должна иметь в запасе служба сопровождения и тем меньше количество обновлений драйверов и случаев модернизации принтеров. Совместное использование принтеров осуществляется через устройство под названием *сервер печати*. Для традиционных серверов печати требовалось обслуживание компьютера, подключенного к сети (к которому принтер подключался через порт LPT), но во все большем количестве сетей применяются специализированные серверы печати типа Netgear PS110 (рис. 16.1). В этой главе мы рассмотрим процессы установки, настройки, тестирования и поиска неисправностей серверов печати в нескольких популярных операционных системах.

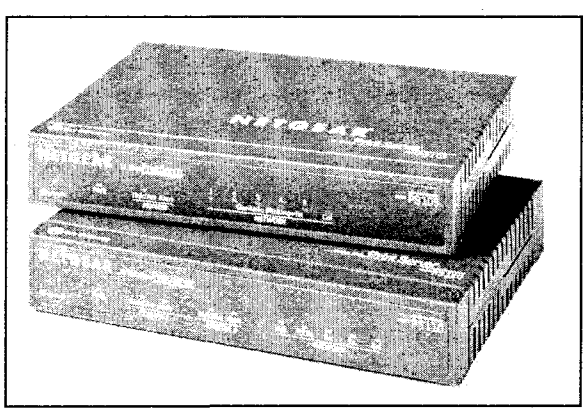


Рис. 16.1. Сервер печати Netgear PS110 поддерживает в сети Ethernet до двух принтеров, подключенных к параллельным портам (публикуется с разрешения Netgear)

Возможности сетевой печати

Традиционный сервер печати представлял собой стандартную систему с подключенным к ней принтером. Этого было достаточно для поддержки операционной системы, драйверов принтера и файлов буферизации. Серверы печати часто обслуживались компьютерами модели 486 (и даже 386). Затем этот компьютер подключался к сети, ему направлялись запросы на печать, а он, в свою очередь, передавал эти задания подключенному через параллельный порт принтеру. Трудность заключалось в том, что система часто замедляла работу из-за заданий печати и не могла решать другие задачи.

Сегодня серверы печати на базе ПК уступают место специализированным серверам печати (см. рис. 16.1). Специализированные серверы подключаются непосредственно к сети. Они дешевле персональных компьютеров и обеспечивают подключение от двух до пяти принтеров, которые при этом находятся в одном месте (таким образом, службы печати в рамках отдела централизованы). Специализированный сервер печати обычно управляется с другого компьютера сети с помощью комплекта программ, которые способны обращаться к его настройкам и контролировать его конфигурацию. Наиболее мощные серверы печати поддерживают множество сетевых протоколов типа IPX/SPX (NetWare), TCP/IP (lpr/lpd в Windows или UNIX), NetBEUI (Windows) и AppleTalk.

Еще одним вариантом организации сетевой печати являются принтеры, "готовые к работе в сети" и располагающие собственным сетевым адаптером. Как и любая другая рабочая станция, они могут подключаться напрямую к коммутатору или концентратору. Подобные сетевые принтеры обычно дороже принтеров, подключаемых через параллельный порт или USB, но они могут находиться практически в любой точке сети (кроме того, обычно они проектируются с расчетом на более высокий среднемесячный уровень использования). Управление сетевыми принтерами производится через Web-программы (т. е. можно обратиться к IP-адресу нужного принтера в Web-браузере, например, http://10.0.0.12).

Специализированные серверы печати

Специализированные серверы печати предусматривают разнообразные функции и возможности, которые смогут удовлетворить ваши запросы, однако, определяясь с выбором конкретной модели, необходимо принимать во внимание следующие характеристики.

- *Поддержка сети.* Сервер печати должен быть совместим с архитектурой вашей сети (например, 100BaseT).
- *Поддержка протоколов.* Сервер печати должен соответствовать применяемому сетевому протоколу (например, TCP/IP).
- *Порты.* Сервер печати может предусматривать от одного до пяти принтерных портов (а иногда и больше). Выбирайте сервер, соответствующий вашим запросам в этом отношении. В целях увеличения скорости и улучшения совместимости с принтерами IEEE 1284 следует отдавать предпочтение двунаправленным принтерным портам.

К примеру, трехпортовый сервер печати Linksys EtherFast 10/100 содержит двунаправленные принтерные порты, способные одновременно обрабатывать множество заданий на печать. Кроме того, он совместим с полудуплексной и дуплексной работой в сети. Буфер объемом 256 Кбайт помогает разгружать трафик печати, а 512-килобайтовая микросхема с микропрограммными средствами допускает флэш-обновления. Другим популярным сервером печати является JetDirect от компании Hewlett-Packard.

Назначение светодиодов

На серверах печати часто имеется комплект светодиодов, помогающих выявить активность и состояние данного устройства в рамках сети. Состав этого комплекта зависит от конкретной модели сервера, наиболее распространенные светодиоды перечислены ниже.

- *Питание.* При включенном питании светодиод питания сигнализирует зеленым светом.
- *Связь.* Светодиод связи сигнализирует зеленым светом, если между сервером печати и сетью через связной порт сервера успешно установлено соединение.
- *Состояние.* Светодиод состояния сигнализирует зеленым светом, когда при загрузке сервера на нем проводится самодиагностика. После успешного завершения этого тестирования светодиод должен гаснуть. Если он продолжает сигнализировать, возможно, вам предстоит поиск неисправностей или его замена.
- *Ошибки.* Светодиод ошибки сигнализирует красным светом при возникновении неисправности на сервере печати, а также в случае, когда на этот сервер записывается информация. При назначении серверу IP-адреса светодиод ошибки должен сигнализировать в течение нескольких секунд.
- *LPTx.* Возможно наличие светодиодов активности для каждого принтерного порта.

Если на специализированном сервере печати есть коммутационные порты, на нем также могут присутствовать дополнительные светодиоды.

- *Связь/активность.* Этот светодиод непрерывно сигнализирует зеленым светом в случае успешного подключения сервера к устройству через соответствующий порт. Прерывистая сигнализация красным светом означает, что сервер печати активно отсылает или принимает данные через этот порт.
- *Дуплексный режим/коллизии.* Этот светодиод непрерывно сигнализирует зеленым светом в случае успешного установления дуплексного соединения через данный порт. Если он не сигнализирует, значит, данные передаются в полудуплексном режиме. Когда зеленый светодиод мигает, соединение сопровождается коллизиями (редкие коллизии не являются отклонением от нормы). Если на коммутаторе возникает слишком много коллизий, проверьте надежность свивания и монтажа кабеля. Если данный светодиод мигает слишком часто, может потребоваться поиск неисправностей или выравнивание сетевой нагрузки.
- *100.* Светодиод 100 сйгнализирует оранжевым светом, если через данный порт успешно установлено соединение на скорости 100 Мбит/с. Если светодиод 100 не сигнализирует, скорость передачи данных соответствует 10 Мбит/с.

Настройки

Возможно, базовые настройки вашего сервера печати определяются с помощью нескольких DIP-переключателей. Расположение и количество таких переключателей зависит от модели сервера, но есть и несколько распространенных вариантов.

- *Автосогласование.* Этот переключатель отвечает за режим автосогласования, который позволяет серверу автоматически определять скорость (10 или 100 Мбит/с), полярность и двусторонность сетевого кабеля. Когда этот переключатель находится в отключенном положении, устройство не выполняет автоматического определения скоростей.
- *Скорость.* Этот переключатель контролирует скорость сервера (т. е. 10 или 100 Мбит/с). К примеру, если установить переключатель в отключенное положение, передача данных будет осуществляться на скорости 100 Мбит/с, а во включенном положении скорость уменьшится до 10 Мбит/с.
- *Двусторонность.* Этот переключатель отвечает за дуплексный режим передачи данных. Когда переключатель установлен во включенное положение, передача данных производится в полудуплексном режиме. В отключенном положении передача данных осуществляется в дуплексном режиме.

Общие принципы установки оборудования

Установка специализированных серверов печати не представляет большой сложности, но к ней нужно подготовиться. Сервер печати использует адаптер переменного тока и способен обеспечивать работу нескольких принтеров, так что как для самого сервера, так и принтеров вам понадобится подходящая розетка переменного тока. Прежде чем приступать к установке, вы должны выяснить имя по умолчанию и адрес узла своего сервера. Как правило, эта информация есть на наклейке, расположенной на задней или нижней плоскости устройства. Найти эту наклейку лучше сразу, т. к. после полной установки сервера сделать это будет сложнее. Запишите имя устройства по умолчанию (например, SC483081). Эти данные понадобятся при установке драйверов. Кроме того, зафиксируйте адрес узла принтера (например, 00C002123456), т. е. физический адрес устройства (он же — MAC-адрес).

Примечание

Представленное здесь руководство может служить лишь в качестве общих справочных данных. Для получения конкретных инструкций всегда следует обращаться к руководству производителя.

На большинстве серверов печати нет переключателя питания — сервер находится во включенном состоянии при условии подключения его адаптера к источнику питания. К счастью, сервер печати можно активировать до, во время или после включения питания вашей сети. Для этого нужно лишь присоединить адаптер к разъему питания сервера (он находится на задней панели устройства), а затем подключить его к стенной розетке. При этом светодиод питания сервера должен начать сигнализировать зеленым светом. Проведите кабель Cat 5 UTP от разъема RJ-45 сервера печати к стандартному порту коммутатора или концентратора.

Выключите питание принтеров и подключите их к соответствующим параллельным портам сервера печати. При использовании принтеров IEEE 1284 необходимы высо-

кокачественные экранированные кабели для параллельных портов, обеспечивающие высокоскоростную двунаправленную передачу данных. После подключения принтеров их можно включить. Теперь на сервере можно устанавливать программные драйверы и/или административное программное обеспечение. Почти во всех случаях эти программы нужно установить только один раз на компьютере администратора.

Конфигурирование и применение серверов печати

Так как сервер печати является сетевым устройством, после его установки и подключения всех принтеров он становится доступен для всех сетевых станций. В определенных случаях может возникнуть необходимость в установке драйверов сервера на каждой рабочей станции, которая предполагает к нему обращаться. Большинство серверов печати — это полностью функциональные сетевые устройства, не требующие наличия драйверов (более подробные инструкции должны содержаться в руководстве по эксплуатации вашего сервера). Почти все серверы печати пользуются тем или иным управляющим программным обеспечением (например, PS Admin для сервера D-Link и Bi-Admin для устройства от Linksys), которое позволяет администратору обращаться к конфигурации сервера и вносить в нее изменения.

Установка административного программного обеспечения

Административное программное обеспечение должно быть установлено на рабочей станции администратора. Если выясняется, что данная платформа управления не соответствует техническим требованиям к системе, взамен можно воспользоваться сетевым теледоступом (Telnet). К примеру, программа PS Admin связывается с сервером печати D-Link средствами протокола IPX, так что для ее работы должны быть установлены сетевой протокол IPX и клиентские службы Novell NetWare. Ниже приведены этапы установки типичного административного программного обеспечения.

1. Вставьте дискету 1 установки программы во флоппи-дисковод вашей системы (A: или B:).
2. В среде Windows 3.1x или Windows NT 3.51 следует последовательно выбрать **Program Manager** (Диспетчер программ), **File** (Файл), **Run** (Выполнить). В операционных системах Windows 9x/Windows NT 4.x (или более поздних версиях) необходимо выбрать **Run** (Выполнить) в меню **Start** (Пуск) в Панели задач. При появлении диалогового окна укажите путь к программе Setup на носителе флоппи-дисковода (например, a:\setup) и нажмите кнопку **OK**.
3. Работа программы Setup начнется с копирования некоторых файлов и запроса на подтверждение. Чтобы продолжить, нажмите кнопку **Next** (Следующий).
4. Затем программа Setup попросит вас выбрать на жестком диске каталог, в который вы предполагаете установить административную программу. Если вы не согласны с путем к каталогу назначения, предложенным по умолчанию, нажмите кнопку **Browse** (Просмотр) и выберите другой каталог. Чтобы продолжить процесс установки, нажмите кнопку **Next** (Следующий).

5. Программа Setup скопирует программные файлы в выбранный каталог и создаст соответствующую программную группу. Чтобы завершить процесс установки, нажмите кнопку **Finish** (Готово).
6. После завершения установки вы можете пользоваться этим программным обеспечением.

Первоначальная настройка

Прежде чем вы сможете приступить к сетевой печати с сервера, вам, возможно, придется выполнить несколько элементарных задач, связанных с настройкой. При возникновении неисправностей сервера печати будет нелишне проверить эти базовые настройки. Как правило, от вас требуется:

- выбрать имя сервера печати;
- установить пароль для защиты настроек сервера от несанкционированных изменений;
- выбрать имена для отдельных принтерных портов сервера и выбрать соответствующие настройки портов;
- протестировать работу сервера и убедиться в надежности его подключения;
- после завершения работы над этими задачами вы можете переходить к сетевой печати в сетях Novell NetWare, Microsoft Networks и AppleTalk, а также в системах UNIX TCP/IP.

Выбор имени

У каждого сервера печати в сети должно быть имя. При производстве сервера печати ему присваивается имя по умолчанию (например, SC483081), где цифры зачастую соответствуют последним шести цифрам Ethernet-адреса (обычно он указывается на наклейке, на нижней плоскости сервера). Имя по умолчанию можно оставить, но можно выбрать и другое; при этом следует учитывать, что:

- длина серверного имени ограничена 15 символами;
- серверное имя не должно соответствовать имени какого-либо файлового сервера в той же сети;
- серверное имя не должно соответствовать именам других серверов печати, присутствующих в сети и настроенных в ее условиях;
- серверное имя не должно соответствовать имени какого-либо клиента или сервера.

Примечание

Между символами в верхнем и нижнем регистрах, составляющими имя сервера печати, различия не проводится.

Большинство производителей рекомендуют ограничивать длину имени сетевого сервера 15 символами — включая буквы от A до Z, цифры от 0 до 9 и знак дефиса. В некоторых сетях имена, отклоняющиеся от этих рекомендаций, могут не действовать. Как правило, изменение имени сервера печати осуществляется следующим образом:

1. В главном окне программы PS Admin выберите на экране имен серверов (или на расширенном экране серверов) нужный сервер.
2. Выберите **Server Device** (Устройства сервера) в меню **Configuration** (Настройка) или нажмите кнопку **Configure Server** (Настроить сервер) на панели инструментов. (Если вы уже определили для данного сервера пароль, введите его.) Программа PS Admin выведет окно **Configuration — Server Device**.
3. В поле **Server Name** (Имя сервера) введите выбранное имя сервера и нажмите кнопку **OK**.
4. Выберите **Save Configuration** (Сохранить настройки) в меню **Configuration** (Настройка) или нажмите кнопку **Save Configuration** (Сохранить настройки) на панели инструментов. В результате новые настройки сервера будут сохранены, а сам он будет перезапущен. Теперь обращения к серверу печати будут производиться с помощью нового имени.

Выбор пароля

Если не установить пароль, изменить настройки сервера печати сможет любой участник сети. Если ваша локальная сеть подключена к сети Интернет, то изменение настройки вашего сервера печати может быть выполнено из любой точки земного шара посредством интерфейса Telnet. Чтобы обеспечить сохранность сервера, для него нужно выбрать пароль и хранить его в безопасном месте. Чтобы установить пароль сервера печати, необходимо выполнить следующие действия.

1. В главном окне программы PS Admin выберите на экране имен серверов (или на расширенном экране серверов) нужный сервер печати.
2. Выберите **Server Device** (Устройства сервера) в меню **Configuration** (Настройка) или нажмите кнопку **Configure Server** (Настроить сервер) на панели инструментов. (Если вы уже определили для данного сервера пароль, введите его.) Программа PS Admin выведет окно **Configuration — Server Device**.
3. В поле **Password** (Пароль) введите выбранный пароль сервера и нажмите кнопку **OK**.
4. Программа попросит вас подтвердить новый пароль. Его нужно будет ввести еще раз, а затем нажать кнопку **OK**.
5. Выберите **Save Configuration** (Сохранить настройки) в меню **Configuration** (Настройка) или нажмите кнопку **Save Configuration** (Сохранить настройки) на панели инструментов. В результате произойдет сохранение новых настроек сервера и его перезапуск.

Примечание

Не забывайте и не теряйте пароли серверов. В крайнем случае, вам придется связаться с представителем службы D-Link и с его помощью поменять пароль.

Изменение настроек портов

На сервере печати можно отрегулировать отдельные принтерные порты, чтобы тем самым добиться оптимальной производительности. К примеру, в большинстве случаев вы можете настроить следующие характеристики каждого порта:

- ❒ имя порта;
- ❒ комментарий с описанием порта;
- ❒ скорость параллельного порта;
- ❒ поддержка параллельным портом протокола PJL (Printer Job Language, язык заданий принтера) компании HP;
- ❒ скорость последовательного порта (скорость двоичной передачи);
- ❒ количество битов данных последовательного порта;
- ❒ количество стоповых битов последовательного порта;
- ❒ четность последовательного порта (четный/нечетный);
- ❒ программное управление потоком для последовательного порта (XON/XOFF);
- ❒ аппаратное управление потоком для последовательного порта (DTR/RTS).

Ниже приводится типичная последовательность действий для задания параметров принтерного порта.

1. В главном окне программы PS Admin выберите на экране имен серверов (или на расширенном экране серверов) нужный сервер печати.
2. Выберите **Server Device** (Устройства сервера) в меню **Configuration** (Настройка) или нажмите кнопку **Configure Server** (Настроить сервер) на панели инструментов. (Если вы уже определили для данного сервера пароль, введите его.) Программа PS Admin выведет окно **Configuration — Server Device**.
3. Нажмите кнопку, соответствующую тому порту, в настройки которого вы хотите внести изменения. Ниже перечислены параметры параллельного порта, которые можно изменить.

   - *Имя порта.* Это имя, посредством которого данный порт обозначается в сетевых системах. Длина имени порта не должна превышать 32 символа; имя может состоять из букв, цифр и символов тире. Пробелы не допускаются. Если данный порт будет применяться клиентами LAN Manager, то длина его имени не должна превышать восьми символов.
   - *Описание.* Комментарий с описанием порта.
   - *Скорость.* Указывает на то, будет ли сервер печати отправлять данные принтеру на высокой скорости. Большинство новых принтеров допускает высокоскоростную передачу данных. Если ваш принтер теряет символы, вам, вероятно, следует переключиться в низкоскоростной режим.
   - *Принтер PJL.* Определяет принятие или непринятие принтером команд языка управления заданиями принтера. PJL позволяет пользователям получать данные о состоянии принтера. Если принтер подключен к порту, который предусматривает поддержку PJL, то в качестве значения этого поля следует установить **Yes**.

   Что касается последовательного порта, вы можете изменить следующие его параметры.

   - *Имя порта.* Это имя, посредством которого данный порт обозначается в сетевых системах. Длина имени порта не должна превышать 32 символа; имя может состоять из букв, цифр и символов тире. Пробелы не допускаются. Если

данный порт будет применяться клиентами LAN Manager, то длина его имени не должна превышать восемь символов.

- *Описание.* Комментарий с описанием порта.
- *Скорость двоичной передачи.* Устанавливает скорость передачи битов при последовательном обмене (бит/с). По умолчанию в большинстве принтеров принимается значение 9600 бит/с, но зачастую возможны скорости от 300 до 115 200 бит/с.
- *Биты данных.* Устанавливает количество битов (на байт), передаваемых через последовательный порт. В большинстве современных принтеров применяются 8-битные данные.
- *Стоповые биты.* Устанавливает количество стоповых битов (на байт), передаваемых через последовательный порт. В большинстве современных принтеров применяется последовательный протокол с одним стоповым битом.
- *Четность.* Определяет тип контрольного бита четности, отсылаемого с каждым байтом через последовательный порт. В большинстве современных принтеров используется последовательный протокол без контроля по четности.
- *Программное управление потоком.* Определяет, должен ли сервер реагировать на запросы программного управления потоком, исходящие от принтера. При использовании программного управления потоком переполнение буфера принтера обозначается отсылкой серверу символа XOFF (<Ctrl>+<S>), а по окончании периода переполнения буфера ему отсылается символ XON (XON).
- *Аппаратное управление потоком.* Определяет, должен ли сервер реагировать на запросы аппаратного управления потоком, исходящие от принтера. При использовании аппаратного управления потоком принтер контролирует передачу данных сервером с помощью линии управления DTR (Data Terminal Ready — сигнал готовности терминала к передаче данных) или RTS (Request To Send — готовность к передаче), или обеих — это делается для того, чтобы предотвратить переполнение буферов принтера.

4. После выполнения необходимых изменений нажмите кнопку **OK**, чтобы возвратиться к диалоговому окну **Port Settings** (Настройки портов).
5. Чтобы выйти из диалогового окна **Server Device** (Устройства сервера), нажмите кнопку **OK**.
6. Выберите **Save Configuration** (Сохранить настройки) в меню **Configuration** (Настройка) или нажмите кнопку **Save Configuration** (Сохранить настройки) на панели инструментов. В результате произойдет сохранение новых настроек сервера печати и его перезапуск.

Тестирование сервера печати

После настройки всех необходимых параметров и подключения к серверу печати всех принтеров вам следует протестировать каждый принтерный порт — это делается с помощью функции Print Test. В отношении каждого порта, который вы хотите проверить, необходимо выполнить описанные ниже действия.

1. В главном окне программы PS Admin выберите на экране имен серверов (или на расширенном экране серверов) нужный сервер.

2. Выберите **Print Test** (Тест принтера) в меню **Tools** (Инструменты). Программа пригласит вас указать порт, который следует протестировать.
3. Выберите нужный порт и нажмите кнопку **OK**. После этого сервер должен выполнить контрольную распечатку.
4. Повторите эту процедуру для каждого принтерного порта с подключенным к нему принтером.

Печать в среде Novell NetWare

Многие современные серверы печати поддерживают как серверную базу данных Bindery, применяемую в сетях NetWare 3.x, так и общесетевую базу данных NDS (NetWare Directory Services — служба каталогов NetWare), которая используется в сетях NetWare 4.x/5.x. В этой части главы рассматриваются способы применения сетевого сервера печати в среде NDS.

Служба каталогов NetWare (NDS)

В NetWare версии 3.x информация о пользователях, томах файлового сервера, серверах печати, очередях печати и других объектах хранится в базе данных под названием Bindery. Программы администрирования сервера NetWare (такие как SYSCON, PCONSOLE и др.) управляют работой файлового сервера путем внесения изменений в записи этой базы. Основным недостатком базы данных Bindery является то, что она ограничена одним сервером. Управлять сетями, в которых установлено несколько серверов, становится сложнее, т. к. каждый из них приходится настраивать отдельно. В масштабах крупного предприятия это может привести к дезорганизации, потому что каждый отдел будет администрировать свой собственный сервер NetWare, и у каждого это будет получаться по-разному. Таким образом, координация и администрирование файловых серверов в рамках целого предприятия предельно усложняется (если не становится невозможной).

По этой причине в NetWare версии 4.x была представлена база данных NDS (NetWare Directory Services — служба каталогов NetWare), допускающая администрирование как в глобальном, так и в локальном масштабе. NDS систематизирует объекты не по файловым серверам, а по административным доменам. В базе данных NDS объекты хранятся в виде древовидной структуры. Ветви этого дерева представляют региональные офисы, подразделения, отделы и т. д. Объекты (пользователи, серверы, серверные тома, серверы печати, очереди печати) могут помещаться в любую точку древовидной структуры, которая используется совместно всеми серверами. Изменение настройки в рамках этого дерева оказывает воздействие на все серверы, в результате чего важность индивидуального управления серверами уменьшается. В целях совместимости с существующими клиентами и серверами NetWare 3.x в NetWare 4.x/5.x есть эмуляция Bindery, которая в контексте сервера представляет объекты как принадлежащие к Bindery.

Конфигурирование NetWare 5.x

Чтобы активировать аппаратный сервер печати в качестве сервера печати NetWare NDS, для начала вам потребуется создать несколько объектов NDS. Это можно

сделать с помощью программы PCONSOLE или NWADMIN на базе DOS или NWADMN32 NetWare 5.x Administrator на базе Windows. В нашем примере используется NWADMN32, и при необходимости выполнения настройки с помощью PCONSOLE или NWADMIN вы должны будете обратиться к документации по системе NetWare. В первую очередь для каждого сервера печати в рамках сети следует определить уникальное и постоянное имя; после этого, чтобы настроить сервер печати на работу в режиме Pserver для печати в среде NetWare 5.x, вам предстоит выполнить следующие действия.

Примечание

Помните, что вам, возможно, придется установить программу конфигурирования сервера от его производителя.

1. В среде Windows 9x (с Client32) запустите программу NWADMN32 из системного тома (к примеру, F:\public\win32) на файловом сервере.
2. Зарегистрируйтесь в сети NDS как администратор (Admin) или как пользователь с администраторскими полномочиями доступа. Обратите внимание на дерево NDS и контекстное имя NDS, появившееся на экране — впоследствии, при настройке сервера печати, эта информация вам понадобится.
3. Обратитесь к опции **Quick Setup** (Быстрая установка) файлового сервера.
4. Выберите контекст, в который предполагается добавить новые объекты сервера, принтера печати и очереди печати.
5. Выберите в строке меню программы NWADMN32 пункт **Tools** (Сервис).
6. Выберите **Print Services Quick Setup** (Быстрая установка сервера печати) (не NDPS).
7. Введите имя сервера печати в поле **Print Server Name** (Имя сервера печати) (производители часто рекомендуют пользоваться именами по умолчанию).
8. Введите имя нужного принтера в поле **Name** (Имя) (в секции **Printer** окна **Quick Setup**).
9. Выберите **Parallel** (Параллельный) в поле **Type** (Тип).
10. Выберите **Text** (Текст) в поле **Banner**.
11. Введите имя нужной очереди в поле **Name** (в секции **Print Queue** окна **Quick Setup**).
12. Выберите серверный том **NetWare File** в поле **Volume**.
13. Теперь, сохранив изменения, запустите утилиту **Administration** сервера печати. При работе с сервером печати Netgear следует выбрать **Netgear Print Server Administration** с помощью пиктограммы **FirstGear for Print Server** на рабочем столе.
14. Выберите пункт **Print Server** (Сервер печати) в списке **Active Print Server** (Активный сервер печати).
15. Выберите **NetWare Pserver** (Сервер печати сети NetWare).
16. Щелкните по пиктограмме **Advanced** (Расширенные).

17. Выберите **NetWare Pserver**.
18. Нажмите **Print Server Mode** (Режим сервера печати).
19. Выберите **NDS Tree Name** (Имя дерева NDS).
20. Введите **Context Name** (Контекстное имя).
21. Нажмите кнопку **Save to Device** (Сохранить для устройства).

Примечание

За дополнительной информацией о настройке серверов печати, принтеров и очередей печати обращайтесь к документации по системе NetWare.

Настройка удаленных принтеров

Ваш сетевой сервер печати можно настроить как удаленный принтер NetWare 4.x/5.x. Это позволяет немного упростить администрирование, но может привести к увеличению задержек при печати. Нижеследующие инструкции призваны помочь вам настроить удаленный принтерный порт.

1. Зарегистрируйтесь на сервере NetWare как администратор (Admin) или под другой учетной записью с аналогичными полномочиями.
2. Проверьте, задействован ли на сервере протокол NetWare. Эта настройка расположена в окне **Configuration — Server Device**; чтобы обратиться к ней, следует указать нужный сервер печати, а затем выбрать **Server Device** (Устройства сервера) в окне **Configuration** (Настройка).
3. На вашем файловом сервере NetWare сервер печати NetWare должен быть уже создан, и он должен находиться в рабочем состоянии. О том, как это сделать, можно узнать из документации по системе NetWare.
4. Откройте программу администрирования сервера печати и выберите в меню **Configuration** (Настройка) пункт **NetWare Protocol** (Протокол сети NetWare) (или нажмите кнопку **Configure NetWare** на панели инструментов). Перейдите на вкладку **Remote Printer** (Удаленный принтер).
5. Нажмите кнопку, соответствующую номеру порта, который вы предполагаете использовать для обеспечения услуг удаленного принтера.
6. Щелкните на выбранном элементе **NDS Remote Printer**. Программа администрирования сервера печати выведет на экран древовидную структуру содержимого NetWare NDS, доступного из вашей сети.
7. Введите имя элемента, которым предполагаете пользоваться, а также имя сервера печати в этом контексте.
8. Определите, какие номера принтеров на данном сервере печати свободны, и введите неиспользуемый номер принтера в поле **Printer Number**. Номера принтеров находятся в диапазоне от 0 до 15.
9. Нажмите кнопку **OK**, затем выберите в меню **Configuration** (Настройка) пункт **Save Configuration** (Сохранить настройки) (или нажмите кнопку **Save Configuration** на панели инструментов) — тем самым вы сохраните изменения настроек сервера печати. После этого произойдет автоматическая перезагрузка сервера, и

он начнет выполнять функции удаленного принтера для указанного сервера печати.

Печать с клиентских компьютеров сети

После настройки сервера печати на печать с файлового сервера рабочие станции клиентов сети получают возможность подключаться к очереди печати этого файлового сервера. Детали этого процесса обуславливаются операционными системами, которые применяют клиенты.

Клиенты Windows 9x

Windows 9x обеспечивает прямую поддержку доступа NDS лишь в том случае, если вы пользуетесь 32-битным запросчиком NetWare от Novell. Обращаться к очередям принтеров в среде NetWare 4.x можно с помощью эмуляции Bindery.

Клиенты Windows NT 4.0

Рабочая станция с операционной системой Windows NT 4.0 (или более поздней версией) может вставать в очередь печати NetWare посредством перечисленных шагов.

1. Выберите последовательно **Start** (Пуск), **Settings** (Настройки), **Printers** (Принтеры). Windows выведет на экран каталог **Printers**.
2. Дважды щелкните по пиктограмме **Add Printer** (Добавить принтер) в каталоге **Printers**. Windows запустит мастер Add Printer Wizard.
3. Выберите **Network Printer** (Сетевой принтер) и для продолжения нажмите кнопку **Next** (Следующий).
4. В программе просмотра найдите очередь печати, к которой вы планируете присоединиться, и нажмите кнопку **OK**. Элементы содержимого NetWare NDS указываются под элементом **NetWare or Compatible Network**.
5. Windows выведет сообщение — чтобы продолжить, нажмите кнопку **OK**.
6. Мастер Add Printer Wizard пригласит вас выбрать подходящий драйвер принтера, а также может попросить вставить установочный диск Windows NT для того, чтобы найти файлы драйвера.
7. По завершении установки мастер Add Printer Wizard выведет еще одно сообщение. Чтобы завершить инсталляцию принтера, нажмите кнопку **Finish**.

Печать в сетях Microsoft

Вплоть до появления Windows 2000 службы Microsoft Networking базировались на протоколе NetBEUI, который предоставляет пользователям сети службы одноранговой сети. Кроме обращения к файлам и принтерам, расположенным на центральном сервере, каждая рабочая станция имеет возможность делиться своими каталогами файлов и принтерными портами, делая их доступными для других рабочих станций. Большинство серверов печати способны делать подключенные принтеры доступными для рабочих станций Microsoft Networking, работающих на базе сетевых операци-

онных систем типа Windows 9x/NT/2000, LAN Manager и IBM LAN Server. Кроме того, в целях повышения эффективности печати, клиенты служб Microsoft Networking могут поставлять задания в очередь печати на сервере Windows NT, который впоследствии перенаправляет эти задания на сервер печати. В этой части главы рассматриваются общие методики настройки и применения серверов печати в операционной системе Windows.

Конфигурирование Windows

Для того чтобы клиенты Microsoft Networking (работа в сетях Microsoft) могли пользоваться сервером печати, нужно провести небольшую настройку. В первую очередь необходимо пометить флажок NetBEUI в окне **Configuration — Server Device**. Чтобы вывести это окно на экран, укажите нужный сервер печати и выберите в меню **Configuration** (Настройка) пункт **Server Device** (Устройства сервера). Укажите имя рабочей группы и максимальное количество допустимых подключений. Эти настройки производятся в диалоговом окне **Configuration — NetBEUI**, которое открывается путем выбора пункта **NetBEUI Protocol** (Протокол NetBEUI) в меню **Configuration** (Настройка).

Каждая рабочая станция или сервер Microsoft Networking располагает именем рабочей группы. Это имя определяет те серверы и ресурсы, которые по умолчанию будут присутствовать в списках доступных ресурсов. Серверу печати нужно назначить то имя рабочей группы, которым располагают пользователи, предполагающие обращаться к нему чаще всего. Сетевые имена путей для принтеров в системах Microsoft Networking имеют форму

```
\\имя компьютера\имя принтера
```

При использовании сервера печати в среде Microsoft Networking параметр **Server Name** (устанавливается в окне **Configuration — Server Device**) определяет путь к компьютеру, а **Port Name** (устанавливается в окне **Configuration — Parallel Port** или **Configuration — Serial Port**) указывает на имя принтера. К примеру, путь к принтеру, подключенному к порту с именем DJ-660C на сервере PS-142634, определяется как

```
\\PS-142634\DJ-660C
```

Использование очереди печати Windows NT

Клиентские рабочие станции способны напрямую подключаться к сетевому серверу печати, но память этого сервера ограничена, и довольно часто при обращении клиенту приходится ждать завершения больших заданий печати (вместо того, чтобы позволить серверу печати образовать очередь на все задания). Чтобы уменьшить для клиентов время ожидания, вы можете разместить очередь на сервере Windows. В среде Windows NT это делается следующим образом:

1. Сделайте сетевой принтер доступным с сервера NT — для этого, как указано в *разд. "Клиенты Windows NT 4.0"* ранее в этой главе, следует воспользоваться мастером Add Printer Wizard.
2. Правой кнопкой мыши щелкните по подключенному к сети принтеру в окне **Printers** и выберите пункт **Sharing** (Доступ).

3. Включите совместное использование и определите совместное имя (**Sharing Name**) данного принтера.
4. Это не является обязательным, но вы можете выбрать версию (версии) операционных систем, драйвер принтера для которой будет храниться на сервере. Здесь вам понадобятся дистрибутивы этих версий операционных систем.
5. Нажмите кнопку **OK**. Теперь принтер будет доступен другим пользователям сети через сервер Windows NT — при этом будет использоваться дополнительная память, имеющаяся на этом сервере.

Печать с клиентских компьютеров

После настройки сервера на печать в сети Microsoft рабочие станции клиентов вашей сети получают возможность подключаться к очереди печати на файловом сервере. Детали этого процесса зависят от операционной системы, которая применяется каждым из клиентов.

Клиенты Windows 9x

Считайте данные действия руководством по настройке рабочей станции с операционной системой Windows 9x (или с более поздней ее версией) на печать в сети Microsoft непосредственно через сетевой сервер печати.

1. Последовательно выберите **Start** (Пуск), **Settings** (Настройка), **Printers** (Принтеры). Windows выведет на экран каталог **Printers**.
2. Дважды щелкните по пиктограмме **Add Printer** (Добавить принтер) в каталоге **Printers**. Windows запустит мастер Add Printer Wizard. Чтобы перейти к следующему экрану, нажмите кнопку **Next** (Следующий).
3. Выберите **Network Printer** (Сетевой принтер) и для продолжения нажмите кнопку **Next** (Следующий).
4. Введите сетевой путь к серверу печати, указывая, к какому порту вы предполагаете подключиться. К примеру, чтобы воспользоваться принтером, подключенным к порту под именем PS-142634-P2 на сервере печати PS-142634, введите (рис. 16.2):

   ```
   \\PS-142634\PS-142634-P2
   ```

   В качестве альтернативы вводу сетевого пути вы можете нажать на кнопку **Browse** (Просмотр), чтобы найти сервер печати и принтер. Для продолжения нажмите кнопку **Next** (Следующий).
5. На этом этапе Windows пригласит вас выбрать соответствующий принтеру драйвер. Выберите из списка производителя и модель вашего принтера или воспользуйтесь сопровождающей принтер дискетой с драйвером. Выбрав нужный принтер, нажмите кнопку **Next** (Следующий).
6. Windows запросит имя принтера. Введите это имя (или согласитесь с принятым по умолчанию). Затем, чтобы завершить процесс инсталляции, нажмите кнопку **Finish** (Готово).

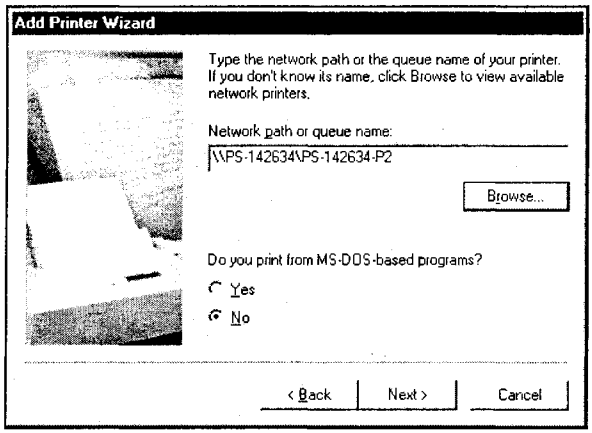


Рис. 16.2. Мастер Add Printer Wizard позволяет ввести путь к принтеру, включающий имя сервера печати

Клиенты Windows NT 4.0

Рабочая станция на базе операционной системы Windows NT 4.0 (или более поздней версии) может напрямую посылать запросы на сервер печати через сеть Microsoft; для того чтобы реализовать эту возможность, следует выполнить действия, подобные приведенным ниже.

1. Последовательно выберите **Start** (Пуск), **Settings** (Настройка), **Printers** (Принтеры). Windows выведет на экран каталог **Printers**.
2. Дважды щелкните по пиктограмме **Add Printer** (Добавить принтер) в каталоге **Printers**. Windows запустит мастер Add Printer Wizard.
3. Выберите **Network Printer** (Сетевой принтер) и для продолжения нажмите кнопку **Next** (Следующий).
4. Введите сетевой путь к серверу, указывая, к какому порту вы предполагаете подключиться. К примеру, чтобы воспользоваться принтером, подключенным к порту под именем PS-142634-P2 на сервере печати PS-142634, введите (рис. 16.2):

   ```
   \\PS-142634\PS-142634-P2
   ```

   В качестве альтернативы вводу сетевого пути вы можете самостоятельно найти в пределах сети сервер печати и принтер. Для продолжения нажмите кнопку **Next**.
5. Windows выведет сообщение. Чтобы продолжить, нажмите кнопку **OK**.
6. На этом этапе Windows пригласит вас выбрать соответствующий принтеру драйвер. Выберите из списка производителя и модель вашего принтера или воспользуйтесь сопровождающей принтер дискетой с драйвером. Выбрав нужный принтер, нажмите кнопку **Next** (Следующий).
7. Если принтер по умолчанию уже существует, Windows спросит, не желаете ли вы использовать только что установленный принтер как новое устройство по умолчанию.

8. После окончания установки Windows выведет еще одно сообщение. Чтобы завершить процесс инсталляции, нажмите кнопку **Finish** (Готово).

Печать в среде UNIX TCP/IP

Некоторые серверы печати (например, D-Link) обеспечивают печать с помощью сетевого протокола печати lpr/lpd (line printer — строкопечатающее устройство, line printer daemon — "демон" линейного принтера). Системы UNIX, как правило, поддерживают lpd. В этой части главы содержатся комментарии к применению административного программного обеспечения сервера печати для конфигурирования этого устройства в расчете на печать TCP/IP, а также методика настройки рабочих станций UNIX на печать через сервер печати. В тех сетях TCP/IP, в которых рабочие станции на базе Windows отсутствуют, для конфигурации сервера печати вы, как правило, можете воспользоваться интерфейсом Telnet этого устройства.

Задание настроек TCP/IP

Чтобы обычный сервер печати мог работать в среде UNIX, его необходимо настроить на разрешение печати на основе TCP/IP, а также на управление средствами SNMP и Telnet. Один из вариантов процедуры, направленной на решение этих задач, приведен ниже.

1. Запустите административное программное обеспечение сервера печати и убедитесь в том, что стек TCP/IP включен. Необходимо пометить флажок TCP/IP в окне **Configuration — Server Device**. Чтобы открыть это окно, определите нужный сервер печати и выберите **Server Device** (Устройства сервера) в меню **Configuration** (Настройка).
2. В меню **Configuration** выберите **TCP/IP Protocol** (Протокол TCP/IP).
3. Настройте IP-адрес сервера, его маску подсети в локальной сети, а также шлюз по умолчанию.
4. Нажмите кнопку **OK**, а затем, чтобы привести изменения в действие, выберите в меню **Configuration** (Настройка) пункт **Save Configuration** (Сохранить настройки) (или нажмите кнопку **Save Configuration** на панели инструментов). После этого сервер печати выполнит автоматическую перезагрузку и будет готов к печати на основе протокола lpd, а также к управлению с помощью протокола Telnet и к централизованному сетевому управлению на основе SNMP.

Основы управления посредством SNMP

Простой протокол сетевого управления (Simple Network Management Protocol, SNMP) стал стандартом управления крупными сетями при участии централизованных консолей управления. Некоторые сетевые серверы печати (например, D-Link) поддерживают базу управляющей информации SNMP (Management Information Base; распространено обозначение MIB-II), которая занимается сбором статистических данных, касающихся основных сетевых операций TCP/IP и Ethernet сервера печати. В SNMP (версии 1) была реализована элементарная форма обеспечения защиты, подразумевавшая указание группового имени (community name — имя сообщества)

в каждом поступающем запросе. Групповое имя представляет собой случайную строку символов, применяемую как пароль для управления доступом к концентратору. Если концентратор получает запрос с групповым именем, узнать которое ему не удается, он запускает аутентификационную "ловушку". Сетевые серверы печати типа D-Link предусматривают возможность задания до трех различных групповых имен, причем права доступа для каждой группы могут быть установлены отдельно и разрешают *только чтение* или *чтение/запись*. Эти имена вам придется координировать с настройками групповых имен, которые применяются в вашей системе сетевого управления. Чтобы определить групповые имена для сервера печати, запустите его программу администрирования и оцените следующие шаги.

1. Выберите в меню **Configuration** (Настройка) пункт **TCP/IP Protocol** (Протокол TCP/IP).
2. Чтобы открыть окно **SNMP Configuration** (Настройка SNMP), нажмите кнопку **SNMP**.
3. По необходимости добавляйте групповые имена и определяйте для каждого из них уровни доступа.
4. Чтобы выйти из окна **SNMP Configuration**, нажмите кнопку **OK**.

В некоторых случаях, например, при включении сервера печати или при подаче запроса SNMP с использованием неизвестного группового имени сервер печати отсылает станциям сетевого управления "ловушки" SNMP (сообщение авторизованному диспетчеру SNMP о запросе со стороны неавторизованного диспетчера). Сервер печати предусматривает маршрутизацию этих "ловушек" максимум на три различных хоста сетевого управления. Чтобы активировать "ловушки" в сервере печати, необходимо запустить его программу администрирования и выполнить следующие действия.

1. Выберите в меню **Configuration** (Настройка) пункт **TCP/IP Protocol** (Протокол TCP/IP).
2. Чтобы открыть окно **Trap Configuration** (Настройка "ловушек"), нажмите кнопку **Trap** ("Ловушка").
3. Чтобы разрешить отправку "ловушек" SNMP, установите флажок **SNMP Trap**.
4. Определите IP-адреса и групповые имена каждого получателя "ловушек".
5. Чтобы после внесения всех изменений выйти из диалогового окна **Trap Configuration**, нажмите кнопку **OK**.

Печать текста в среде UNIX

Текстовые файлы в системах UNIX содержат строки, завершающиеся символами "разделителей" — в противоположность операционным системам DOS и Windows, в которых строка завершается возвратом каретки, за которой следует символ новой строки. Большинство принтеров требуют наличия в конце каждой строки пары "возврат каретки/перевод строки", в результате чего возникает необходимость некоего преобразования, которое в отношении большинства принтеров должно выполняться до распечатки текстовых файлов UNIX. Для этой цели вы можете определить два принтера на один и тот же принтерный порт: первый будет печатать на сам порт, а второй — печатать на имя порта с добавленным к нему окончанием _TEXT. Файлы,

распечатка которых происходит через второй порт, будут преобразовываться таким образом, чтобы принтер получал необходимую пару "возврат каретки/перевод строки". К примеру, вы можете определить принтер hp51, который будет печатать в порт PS-142634-P1, и принтер hp51t, который будет печатать в порт PS-142634-P1_TEXT. Таким образом, графические файлы можно печатать на принтере hp51, а текстовые файлы — на принтере hp51t.

Печать в среде BSD UNIX

Что касается версий UNIX, связанных с выпусками BSD (Berkeley Software Distribution — программное изделие Калифорнийского университета) или производных от них (например, SunOS 4.x, Linux, BSD/OS, FreeBSD или NetBSD), для того, чтобы пользователи могли осуществлять печать на принтере, подключенном к серверу печати, вы можете выполнить следующее.

1. Зарегистрируйтесь под именем **superuser** (корневая учетная запись).
2. Добавьте в файл хоста /etc/hosts запись сервера печати, указав имя хоста, соответствующее IP-адресу этого сервера. Строка в файле /etc/hosts содержит IP-адрес, а также один или несколько псевдонимов хоста. В качестве примера можно привести следующую запись: 202.39.74.40 ps-142634 ps-142634.dlink.com.tw. При использовании протокола DNS в базу данных DNS можно добавить адресную запись, соответствующую серверу печати.
3. Создайте для принтера каталог буферизации. В системах SunOS в этой роли должен выступать подкаталог каталога /var/spool, причем его имя должно соответствовать имени принтера. В системах Linux следует создать подкаталог каталога /usr/spool/lp. В системах BSD/OS, FreeBSD или NetBSD нужно создать подкаталог каталога /var/spool.
4. Измените принадлежность и полномочия каталога таким образом, чтобы он мог перезаписываться; для этого нужно ввести следующие команды:

```
chown bin.daemon /var/spool/hp51
chmod 775 /var/spool/hp51
```

5. Добавьте запись данного принтера в каталог /etc/printcap; она должна выглядеть примерно так:

```
hp51:\
:lp=:sd=/var/spool/hp51:mx#0:\
:rm=ps-142634:rp=PS-142634-P1;
```

6. Путь к каталогу, указанный в записи каталога буферизации sd, должен соответствовать имени каталога, который вы недавно создали. Если запись занимает несколько строк, избежать разделителя строк вы можете с помощью обратной косой черты. Значения каждой записи приводятся ниже:
   - `lp=`. Запись `lp` указывает на локальное устройство печати. Так как принтер является удаленным устройством, эта запись должна быть пустой.
   - `sd=`*каталог*. Местонахождение локального каталога буферизации данного принтера.

- mx#блоки. Ограничение по количеству файлов заданий на печать в локальном каталоге буферизации; 0 означает отсутствие предела.
- rm=адрес. Хост, на котором расположен удаленный принтер. В нашем случае таким хостом является сервер печати D-Link.
- rp=принтер. Имя принтера на удаленном хосте. В случае с сервером печати D-Link следует указать имя порта (чувствительно к регистру).

7. Дайте команду запуска управления буферизацией для данного принтера (после этого принтером можно будет пользоваться):

```
lpc start hp51
```

8. Хотя это и не обязательно, но вы можете ввести еще одну запись printcap (и дать еще одну команду lpc start) для другого принтера — используя порт port_TEXT. Имя второго принтера можно активировать для распечатки текстовых файлов. Записи в /etc/printcap начинаются с имени принтера или списка имен, разделенных вертикальных чертой ("|").

Печать в среде Windows NT

Версии Windows NT, начиная с 3.51, обеспечивают поддержку печати через протокол lpd. Чтобы выполнить распечатку через сетевой сервер печати (такой как D-Link) с рабочей станции или сервера Windows NT 4.0, сделайте следующее.

1. Проверьте, установлен ли протокол TCP/IP и служба Microsoft TCP/IP Printing. При необходимости их можно установить с панели управления **Network** (Сеть).
2. Последовательно выберите **Start** (Пуск), **Settings** (Настройка), **Printers** (Принтеры). Windows откроет каталог **Printers**.
3. Дважды щелкните по пиктограмме **Add Printer** (Добавить принтер) в каталоге **Printers**. Windows откроет мастер Add Printer Wizard.
4. Выберите элемент **My Computer** (Мой компьютер), чтобы продолжить, нажмите кнопку **Next** (Следующий).
5. Чтобы добавить сервер печати lpd в перечень портов, нажмите кнопку **Add Port** (Добавить порт).
6. Выберите тип порта **LPR** и нажмите кнопку **New Port** (Новый порт).
7. Введите IP-адрес сетевого сервера печати, а также имя порта принтера, который вы хотите активировать.
8. Чтобы вернуться к окну **Printer Ports**, нажмите кнопку **OK**, а затем, для возврата к мастеру Add Printer Wizard, нажмите кнопку **Close** (Закрыть).
9. Чтобы продолжить процесс установки принтера, нажмите кнопку **Next** (Следующий) и следуйте инструкциям на экране. Мастер Add Printer Wizard попросит вас выбрать для принтера подходящий драйвер, а также присвоить этому принтеру имя. По окончании установки принтера вы получите возможность использовать по отношению к нему все обычные команды печати.

Основы администрирования Telnet

Большинство серверов печати поставляются в комплекте с управляющим программным обеспечением (таким как Bi-Admin для Linksys или PS Admin для D-Link). Этих программ более чем достаточно для проверки состояния устройства и внесения изменений в конфигурацию сервера печати. Тем не менее в некоторых случаях управляющей программы может не оказаться в наличии; кроме того, ваша административная платформа может не соответствовать требованиям этой программы. В подобных ситуациях у вас, скорее всего, будет возможность получить доступ к серверу печати и управлять им средствами Telnet. В этой части главы рассматриваются примеры процедур ручной конфигурации с помощью общепринятых сетевых средств.

Настройка IP-адреса

Программа администрирования (например, PS Admin) позволяет вам определять IP-адрес (и другие параметры TCP/IP) сервера печати. Если у вас нет рабочей станции на базе Windows, но при этом вы должны установить адрес сервера печати, вы можете воспользоваться либо сервером BOOTP (Bootstrap Protocol — протокол начальной загрузки, сетевой протокол, определяющий процедуры взаимодействия с узлами, не имеющими жестких дисков), либо ручным методом, описанным ниже. Для того чтобы решить задачу с помощью BOOTP, в вашей локальной сети Ethernet должен присутствовать BOOTP-сервер: В таблице этого сервера должна быть запись с указанием Ethernet-адресов (MAC-адресов) сервера печати, IP-адреса, который вы хотите этому серверу присвоить, сетевой маски и адреса шлюза по умолчанию (маршрутизатора). Если вы не пользуетесь BOOTP, то присвоить IP-адрес можно вручную, в качестве примера взяв следующий метод.

Примечание

За информацией о том, как можно добавить запись в серверную таблицу, обращайтесь к документации вашего BOOTP-сервера.

1. Зафиксируйте Ethernet-адрес (MAC-адрес) сервера печати. Ethernet-адрес представляет собой 12-значное шестнадцатеричное число, которое указывается на наклейке, прикрепленной на нижней плоскости сервера печати.
2. Воспользуйтесь хостом, расположенным в той же локальной сети Ethernet, что и сервер печати. Отредактируйте таблицу ARP (Address Resolution Protocol — протокол разрешения адресов) этого хоста, добавив в нее соответствующий Ethernet-адресу сервера печати IP-адрес, который вы хотите назначить. Во многих системах TCP/IP это можно сделать с помощью команды типа:

   ```
   arp ip-адрес Ethernet-адрес
   ```

3. К примеру, чтобы назначить адрес 202.39.74.40 серверу печати с MAC-адресом 00 80 C8 14 26 34, нужно дать команду

   ```
   arp 202.39.74.40 0080C8142634
   ```

4. В системе на базе UNIX для выполнения команды `arp` у вас должны быть полномочия, соответствующие корневой учетной записи. С хоста, на котором вы

только что редактировали таблицу ARP, отправьте эхо-запрос ICMP на сервер печати — для этого нужно дать команду ping:

```
ping 202.39.74.40
```

5. Когда сервер печати получает на свой Ethernet-адрес ICMP-запрос, но в нем указывается IP-адрес, отличный от ожидаемого, сервер изменяет свою настройку IP-адреса.
6. Теперь сервер будет реагировать на новый IP-адрес. На данном этапе для изменения других настроек этого хоста вы можете пользоваться интерфейсом Telnet (как показано ниже).

Использование Telnet

Обращаться к интерфейсу Telnet вашего сервера печати можно с помощью обычной клиентской программы Telnet. Во многих системах командой, запускающей клиента Telnet, является

```
telnet ip-адрес
```

При этом указывается IP-адрес (ip-адрес), который вы назначили серверу печати. При первом сетевом теледоступе к серверу печати он выводит регистрационное сообщение, приведенное на рис. 16.3.

```
**********************************
* Welcome to Print Server        *
* Telnet Console                 *
**********************************
Server Name  : PS-132544
Server Model : DP-3xx
F/W Version  : 1.02
MAC Address  : 00 80 C8 14 26 34
Up Time      : 5 days, 06:14:38
Please Enter Password:
```

Рис. 16.3. Для администрирования некоторых серверов печати предусматривается интерфейс Telnet. В начале сеанса выводятся подробные данные о работе сервера

На этом этапе вы можете ввести пароль, назначенный для сервера печати. Если с паролем вы еще не определились, просто нажмите клавишу <Enter>. После этого сервер печати отобразит главное меню интерфейса Telnet, показанное на рис. 16.4.

Изменение настроек TCP/IP

После первоначального присвоения IP-адреса сервера печати вам может понадобиться изменить этот адрес или другие конфигурационные данные TCP/IP — например, маску локальной сети, шлюз по умолчанию, допускаемые групповые имена SNMP или перечень получателей "ловушек" SNMP. Для этого, находясь в главном меню, следует выбрать пункт **TCP/IP Configuration** (Настройка TCP/IP). В результате сервер печати выведет на экран меню **TCP/IP Configuration** (рис. 16.5).

```
[Main Menu]
1 - Server Configuration
2 - Port Configuration
3 - TCP/IP Configuration
4 - AppleTalk Configuration
5 - Display Information
6 - Tools
7 - Save Configuration
0 -Quit
Enter Selection:
```

Рис. 16.4. Главное меню Telnet позволяет вам определять основные настройки сервера печати

```
1 - IP Address <168.8.100.52>
2 - Subnet Mask <255.255.0.0>
3 - Default Gateway <168.8.100.254>
4 - SNMP Community
5 - SNMP Traps
0 - Return to Main Menu
Enter Selection:
```

Рис. 16.5. Меню TCP/IP позволяет управлять сетевыми настройками сервера печати

Чтобы изменить IP-адрес, маску локальной подсети или шлюз по умолчанию, выберите соответствующий пункт меню. Сервер печати пригласит вас ввести новое значение выбранного параметра. Введите новое значение и нажмите клавишу <Enter>. Чтобы изменить групповые имена SNMP, выберите соответствующий пункт меню. Сервер печати выведет на экран меню **SNMP Community** (Сообщество SNMP) (рис. 16.6).

```
[SNMP Community]
1 - Community 1 Name <public>
2 - Community 1 Access <Read Only>
3 - Community 2 Name <>
4 - Community 2 Access <Read Only>
5 - Community 3 Name <>
6 - Community 3 Access <Read Only>
0 - Return to TCP/IP Menu
Enter Selection:
```

Рис. 16.6. Меню **SNMP Community** позволяет регулировать параметры SNMP-управления, связанные с сервером печати

В отношении каждого из трех совокупностей групповых имен, поддерживаемых сервером печати, вы можете назначить как само имя, так и уровень доступа (*только чтение* или *чтение/запись*), предоставляемый каждому запросу. SNMP-совместимые станции сетевого управления могут пользоваться заданными групповыми именами для обращения к управляющей и статистической информации, которую собирает

сервер печати. Чтобы изменить запись, выберите соответствующий пункт меню. После того как сервер печати пригласит вас ввести новое значение, введите его, а затем нажмите клавишу <Enter>. Закончив настройку групповых имен, нажмите клавишу <0> — так вы сможете возвратиться в меню **TCP/IP Configuration**. Чтобы изменить настройки "ловушек" SNMP, выберите в меню **TCP/IP Configuration** соответствующий пункт. Сервер печати выведет на экран меню **SNMP Trap** (рис. 16.7).

```
[SNMP Traps]
1 - Traps <Disable>
2 - Target 1 IP Address <0.0.0.0>
3 - Target 1 Community Name <>
4 - Target 2 IP Address <0.0.0.0>
5 - Target 2 Community Name <>
6 - Target 3 IP Address <0.0.0.0>
7 - Target 3 Community Name <>
0 - Return to TCP/IP Menu
Enter Selection:
```

Рис. 16.7. "Ловушки" SNMP позволяют изменять способы взаимодействия SNMP с сервером печати

По умолчанию, "ловушки" SNMP находятся в отключенном состоянии. Чтобы активировать или блокировать отправку ловушек, выберите пункт меню **Traps**. После активации ловушек вы можете назначить до трех различных хостов, которые станут получателями ловушек. С IP-адресом каждого получателя ловушек должно быть связано групповое имя SNMP, которое будет включаться в IP-запрос. Чтобы изменить IP-адрес или групповое имя, следует выбрать соответствующий пункт меню и ввести желаемое значение. Закончив с редактированием настроек TCP/IP, нажмите клавишу <0> — так вы сможете возвратиться в главное меню. Наконец, выберите опцию **Save Configuration** и подтвердите сохранение. После этого соединение Telnet будет разорвано, и сервер печати выполнит автоматическую перезагрузку, чтобы изменения конфигурации вступили в силу.

Изменение настроек сервера печати

В меню **Server Configuration** (Настройки сервера) можно изменить имя сервера, а также значения полей **Location** и **Contact** (в них указывается местоположение сервера печати и лицо, ответственное за его сопровождение). Чтобы изменить настройки сервера печати, выберите в главном меню пункт **Server Configuration** — после этого сервер выведет на экран меню **Server Configuration** (рис. 16.8).

Чтобы изменить имя сервера, его местоположение или административные контакты, выберите соответствующий пункт меню. Сервер печати пригласит вас ввести новое значение. По окончании нажмите клавишу <0> — так вы сможете возвратиться в главное меню. Затем выберите опцию **Save Configuration** (Сохранить настройки) и подтвердите произведенные изменения. После этого соединение Telnet будет разорвано, и сервер выполнит автоматическую перезагрузку, чтобы изменения конфигурации вступили в силу.

Изменение пароля сервера печати

Пароль сервера печати применяется для защиты конфигурационных данных сервера от несанкционированных изменений, которые могут проводиться как с помощью административных программ, так и через интерфейс Telnet. Чтобы изменить пароль сервера, выберите в главном меню опцию **Server Configuration** (Настройки сервера). Сервер печати выведет на экран меню **Server Configuration** (рис. 16.8).

```
[Serer Configuration]
1 - Server NAME <PS-142634>
2 - Location <Massachusetts Office>
3 - Admin Contact <Joseph>
4 - Change Password
0 - Return to Main Menu
Enter Selection:
```

Рис. 16.8. С помощью меню **Server Configuration** вы можете регулировать основные настройки сервера печати

Выберите пункт меню **Change Password** (Изменить пароль). После этого сервер печати попросит ввести старый пароль (если раньше пароль не устанавливался, нажмите клавишу <Enter>). Теперь сервер печати пригласит вас определить новый пароль (символы пароля будут отображаться в виде звездочек "*"), причем ввести его нужно будет дважды. Чтобы подтвердить правильность ввода, во второй раз необходимо указать тот же пароль, что и в первый раз. Чтобы вернуться к главному меню и сохранить изменения настроек, нажмите клавишу <0>. Соединение Telnet будет разорвано, и сервер выполнит автоматическую перезагрузку, чтобы изменения конфигурации вступили в силу.

Изменение настроек портов

У каждого порта сервера печати есть несколько настроек. Вам может потребоваться их регулировка для того, чтобы установить соответствие между вашей конфигурацией и моделью принтера, подключенного к порту. Чтобы изменить одну или несколько настроек портов, выберите в главном меню пункт **Port Settings** (Настройки портов). После этого сервер печати выведет меню, соответствующее типу выбранного порта (меню последовательных и параллельных портов различаются между собой).

Чтобы изменить любую из выведенных на экран настроек, выберите соответствующий пункт меню. Сервер печати пригласит вас ввести новое значение. Закончив регулировку настройки порта, нажмите клавишу <0> — так вы сможете вернуться к меню этого порта. Закончив регулировку всех необходимых настроек отдельного порта, нажмите клавишу <0> еще раз — в результате вы окажетесь в главном меню. Выберите пункт меню **Save Configuration** (Сохранить настройки) и подтвердите сохранение изменений. Соединение Telnet будет разорвано, и сервер выполнит автоматическую перезагрузку, чтобы изменения конфигурации вступили в силу.

Отображение информации

Интерфейс Telnet сервера печати предусматривает два варианта меню с информацией о сервере печати и принтерах, которые к нему подключены. Выбор **Display Information** (Отобразить информацию) в главном меню приводит к открытию меню **Display Information**. Выбор **Display Configuration** (Отобразить настройки) приводит к выводу нескольких страниц информации об аппаратном и внутреннем программном обеспечении сервера печати, а также о его настройках. Там же приводится информация о настройках портов. Выбор **Display Port Status** (Отобразить состояние портов) дает возможность просмотреть статистику и информацию о заданиях, выполняемых через каждый из портов сервера печати (рис. 16.9).

```
Port Number          1              2              3
= = = = = = = = = = = = = = = = = = = = = = = = = = =
[Total Status]
Jobs                 45             1              0
Sizes (KB)           23179          0              0
Timeouts             0              0              0
- - - - - - - - - - - - - - - - - - - - - - - - - - -
[Current Job]
Printer Status       On Line        Off Line       On Line
Index                0              1              0
Protocol NETWARE
Name 00C60001
Spooling Bytes       0              172032         0
Printing Bytes       0              153600         0
= = = = = = = = = = = = = = = = = = = = = = = = = = =
1 - Refresh Port Status
0 - Return to Display Information Menu
Enter Selection:
```

Рис. 16.9. Интерфейс Telnet поддерживает детализованный отчет о различных портах сервера печати

Перезапуск сервера печати

В некоторых случаях возникает необходимость в перезапуске сервера печати — при этом сбрасываются все внутренние статистические счетчики и другие данные, связанные с состоянием сервера. В интерфейсе Telnet предусматривается два типа сброса: простой и заводской. По своему действию простой сброс аналогичен выключению питания сервера печати с его последующей повторной подачей. Статистические счетчики сбрасываются, но все настройки сервера печати остаются в силе. При выполнении заводского сброса происходит не только перезапуск сервера, но и возврат всех настроек конфигурации на исходные значения (т. е. производственные настройки).

Примечание

Пользуйтесь заводским сбросом только в том случае, если вы абсолютно в этом уверены. В результате этой операции все настройки (включая сетевой адрес TCP/IP сервера печати) будут стерты и заменены исходными значениями.

Чтобы произвести сброс сервера печати, выберите в главном меню пункт **Tools** (Сервис). В зависимости от нужного типа сброса, следует выбрать опцию **Reset** (Сброс) или **Factory Reset** (Сброс с установкой заводских настроек). После этого сервер запросит подтверждение. Подтвердите сброс и нажмите клавишу <Enter>. Соединение Telnet будет разорвано, и сервер выполнит автоматическую перезагрузку. Если вы выбрали **Factory Reset**, произойдет восстановление значений конфигурации, принятых по умолчанию.

Поиск неисправностей серверов печати

Современные серверы печати, как правило, демонстрируют достаточную надежность; их инсталляция и сопровождение связаны с минимальными трудностями. Тем не менее неприятности иногда случаются — они могут локализоваться в самом сервере печати, в подключенных к нему принтерах или в сетевой конфигурации сервера. На случай возникновения проблем на сервере печати существуют определенные процедуры, которые призваны помочь вам избавиться от проблем как можно быстрее.

Диагностическое тестирование

В большинстве случаев при первоначальной подаче питания серверы печати выполняют процедуру самотестирования. Ее результаты представляются на светодиодах сервера. Нормальный (безошибочный) результат обозначается тремя вспышками индикатора LPT и началом нормальной работы сервера. Если в процессе тестирования ряда компонентов обнаруживается сбой, проверка приостанавливается, а о конкретной ошибке постоянно сигнализирует светодиод LPT. В табл. 16.1 приводятся коды ошибок для сервера печати D-Link, но коды для вашей модели устройства следует искать в его документации.

Таблица 16.1. *Диагностические сообщения светодиодов для типичного сервера печати D-Link*

Режим вспышек светодиода LPT	Тип ошибки
Постоянные продолжительные вспышки	Требуется перезагрузка микропрограммного обеспечения
Непрерывная сигнализация	Ошибка динамической памяти
Одна продолжительная, две кратковременных вспышки	Внутренняя ошибка таймера
Одна продолжительная, три кратковременных вспышки	Защита от групповых операций
Одна продолжительная, четыре кратковременных вспышки	Ошибка идентификации групповой операции
Одна продолжительная, пять кратковременных вспышек	Ошибка группового стирания /программирования

Таблица 16.1 (окончание)

Режим вспышек светодиода LPT	Тип ошибки
Одна продолжительная, шесть кратковременных вспышек	Ошибка контроллера локальной сети
Одна продолжительная, семь кратковременных вспышек	Ошибка памяти локальной сети
Одна продолжительная, восемь кратковременных вспышек	Ошибка параллельного контроллера
Одна продолжительная, десять кратковременных вспышек	Ошибка построчного принтера (LPT)
Постоянные кратковременные вспышки	Ошибка EERPROM
Одна продолжительная, одиннадцать кратковременных вспышек	Базовая ошибка локального ввода/вывода

Обновление микропрограммного обеспечения

Внутреннее программное обеспечение сервера печати хранится во флэш-памяти, что позволяет заменять его более новыми версиями без помощи производителя. Когда появляются обновления микропрограммного обеспечения, они публикуются на Web-сайте производителя. Обновления прошивки сервера печати часто содержатся в двух связанных файлах: один из них — с расширением bin — большего объема, а второй — с расширением dwl — меньшего объема. Для успешного выполнения флэш-обновления необходимы оба этих файла. После получения новой версии микропрограммного обеспечения необходимо провести процедуру его обновления. Это можно сделать, например, так.

1. Прежде чем записывать новую версию микропрограммного обеспечения поверх старой, необходимо сделать резервные копии старой версии.
2. Откройте программу администрирования сервера печати (или интерфейс Telnet). Выберите пункт **Reload Firmware** (Перезагрузить прошивку) в меню **Tools** (Сервис). Сервер пригласит вас указать имя файла .bin с обновленным загрузочным модулем.
3. Введите путь к файлу .bin или нажмите кнопку **Browse** (Просмотр), чтобы найти этот файл посредством стандартного диалогового окна.
4. Нажмите кнопку **OK**. Как правило, на этом этапе программа администрирования выводит информационно-предупредительное сообщение.
5. Нажмите кнопку **OK**. После этого начнется процесс обновления флэш-памяти под контролем программы администрирования сервера печати.
6. По окончании обновления программа выведет информационное сообщение, после которого вам, возможно, придется отключить, а затем сразу включить питание сервера.

Примечание

При проведении флэш-обновления программного обеспечения ни в коем случае нельзя прерывать передачу путем выключения сервера печати или его отключения от сети. В большинстве случаев сервер сможет восстановиться после прерванной передачи. Тем не менее в некоторых ситуациях для восстановления сервера после прерванного цикла флэш-обновления его придется отдавать в ремонт

Симптомы неисправностей

В дополнение к результатам самотестирования посредством светодиодов существует множество признаков, которые могут указать на отдельные сбои в работе сервера печати.

Симптом 16.1. Светодиоды сервера печати не сигнализируют

В большинстве случаев это связано с неисправностями энергоснабжения — адаптер переменного тока либо отключен, либо неисправен. В любом случае, качество энергоснабжения сервера печати следует проверить. Замените силовой адаптер переменного тока или воспользуйтесь другим сервером печати.

Симптом 16.2. Светодиод состояния сервера печати сигнализирует беспрерывно

Произошел аварийный отказ сервера печати. В большинстве случаев эту неисправность поможет устранить холодная перезагрузка сервера. Отключите сервер от источника питания, а затем подключите его вновь. Если неисправность сохранится, замените сервер печати.

Симптом 16.3. Светодиоды состояния и питания сервера печати сигнализируют беспрерывно

Произошел аварийный отказ сервера печати. Довольно часто эту неисправность можно устранить с помощью перезагрузки сервера кнопкой Reset или отключения его от источника питания с последующим повторным подключением.

Симптом 16.4. При использовании DHCP появляется конфликт IP-адресов с участием сервера печати

В условиях динамической адресации сетевых устройств эта неисправность возникает довольно часто. Если после выключения DHCP-сервера сервер печати продолжает работать, он сохраняет свой IP-адрес, не информируя об этом DHCP-сервер. Чтобы сервер печати получил новый IP-адрес, его следует перезагрузить. Кроме того, эта неисправность возникает в случае выделения серверу печати статического IP-адреса в пределах диапазона, применяемого DHCP-сервером. Если это так, назначьте для него другой адрес, находящийся вне диапазона, используемого DHCP-сервером.

Симптом 16.5. Возникают трудности при попытке применения WPCONFIG для настройки сервера печати в среде Windows 9x

Неисправность связана с программной несовместимостью. Убедитесь в том, что применяемое вами административное программное обеспечение совместимо с операционной системой. Утилита WPCONFIG предназначена только для Windows 3.1.

В среде Windows 9x или NT следует пользоваться более подходящими утилитами типа Bi-Admin, PS Admin или другими программами администрирования.

Симптом 16.6. Светодиод на трехпортовом сервере печати не сигнализирует

Неисправность связана с кабелем. Проверьте проводку кабелей и убедитесь в том, что светодиод связи на концентраторе или коммутаторе горит. Чтобы отрегулировать конфигурацию сервера печати, измените настройки DIP-переключателя на этом устройстве.

Симптом 16.7. При использовании кабеля 10BaseT сервер печати не работает

Проверьте, горит ли соответствующий порту сервера печати светодиод связи, расположенный на концентраторе или коммутаторе. Если он отключен, неисправность заключается в проводке сетевого кабеля. При использовании 10BaseT или 100BaseTX следует проверить светодиод, расположенный рядом с коннектором. Если сетевое соединение установлено, он должен быть включен. Если этот светодиод не работает, попробуйте отсоединить кабель, а затем смонтировать его вновь или воспользуйтесь другим кабелем. Попробуйте подключить сервер к другому порту коммутатора или концентратора. При необходимости проверьте и откорректируйте настройки DIP-переключателя на сервере печати. После внесения изменений в любой из DIP-переключателей перезагрузите сервер.

Симптом 16.8. Принтер, подключенный к серверу печати, не может печатать (или печатает с дефектами)

Зачастую подобные неисправности локализуются в самом принтере. Убедитесь в том, что принтер включен и работает в нормальном режиме (перезагрузите принтер и попробуйте запустить процедуру самотестирования). Неуспешное завершение самотестирования свидетельствует о неисправности принтера и необходимости его замены. Если самотестирование проходит без сбоев, проверьте прокладку кабелей между принтером и сервером — высококачественный кабель (предпочтительно экранированный кабель IEEE 1284) должен быть надежно закреплен с обеих сторон. Кроме того, убедитесь в том, что общая протяженность кабеля между сервером и принтером не превышает 10 футов (304 см) (попробуйте проложить более короткий кабель). Наконец, проверьте, чтобы на сервере печати была установлена последняя версия драйвера данного принтера (а также принтера, выбранного в конкретном приложении).

Симптом 16.9. Не удается внести изменения в конфигурацию сервера печати

К примеру, кнопка **Configuration** на экране **Printer Status** программы Linksys Bi-Admin находится в затененном состоянии — несмотря на то, что принтер является двунаправленным. Как правило, это связано с активностью принтера. Изменить настройки принтера можно только тогда, когда принтер завершит выполнение заданий и войдет в состояние незанятости. Прежде чем пытаться настраивать сервер, дождитесь окончания всех текущих заданий на печать.

Симптом 16.10. В среде NetWare сервер печати печатает с дефектами

В первую очередь, воспользовавшись PSCONFIG или утилитой администрирования сервера печати (например, Linksys Bi-Admin), распечатайте диагностический файл.

Для этого, например, можно запустить утилиту PSCONFIG, выбрать из списка нужный сервер, а затем нажать **Print Diagnostic Report**. Протестируйте все порты и распечатайте диагностический отчет. Успешно ли прошла его распечатка? Если да, значит, возможно, неисправность вызвана неверной конфигурацией системы. Если диагностический отчет распечатан некорректно, проверьте принтер. Если во время осмотра принтера никаких неисправностей выявлено не будет, значит, возможно, замены требует сервер печати.

После этого попробуйте распечатать тестовый текстовый и графический файлы. Если текстовый файл распечатается успешно, а графический — с дефектами, введите опцию `/NT` (без табуляции) команды `nprint` или `capture` и запустите печать еще раз. Если оба теста распечатаются некорректно, временно отключите сервер, обрабатывающий очередь печати, и попробуйте выполнить следующие действия (для NetWare 2.x и 3.x).

1. Запустите PCONSOLE.
2. Выберите **Print Queue Information** (Информация об очереди печати), укажите очередь печати, которую обрабатывает сервер, а затем выберите **Current Queue Status** (Текущее состояние очереди).
3. Установите опцию **Servers can service entries in queue** (Серверы могут обслуживать элементы очереди) в значение **NO**.
4. Нажмите клавишу <Esc> и выберите **Print Queue ID** (Распечатать идентификатор очереди). Запишите идентификатор очереди.
5. Отправьте тестовые файлы в очередь печати, пользуясь нормальными командами печати.

Для режимов Bindery и NDS в NetWare 4.x и 5.x:

1. Запустите PCONSOLE.
2. Выберите **Print Queues** (Очереди печати), укажите очередь печати, которую обрабатывает сервер, а затем выберите **Status** (Состояние).
3. Установите опцию **Allow service by current print servers** (Разрешить обслуживание текущими серверами печати) в значение **NO**.
4. Нажмите клавишу <Esc>, выберите **Information** и запишите идентификатор очереди.
5. Отправьте тестовые файлы в очередь печати, пользуясь обычными командами печати.

Примечание

Когда неисправность будет устранена, не забудьте вернуть эти параметры в исходные значения.

Если неисправность сохранится, замените сетевую печать локальной. Отсоедините принтер, подключенный к серверу печати, и подключите его к порту LPT1 вашего компьютера. Перейдите на диск и в каталог файлового сервера, в котором содержится очередь печати. Название этого каталога должно соответствовать идентификатору очереди (это может быть \queues\Q_ID в режиме NDS или system\Q_ID в режиме Bindery). Тестовые файлы, которые вы распечатывали ранее, должны нахо-

диться в этом каталоге очереди. Эти файлы следует распечатать на локальном принтере; для этого нужно ввести команду COPY с опцией /b — например, так:

```
copy /b test.txt LPT1
```

Сравните распечатки, полученные при выполнении заданий под управлением компьютера и сервера печати. Если они идентичны, значит, неисправность не имеет отношения к серверу. Возможно, выбран неправильный драйвер принтера, или настройка блокировки по времени в команде capture определяет слишком короткий временной промежуток. Если же две эти распечатки отличаются, то неисправность может быть связана с сервером. Попробуйте заменить его.

Симптом 16.11. В списке активных устройств (Active Device List) программы NetWare PSCONFIG сервер печати отсутствует

Иногда подобные трудности обуславливаются неправильной сборкой физической сети. Проверьте, находится ли сервер печати в том же сетевом сегменте, что и компьютер. Если сервер расположен в другом сегменте сети, то обращаться к нему, вероятно, придется с другого административного компьютера (т. е. системы, на которой установлено административное программное обеспечение сервера печати, такое как Bi-Admin или PS Admin), который находится там же, где и сервер.

В некоторых случаях возникает необходимость в загрузке на компьютер совместимого протокола. К примеру, чтобы административное программное обеспечение сервера печати имело возможность подключения через NetBEUI, этот протокол необходимо установить в системе. Проверьте документацию к серверу и убедитесь в том, что применяемая административная система соответствует всем системным требованиям для программного обеспечения сервера печати. Установив соединение с сервером, проверьте, активирован ли на административном компьютере протокол NetWare. Тип кадров Ethernet, применяемый на компьютере, может отличаться от того типа, который используется на сервере — активируйте все типы кадров Ethernet и попробуйте подключить сервер еще раз.

Симптом 16.12. Сервер печати настроен на работу с NetWare, но не может зарегистрироваться на файловом сервере

Почти во всех случаях эта неисправность связана с конфигурацией сервера печати. Начните с проверки настроек сервера печати с помощью утилиты PSCONFIG или административного программного обеспечения сервера печати (например, Bi-Admin или PS Admin). Если устройство настроено как сервер печати NetWare, то данные, которые вы увидите, будут похожи на данные, показанные на рис. 16.10.

Убедитесь в правильности присвоения имени ведущему файловому серверу (Master File Server) и проверьте текущее состояние вашего файлового сервера. Возможно одно из следующих состояний.

- *Connected* (Подключен). Никаких действий не требуется — устройство отвечает в нормальном режиме.
- *No file server* (Файловый сервер отсутствует). Вы должны назначить ведущий файловый сервер — для этого можно воспользоваться утилитой PSCONFIG или административным программным обеспечением сервера печати.
- *Connecting to server* (Подключение к серверу). Подождите и проверьте, существует ли файловый сервер.

- *Password mismatch* (Несоответствие пароля). Сбросьте пароль NetWare (с помощью PCONSOLE) или задайте правильный пароль для сервера печати (с помощью PSCONFIG или программы администрирования).
- *Print server not defined* (Сервер печати не определен). Переустановите сервер.

```
Server Name                    : SC110049
NetWare Information            :
Master File Server             : ICE
Print Server Mode Status       :
Your_File_Server               : Current Status
Remote Printer Mode Status     : N/A
```

Рис. 16.10. Проверка конфигурации сервера печати, как правило, дает возможность обнаружить очевидные ошибки в настройках

В среде NetWare необходимо проверить, находится ли сервер печати на файловых серверах в состоянии готовности. Если это не так, ознакомьтесь с сообщением об ошибке и внесите необходимые изменения. Далее следует проверить длину имени файлового сервера NetWare. Она не должна превышать 15 символов (включая буквы, цифры и дефис). Если эти требования не соблюдены, измените имя файлового сервера. Наконец, если файловый сервер в таблице состояния отсутствует, но при этом сервер печати зарегистрировался на ведущем файловом сервере, значит, данный файловый сервер сервером печати не обслуживается. Проверьте, присутствует ли этот файловый сервер в перечне элементов **File Server To Be Serviced** (Обслуживаемые файловые серверы) в PCONSOLE. Если имени нужного файлового сервера в этом перечне нет, введите его.

Симптом 16.13. Сервер печати настроен как удаленный принтер NetWare, но он не может зарегистрироваться на сервере печати NetWare

Для начала проверьте конфигурацию сервера печати NetWare и соберите данные о его настройках — так, как описано в предыдущем пункте. Теперь проверьте содержимое поля **Remote Printer Mode Status** (Состояние режима работы удаленного принтера). В нем должна быть запись состояния для каждого логического принтера. Возможны несколько вариантов состояния.

- *Connected* (Подключен). Никаких действий не требуется — устройство отвечает в нормальном режиме.
- *Unable to find server* (Найти сервер не удается). Загрузите программное обеспечение сервера печати NetWare.
- *Connecting to server* (Подключение к серверу). Подождите и проверьте, загружен ли сервер NetWare.
- *Printer not defined* (Принтер не определен). Установите устройство как удаленный принтер сервера печати NetWare.

В среде NetWare нужно проверить, находится ли сервер печати в состоянии готовности. Если это не так, ознакомьтесь с сообщением об ошибке и выполните необходимые корректирующие действия. Наконец, следует проверить длину имени фай-

лового сервера NetWare. Она не должна превышать 15 символов (включая буквы, цифры и дефис). Если эти требования не соблюдаются, измените имя файлового сервера.

Симптом 16.14. Сервер печати не выполняет задания, которые направляются в очередь печати NetWare

В первую очередь проверьте подключение принтера к источнику питания. Кроме того, проверьте факт регистрации сервера печати на файловом сервере NetWare и убедитесь в правильности номера принтера NetWare — например, он может быть таким:

- 0 = параллельный порт 1 сервера печати;
- 1 = параллельный порт 2 сервера печати;
- 2 = параллельный порт 3 сервера печати.

Проверьте текущее состояние очереди печати. Запустите PCONSOLE и выберите **Print Queue Information** (Информация об очереди печати). Затем выберите нужную очередь и нажмите **Current Queue Status** (Текущее состояние очереди). Всем трем параметрам должны быть присвоены значения YES; в противном случае попробуйте запустить задание на печать еще раз.

Затем убедитесь в том, что по отношению к рассматриваемой очереди печати ваш сервер печати действует как сервер статической очереди. Запустите PCONSOLE и нажмите **Print Server Information** (Информация о серверах печати). Последовательно выберите **Print Server Configuration** (Настройка сервера печати), **Queues Services by Printer** (Очереди, обслуживаемые принтером). Затем укажите нужный принтер и проверьте, присутствует ли в его списке рассматриваемая очередь. Если этой очереди в списке нет, ее можно добавить, нажав клавишу <Insert>. Чтобы сервер печати смог приступить к обслуживанию новой очереди, его нужно перезапустить. Наконец, общее количество обслуживаемых очередей, возможно, превысило допустимый предел (которым может быть, например, 56). Если это так, уменьшите количество очередей до приемлемого уровня и попробуйте запустить задание на печать еще раз.

Симптом 16.15. Для выполнения задания на печать использовалась команда *capture* NetWare, но задание было разделено на две части

Возможно, период блокировки по времени, заданный командой `capture`, недостаточен. Чтобы увеличить значение блокировки по превышению времени, дайте команду `capture` с опцией `/TI=n`, где упомянутое значение представляет `n`.

Симптом 16.16. Утилита PSCONFIG или программа администрирования выводит сообщение "нет ответа"

Эта неисправность может обуславливаться несколькими причинами — например, избыточным сетевым трафиком: если сеть занята, нужно в течение некоторого времени подождать, а затем попробовать отправить задание на печать еще раз. Кроме того, вполне возможно, что сервер печати отключен от питания или кабельной проводки, тогда следует проверить источник питания и сетевой кабель сервера печати. Наконец, адрес узла сервера может дублироваться адресом узла другого устройства, расположенного в той же сети. Возможно, вам придется изменить адрес узла сервера печати (или конфликтующего с ним устройства).

Симптом 16.17. При проверке регистрации сервера печати на файловом сервере команда *quickset* блокируется по превышению лимита времени

Во многих случаях это означает, что сервер печати не зарегистрирован на ведущем файловом сервере. Обычно причиной этого является несоответствие типов кадров Ethernet. Попытайтесь определить тип кадра, применяемый сервером печати, воспользовавшись для этого утилитой PSCONFIG или административным программным обеспечением этого устройства (например, Bi-Admin). Настройте тип кадров сервера печати таким образом, чтобы он совпадал с типом кадров, применяемым на ведущем файловом сервере (и отключите все остальные типы кадров).

Симптом 16.18. В среде NetWare 4.x сообщения с уведомлениями не поступают

Довольно часто эта неисправность имеет отношение к конфигурации. Убедитесь в том, что вы являетесь участником рассылки уведомлений (Notify) сервера печати. Запустите NetAdmin и задайте имя сервера, принимающего оповещения по умолчанию.

Симптом 16.19. Установить состояние принтера не удается, или он определяется как "нефункционирующий"

К примеру, вам не удается определить состояние принтера с помощью утилиты PCONSOLE или административного программного обеспечения принтера (например, Bi-Admin). Кроме того, текущее состояние сервера в **Printer Server Information** в среде NetWare 4.x обозначается как Down ("не функционирует"). Возможно, вы создали объект сервера печати в среде NetWare 3.x, а для просмотра его состояния пытаетесь использовать PCONSOLE в среде NetWare 4.x. Убедитесь в том, что сервер печати включен (ON) и удалите соответствующий ему объект среды. При необходимости проведите повторную установку сервера печати в среде NetWare 4.x с NDS.

Симптом 16.20. Настройки "String Before Job" и/или "String After Job" в разделе логических принтеров (Logical Printers) работают некорректно

Проверьте длину управляющих строк (по длине ни одна строка не может превышать 15 символов). Убедитесь в том, что управляющие строки представлены в шестнадцатеричном формате.

Симптом 16.21. Появляются трудности при обслуживании дополнительных файловых серверов NetWare Bindery

Если ваш сервер печати настроен как NetWare Print Server, но предполагается, что он должен обслуживать несколько файловых серверов Bindery, попробуйте выполнить следующие действия.

1. Зарегистрируйтесь (с диспетчерскими правами) на тех файловых серверах, которые должен обслуживать сервер печати.
2. Создайте запросы и имя сервера печати на каждом из этих файловых серверов.
3. Зарегистрируйтесь (с диспетчерскими правами) на том файловом сервере, который по отношению к серверу печати является ведущим.
4. Запустите PCONSOLE.

5. Выберите **Print Server Information** (Информация о сервере печати), а затем выделите из списка серверов печати тот, который вам нужен.
6. Последовательно выберите **Printer Server Configuration** (Настройки сервера печати), **File Server To Be Serviced** (Обслуживаемые файловые серверы).
7. Введите имя (имена) других файловых серверов, которые будут обслуживаться сервером печати.
8. Перезапустите сервер.

Симптом 16.22. Появляются трудности при подключении к нескольким серверам печати NetWare

Если, находясь в режиме удаленного принтера (Remote Printer) NetWare, вы хотите подключить каждый порт сервера печати к другим серверам печати NetWare, воспользуйтесь PCONSOLE для создания и назначения нужных принтеров и очередей. Теперь запустите утилиту PSCONFIG и выберите **Set to NetWare Remote Printer Mode** (Установить в режим удаленного принтера NetWare). Введите точные имена серверов печати NetWare в соответствующие поля и выберите **Execute Setup** (Запустить установку).

Симптом 16.23. Документы приложений Windows распечатываются некорректно

К примеру, печать из некоторых Windows-приложений (таких как PowerPoint) растягивается на долгое время, а распечатки получаются дефектными. Как правило, причина этого заключается в том, что принтер запускает печать после подкачки первой страницы. Чтобы изменить настройки буферизации, сделайте следующее:

1. Последовательно выберите **Control Panel** (Панель управления), **Printers** (Принтеры).
2. Щелкните правой кнопкой мыши по нужному принтеру и последовательно выберите **Properties** (Свойства), **Details** (Подробности).
3. Нажмите кнопку **Spool Settings** (Настройки подкачки данных).
4. Выберите **Start printing after last page is spooled** (Начать печать после закачки последней страницы) и нажмите кнопку **OK**. Попробуйте запустить печать еще раз.

Симптом 16.24. При подключении нового принтера в среде Windows 9x появляется сообщение о том, что принтер не найден

При настройке некоторых принтеров как локальных, их драйверы проводят опросы подключений. Так как принтер находится в сети, он не обнаруживается (и, соответственно, генерируется ошибка). Чтобы переустановить сетевой принтер, сделайте следующее.

1. Когда мастер Add Printer Wizard спросит **How is the printer attached to your computer?** (Как принтер подключен к вашему компьютеру?), выберите ответ **Network Printer** (Сетевой принтер).
2. При появлении приглашения на ввод сетевого пути (**Network Path**) или имени очереди (**Queue Name**), введите произвольное значение типа `\\SCnum\P1` (или `P2` и `P3` для LPT2 и LPT3, соответственно) и нажмите кнопку **Next** (Следующий).

3. Мастер Printer Wizard выведет сообщение о том, что сетевой принтер находится в неоперативном режиме; продолжайте установку принтера.
4. По окончании процедуры войдите в **Control Panel** (Панель управления) и двойным щелчком мыши откройте каталог **Printer**, в котором вам предстоит выбрать нужный принтер — его пиктограмма будет затенена (это означает, что данный принтер не готов).
5. Щелкните на этой пиктограмме правой кнопкой мыши, выберите **Properties** (Свойства), а затем перейдите на вкладку **Details** (Подробности). В поле **Print to the following port** (Печать в следующий порт) выберите **Print Server** (Сервер печати).
6. Нажмите кнопку **Apply** (Применить), затем — **OK** и закройте диалоговое окно **Properties** (Свойства).
7. Выберите нужный принтер, затем зайдите в меню **File** (Файл) и убедитесь в том, что опция **Work Offline** (Отложенная печать) отключена.
8. Если принтер надлежащим образом подключен к источнику питания и к кабелю, затенение с его пиктограммы должно быть снято, а у вас должна появиться возможность печатать.

Симптом 16.25. Вы подключили и настроили принтер WPS (система печати Windows), но выполнить на нем задание печати не удается

Перед отправкой данных печати драйверы WPS проводят опросы своих принтеров. Так как принтер находится сети, он не обнаруживается, и данные не отсылаются. Чтобы устранить эту неисправность, нужно представить данный принтер как сетевой — о том, как это сделать, рассказывалось в предыдущем пункте. Ниже приведен список из нескольких распространенных WPS-принтеров:

- Canon LBP-430W;
- Epson ActionLaser 1300/W, Epson EPL-5500/W;
- HP LaserJet 5L, линейка Lexmark WinWriter;
- линейка NEC SuperScript, Olivetti PG304;
- линейка Samsung MyLaser;
- линейки HP DeskJet CX и CS.

Симптом 16.26. В среде Windows текст распечатывается хорошо, а графика — с дефектами

Эта неисправность часто связана с драйвером. В таком случае нужно получить от производителя последнюю версию драйвера и установить его. Кроме того, можно попробовать отрегулировать настройки буферизации — например, так, как показано в следующем примере.

1. Последовательно выберите **Start** (Пуск), **Settings** (Настройка), **Printers** (Принтеры).
2. Щелкните на пиктограмме нужного принтера правой кнопкой мыши и выберите **Properties** (Свойства).
3. В среде Windows 9x откройте вкладку **Details** (Подробности), затем выберите **Spool Settings** (Настройка подкачки данных) и измените текущее значение пара-

метра на **Spool Data Format (RAW)**. Для пользователей Windows NT: откройте окно **Properties** (Свойства), относящееся к вашему принтеру, и нажмите **General** (Общие). Для параметра **Print Processor** (Обработчик печати) выберите значение **RAW** или **EMF**. Нажмите **Always Spool RAW Data Type** (Всегда подкачивать данные типа RAW).

4. Дважды нажмите кнопку **OK**.

Симптом 16.27. Появляется сообщение об ошибке соединения SPX

Такая ошибка, к примеру, может появляться при попытке задать или изменить настройки TCP/IP сервера печати. Довольно часто эта неисправность связана с протоколом — она возникает, когда утилиты, применяемые сервером печати, требуют установки протокола IPX/SPX. Если это так, то вам, вероятно, придется установить IPX/SPX до применения сервера печати. Нужно также проверить прокладку кабеля и убедиться в том, что на концентраторе и сервере печати горят светодиоды связи. При необходимости вы можете сбросить или восстановить заводские настройки по умолчанию для сервера печати, воспользовавшись административным программным обеспечением этого устройства (например, программой Bi-Admin) или интерфейсом Telnet.

Симптом 16.28. Некоторые DOS-программы не работают в одноранговой среде Windows 9x

Для печати из некоторых DOS-приложений требуется порт LPT. В этом случае можно подключить протокол NetBEUI и настроить порт на поддержку DOS. В вашей сети должен быть установлен протокол NetBEUI. В качестве примера вы можете руководствоваться следующими действиями.

1. Запустите административное программное обеспечение сервера печати (например, Bi-Admin), выберите опцию **Configuration Menu** (Меню настройки), а затем — **NetBEUI**.
2. В строке **Domain** (Домен) введите имя вашей сетевой рабочей группы.
3. Нажмите **Save to Device** (Сохранить).
4. Откройте каталог **Network Neighborhood** (Сетевое окружение). В нем должен быть указан сетевой сервер печати. Если его там нет, нужно несколько раз нажать клавишу <F5> — так вы сможете обновить окно.
5. Дважды щелкните на записи сервера печати (например, "SCE15223" или "SCC15232").
6. Вы должны увидеть запись порта в форме "Pn" (например, P1, где n — это номер порта на сервере печати).
7. Правой кнопкой мыши щелкните на порте, который хотите захватить (например, P1) и выберите **Capture Printer Port** (Захватить порт принтера).
8. Появится окно с требованием указать устройство. Выберите порт, который вы предполагаете использовать (например, LPT1 или LPT2).
9. Выберите флажок **Reconnect at logon** (Переподключаться при регистрации) — в результате вы сможете подключаться к серверу печати после перезагрузки компьютера.

10. Чтобы настроить принтер, последовательно выберите **Start** (Пуск), **Settings** (Настройка), **Printers** (Принтеры).
11. Правой кнопкой мыши щелкните на принтере, который предполагается настроить, и выберите **Properties** (Свойства).
12. Откройте вкладку **Details** (Подробности).
13. Измените номер порта **Print to the LPT port** (Печать в порт LPT), определенный на 8 этапе.
14. Чтобы завершить процедуру, нажмите кнопку **Apply** (Применить), затем — **OK**.
15. Перезагрузите компьютер.

Примечание

За более подробной информацией о NetBEUI обращайтесь к документации по операционной системе.

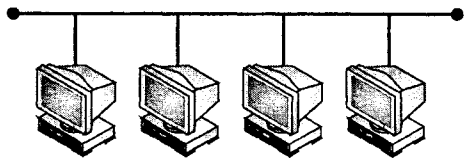
Дополнительные ресурсы

D-Link: **www.dlink.com**.

Hewlett-Packard: **www.pandi.hp.com/seg/ps_ns.html**.

Intel: **support.intel.com/support/network/index.htm**.

Linksys: **www.linksys.com**.



ГЛАВА 17

Электропитание

Работа сети любой конфигурации и размера зависит от подачи электропитания (переменного тока). Сетевой администратор осуществляет управление подачей электропитания, чтобы обеспечить надежное энергоснабжение сети, а также продолжение работы в условиях штормов, аварий и других факторов, которые часто неподвластны контролю. В этой главе рассматриваются методы управления питанием, а также применение резервных источников бесперебойного питания.

Сетевое управление питанием

Конфигурация современных компьютерных сетей становится все крупнее и сложнее. Из-за повышения расходов на электроэнергию (и внимания, уделяемого сегодня рациональному использованию энергии) управление питанием становится приоритетной задачей для сетевых администраторов, которые часто вынуждены поддерживать производительность и доступность сети в условиях ограниченного бюджета на обслуживание сети. При проектировании систем, которые используют меньше электроэнергии благодаря современным методикам энергосбережения, во время периодов простоя компьютер можно вообще не выключать, и при этом он будет потреблять всего лишь около 5 В в состоянии энергосбережения (что меньше, чем энергопотребление ночника). Это позволяет существенно сократить расходы на электроэнергию и издержки на поддержание сети. В этой части главы мы рассмотрим современные технологии рационального использования электроэнергии и методики оптимизации энергопотребления простаивающих устройств.

Управление питанием и Windows 2000

Поддержка управления питанием должна обеспечиваться со стороны нескольких важных компонентов: BIOS, набора микросхем, устройств и операционной системы. Операционная система включает элементы управления и диалоговые окна, необходимые для выбора схемы управления питанием, а также различные драйверы, управляющие электропитанием устройств системы. С точки зрения контроля энергопотребления системы Windows 98 и Windows ME считаются ведущими операционными системами для конечного пользователя, но функции управления питанием представлены и в Windows 2000. С помощью диалогового окна **Power Options Properties**

(Свойства: Электропитание) можно настроить каждый компонент персонального компьютера. Вид этого диалогового окна в среде Windows 2000 представлен на рис. 17.1.

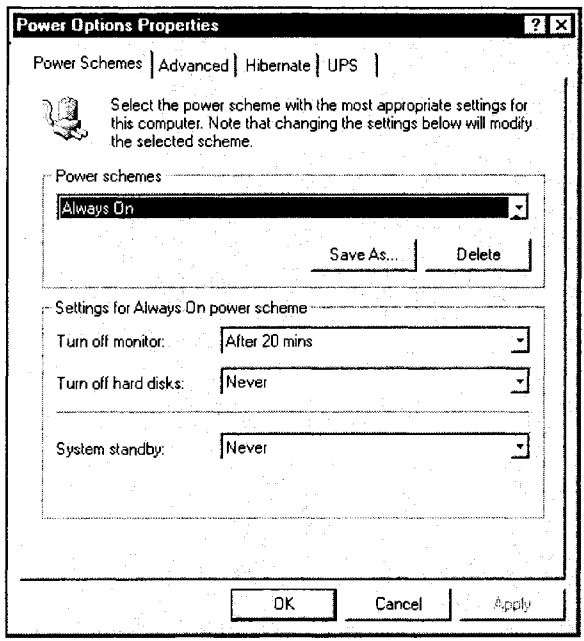


Рис. 17.1. Диалоговое окно **Power Options Properties** в системе Windows 2000

Управление питанием в Windows начинается с выбора *схемы управления питанием* — эта базовая модель использует совокупность настроек, которые управляют периодами снижения электропотребления аппаратных устройств. Однако ничто не мешает вам отрегулировать эти настройки в соответствии с вашими предпочтениями. Существует три основных режима энергосбережения.

- *Базовый режим энергосбережения.* По прошествии определенного периода бездеятельности ваш монитор (или подсветка жидкокристаллического дисплея), а также жесткий диск автоматически выключаются (в результате происходит существенное снижение энергопотребления, хотя все остальные компоненты системы могут продолжать работать).
- *Ждущий режим.* Во время простоя компьютера можно активировать ждущий режим. В этом режиме монитор и жесткие диски выключаются, а энергоснабжение некоторых других компонентов компьютера снижается. При необходимости дальнейшего применения компьютера он способен выйти из ждущего режима довольно быстро, и ваш рабочий стол (и важные документы) восстанавливается точно в таком же виде, как до перехода в режим ожидания. Ждущий режим особенно удобен для рационального использования заряда батареи ноутбука.
- *Спящий режим.* На компьютере можно активировать спящий режим по истечении длительных периодов простоя (например, когда вы уходите из офиса на це-

лый день). Спящий режим в первую очередь отключает монитор и жесткие диски (т. е. сначала происходит вхождение в ждущий режим). Если простой продолжается, система сохраняет все данные, находящиеся в памяти, на диске, а затем отключает компьютер. При повторном запуске компьютера его последнее состояние восстанавливается в памяти с помощью данных, сохраненных на диске, и рабочий стол выводится в том же виде, в котором вы его оставили.

В следующих разделах рассматривается несколько схем управления питанием в среде Windows 2000.

Выбор схемы управления питанием

Чтобы активировать ждущий режим и воспользоваться функциями компьютера, связанными с управлением питанием, вы в первую очередь должны выбрать схему управления питанием. Для этого последовательно выберите **Start** (Пуск), **Settings** (Настройка), **Control Panel** (Панель управления) и двойным щелчком выберите пиктограмму **Power Options** (Электропитание). В результате на экране появится диалоговое окно **Power Options Properties** (Свойства: Электропитание) (см. рис. 17.1). Откройте выпадающее меню **Power schemes** (Схемы управления питанием) и выберите один из возможных вариантов; их названия в некоторой степени характеризуют методы использования компьютера:

- **Always On** (Всегда включен);
- **Home/Office Desk** (Домашний/Настольный);
- **Portable/Laptop** (Портативная);
- **Presentation** (Презентационная);
- **Minimum Power Management** (Диспетчер энергосбережения);
- **Maximum Battery** (Экономия батарей).

При выборе схемы следует обратить внимание на то, что ее настройки (**System standby** (Ждущий режим через), **Turn off monitor** (Отключение дисплея) и **Turn off hard disks** (Отключение дисков)) используют значения по умолчанию. Если вы хотите изменить значения таймеров по умолчанию (т. е. увеличить период времени, по прошествии которого система будет входить в ждущий режим), щелкните на нужном таймере и выберите нужное значение времени из появившегося выпадающего списка. С помощью этих временных значений можно настроить монитор, жесткий диск и задержки до вхождения в ждущий режим в соответствии с вашими личными предпочтениями. Не забудьте о том, что применить (с помощью кнопки **Apply**) новые значения нужно перед нажатием кнопки **OK**.

Примечание

На ноутбуке вы можете по отдельности указать два времени запуска ждущего режима: для аккумулятора и для источника переменного тока.

Сохранение/удаление схемы управления питанием

Если вы внесли изменения в значения таймеров схемы управления питанием, то новые настройки можно сохранить в виде отдельной схемы. Для этого, отрегулиро-

вав значения таймеров, нажмите кнопку **Save As** (Сохранить как) и введите имя новой схемы — в результате она появится в выпадающем списке **Power schemes** (Схемы управления питанием). Если какая-то схема управления питанием вам больше не нужна, выберете ее в выпадающем списке **Power schemes** и нажмите кнопку **Delete** (Удалить).

Ручной переход в ждущий режим

Простейший способ активации ждущего режима предполагает использование диалогового окна **Shut Down Windows** (Завершение работы) (рис. 17.2). Вы можете настроить систему таким образом, чтобы она входила в ждущий режим при каждом нажатии кнопки Power (или при закрытии крышки ноутбука). Для этого последовательно выберите **Start** (Пуск), **Settings** (Настройка), **Control Panel** (Панель управления), двойным щелчком выберите пиктограмму **Power Options** (Электропитание). В результате появится диалоговое окно **Power Options Properties** (Свойства: Электропитание). Откройте вкладку **Advanced** (Дополнительно) (рис. 17.3). Найдите запись **When I press the power button on my computer** (При нажатии кнопки включения питания компьютера) и выберите настройку **Standby** (Переход в ждущий режим). Если вы работаете на ноутбуке, найдите запись **When I close the lid of my portable computer** (При закрытии крышки моего портативного компьютера) и выберите **Standby** (Переход в ждущий режим). Нажмите кнопку **Apply** (Применить) (или **OK**), а затем выключите питание компьютера или (при использовании ноутбука) закройте его крышку.

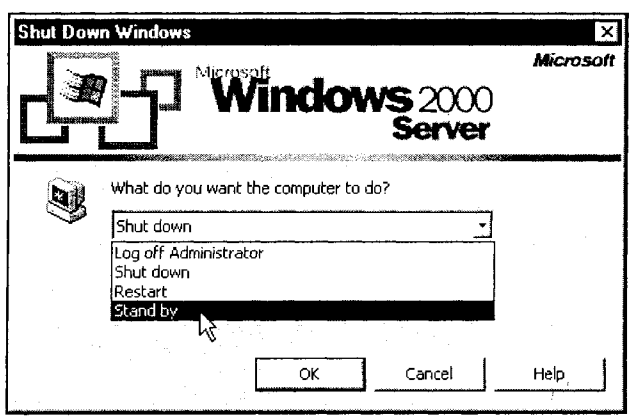


Рис. 17.2. Применение функции перехода в ждущий режим с помощью диалогового окна **Shut Down Windows** в системе Windows 2000

Примечание

Перед активацией ждущего режима нужно сохранить работу. Когда компьютер находится в этом режиме, информация в оперативной памяти компьютера не сохраняется на жестком диске — если случится сбой электропитания, эта информация может быть потеряна.

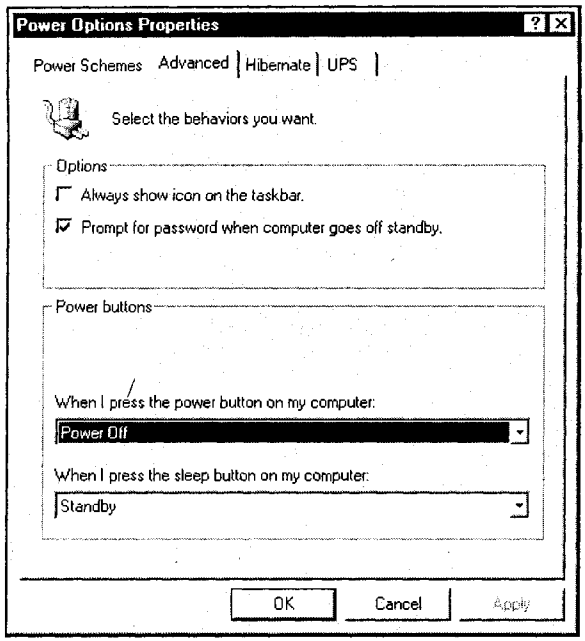


Рис. 17.3. Вкладка **Advanced** диалогового окна **Power Options Properties** в системе Windows 2000

Ручной переход в спящий режим

При активации спящего режима на жесткий диск сохраняется все содержимое памяти. При выведении компьютера из этого режима все программы и документы, которые были открыты ранее, восстанавливаются на рабочем столе. Последовательно нажмите **Start** (Пуск), **Settings** (Настройка), **Control Panel** (Панель управления) и двойным щелчком выберите пиктограмму **Power Options** (Электропитание). В результате появится диалоговое окно **Power Options Properties** (Свойства: Электропитание). Откройте вкладку **Hibernate** (Спящий режим) и установите флажок **Enable hibernate support** (Разрешить спящий режим) (рис. 17.4). Откройте вкладку **Advanced** (Дополнительно), найдите запись **When I press the power button on my computer** (При нажатии кнопки включения питания компьютера) и выберите вариант **Hibernate** (Переход в спящий режим). Если вы работаете на ноутбуке, найдите запись **When I close the lid of my portable computer** (При закрытии крышки моего портативного компьютера) и выберите **Hibernate** (Переход в спящий режим). Нажмите кнопку **Apply** (Применить) (или **OK**), а затем выключите питание компьютера или закройте крышку ноутбука.

Примечание

Если вкладка **Hibernate** (Спящий режим) не отображается, значит, ваш компьютер с его текущим комплектом аппаратного и программного обеспечения не поддерживает эту функцию.

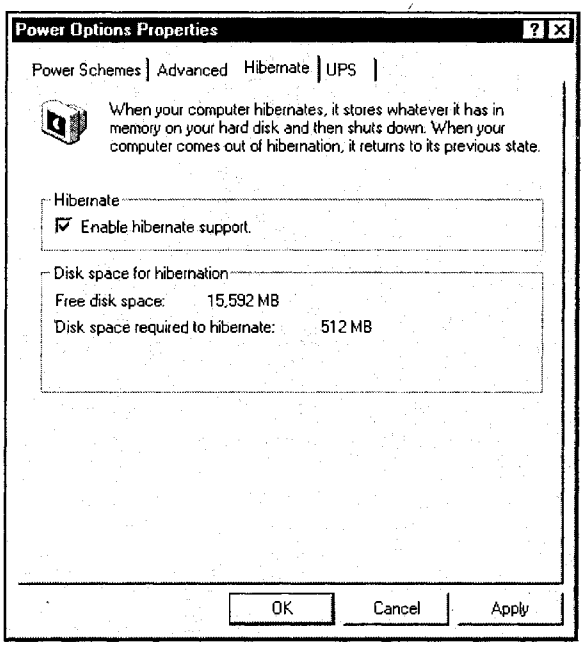


Рис. 17.4. Включение спящего режима в системе Windows 2000

Пароли в ждущем и спящем режиме

Чтобы предотвратить несанкционированный вывод компьютера из ждущего или спящего режима с помощью мыши или клавиатуры, вы можете определить пароли, которые будут охранять компьютер во время его пробуждения. Для этого последовательно выберите **Start** (Пуск), **Settings** (Настройка), **Control Panel** (Панель управления), а затем двойным щелчком выберите пиктограмму **Power Options** (Электропитание). В результате появится диалоговое окно **Power Options Properties** (Свойства: Электропитание). Войдите на вкладку **Advanced** (Дополнительно) и установите флажок **Prompt for password when computer goes off standby** (Запрашивать пароль при выходе из спящего режима). Как для ждущего режима, так и для спящего режима следует использовать ваш Windows-пароль. Имейте в виду, что применение пароля не является обязательным условием, но пароль позволяет обеспечить определенный уровень безопасности — ведь ваша система будет работать и тогда, когда вас не будет рядом.

Усовершенствованный интерфейс конфигурирования системы и управления электропитанием (ACPI)

Усовершенствованный интерфейс конфигурирования системы и управления электропитанием (ACPI, Advanced Configuration and Power Interface) — это открытая промышленная спецификация, которая представляет собой гибкий и расширяемый

аппаратный интерфейс для материнской платы. Разработчики программного обеспечения пользуются этой спецификацией для интеграции функций управления электропитанием во все компоненты системы, включая аппаратное и прикладное программное обеспечение и операционную систему. Подобная интеграция позволяет Windows 2000 определять, какие приложения находятся в активном состоянии, и управлять всеми ресурсами управления питанием, связанными с подсистемами и периферийными устройствами компьютера. К примеру, система ACPI способна отключать ("уменьшать") широкий спектр устройств, включая приводы CD-ROM и DVD-ROM, модемы, сетевые устройства и т. д. Интерфейс ACPI позволяет системе пробуждаться и выполнять определенные задачи на основе реальных событий. К примеру, система ACPI может осуществлять пробуждение системы при получении вызова модемом, затем подключаться и обмениваться данными, а после завершения вызова возвращаться в ждущий или спящий режим. В современных компьютерах применяется спецификация ACPI 2.0, которая впервые была представлена в июле 2000 г.

Примечание

Соблюдение спецификации ACPI является необходимым условием достижения всей полноты возможностей управления питанием и Plug-and-Play в системе Windows 2000. Если вы не уверены в том, что ваш компьютер соответствует ACPI, ознакомьтесь с документацией производителя.

В дополнение к функциям управления питанием, которые поддерживаются операционной системой, ACPI обеспечивает совместимость с PnP, а также независимый от операционной системы интерфейс для управления настройками устройств. Таким образом, система ACPI может управлять питанием и конфигурацией устройств. В результате ACPI представляет собой сочетание технологий Plug-and-Play и APM (Advanced Power Management — расширенное управление питанием), обеспечивающее более точный и гибкий контроль над системными устройствами.

BIOS системы ACPI

Система BIOS компьютера представляет собой комплект программного обеспечения, посредством которого операционная система (или Setup) взаимодействует с системными аппаратными устройствами. ACPI является современным стандартом управления питанием, реализованным в BIOS. Windows 2000 поддерживает не только ACPI-совместимые версии BIOS, но также некоторые версии BIOS, основанные на более старых технологиях APM и Plug-and-Play.

Некоторые версии BIOS на базе ACPI не соответствуют требованиям этого стандарта. Чем современнее версия ACPI BIOS, тем более вероятно, что она соответствует этим требованиям. BIOS на базе ACPI, не соответствующая стандарту ACPI, может не обеспечивать поддержку реального взаимодействия между операционной системой (или Setup), с одной стороны, и аппаратным обеспечением, с другой. В отсутствие поддержки реального взаимодействия Setup приостанавливает свою работу и выводит инструкции, в соответствии с которыми вы должны связаться с производителем аппаратного обеспечения или предпринять другие действия для решения возникшей проблемы. Поэтому полезно проверить используемую версию BIOS системы перед установкой (или модернизацией до) Windows 2000. Систему BIOS, которая не соответствует стандарту ACPI, обычно можно обновить.

ACPI и Plug-and-Play

Наиболее полно возможности Plug-and-Play реализуются только в системе на базе ACPI в режиме ACPI (настраиваемом с помощью ACPI Setup), причем все входящие в нее аппаратные устройства должны поддерживать технологию PnP. Не забывайте, что именно ОС (а не аппаратное обеспечение) в среде ACPI осуществляет настройку и мониторинг компьютера. Операционная система Windows 2000 определяет, какие программы находятся в активном состоянии, и координирует все потребляемые мощности подсистем и периферийных устройств компьютера. ACPI позволяет операционной системе направлять электроэнергию устройствам по мере необходимости, что исключает избыточное энергопотребление в системе.

Так как Windows 2000 контролирует ресурсы и конфигурацию вашего компьютера, вы можете устанавливать аппаратные устройства PnP без его перезагрузки. Windows 2000 автоматически обнаруживает новое оборудование и устанавливает все необходимые драйверы. Если вы используете другую ОС, при установке новых аппаратных устройств может потребоваться ручная настройка и перезагрузка.

Поиск неисправностей в управлении питанием

Управление питанием дает неоспоримые преимущества компьютерам, которые могут быстро откликаться, но при этом в состоянии незанятости потребляют очень мало электроэнергии. Система BIOS, набор микросхем, устройства и операционная система должны работать в идеальной координации, чтобы избежать аварийных отказов и повреждения данных в системе. К сожалению, такая ситуация складывается далеко не всегда (особенно это относится к старым системам). Несовместимость BIOS, поврежденные драйверы и аппаратные устройства, не соответствующие стандартам, — это лишь некоторые проблемы, которые могут привести к сбоям в управлении питанием. В этой части главы рассматривается несколько возможных неисправностей управления питанием и способов их устранения.

Симптомы неисправностей ACPI

Интерфейс ACPI в настоящее время является стандартной технологией управления питанием, применяемой в современных компьютерах типа сетевых серверов и рабочих станций последних моделей. ACPI, несомненно, обеспечивает более полный и гибкий контроль над многими устройствами в системе, но его применение повышает вероятность возникновения сбоев и неисправностей. Приведенные ниже симптомы предлагают вашему вниманию срез таких наиболее общих проблем ACPI, которые нужно знать.

Симптом 17.1. После отключения поддержки ACPI появляется сообщение об ошибке

Если при первоначальной инсталляции Windows 2000 в системе BIOS вашего компьютера опция ACPI находилась в активном состоянии, то после ее отключения во время запуска Windows 2000 на синем экране появляется следующее сообщение об ошибке:

```
0x00000079 (0x00000004, 0x0000AC31, 0x00000000, 0x00000000)
```

Эта ошибка появляется потому, что для поддержки ACPI Windows 2000 использует отдельный уровень HAL (Hardware Abstraction Layer — уровень аппаратных абстракций). Если вы хотите отключить поддержку ACPI после установки Windows 2000, то операционную систему надо переустановить и при этом интерфейс ACPI в системе BIOS компьютера должен быть отключен. Так как в реестре и системных файлах производится множество изменений, установка обновления невозможна.

Симптом 17.2. Система не может перейти в спящий режим

Спящий режим — это специальная разновидность режима пониженного энергопотребления, при которой все текущее состояние системы сохраняется на зарезервированной области жесткого диска и восстанавливается при пробуждении. Не все компьютеры стандарта ACPI поддерживают спящий режим. На тех компьютерах, которые обеспечивают его поддержку, драйвер ACPI осуществляет проверку каждого устройства с целью определения самого низкого поддерживаемого им состояния пониженного энергопотребления. Затем для каждого устройства драйвер ACPI выявляет самое низкое состояние пониженного энергопотребления, которое реагирует на событие пробуждения. Если уровень пробуждения данным устройством не поддерживается, драйвер ACPI предполагает, что оно прореагирует на него сообщением о "неопределенности". При попытке ввести компьютер на базе Windows 2000 в ждущий или спящий режим может появиться следующее сообщение об ошибке:

```
The system cannot go to standby mode because the driver
(компьютер не может перейти в спящий режим, поскольку драйвер)
<диск>\<имя драйвера устройства>
failed the request to standby.
(отказал в запросе на переход в спящий режим).
```

Компьютер может перейти в спящий режим лишь в том случае, если поддержка этого режима обеспечивается всеми входящими в его состав устройствами. Как правило, некачественные драйверы устройств или устройства, некорректно отвечающие на запросы ACPI, тем не менее, пытаются войти в спящий режим. Когда устройство не отвечает на запрос об изменении режима ACPI, появляется сообщение об ошибке.

Эта неисправность может возникнуть, если драйвер устройства не соответствует требованиям стандарта ACPI. Если же само устройство несовместимо с ACPI, вам следует связаться с его производителем для получения его исправления или обновления. Подобная неисправность может возникнуть, если драйвер устройства не поддерживает уровень пониженного энергопотребления, достаточный для перехода в спящий режим. Это может быть вызвано множеством факторов, включая устаревшие драйверы устройств или установку в Windows 2000 драйверов для Windows 4.0. Убедитесь в том, что в вашей системе установлен наиболее современный драйвер для Windows 2000 и проверьте, действительно ли рассматриваемое устройство обеспечивает достаточную поддержку спящего режима.

Симптом 17.3. Невозможно отключить монитор средствами Power Options

В диалоговом окне **Power Options** (Электропитание) в системе Windows 2000 опция **Turn Off Monitor** (Отключение дисплея) отсутствует. Такая ситуация может сложиться в том случае, если ваш видеоадаптер и его драйвер не поддерживают управление питанием на основе ACPI. Драйвер видеоадаптера должен быть совместимым с ACPI и обеспечивать полное соответствие методов управления, которые считывают-

ся файлом ACPI.SYS для формирования опций, отображаемых в диалоговом окне **Power Options**. К примеру, подобного рода трудности могут возникнуть при использовании устаревшего драйвера видеоадаптера, а также в случае некорректной реализации блока описаний ACPI Control Method.

Чтобы устранить эту неисправность, вам следует связаться с производителем видеоадаптера и узнать о наличии специального драйвера этого устройства для Windows 2000 (лучше выбрать драйвер, который поддерживает все функции управления питанием в ACPI).

Симптом 17.4. Компьютер игнорирует настройки таймера ожидания в Windows 2000

При задании настроек таймера ожидания в диалоговом окне **Power Options** (Электропитание) они могут вступить в силу. Но вполне возможно, что выйти из экономичного режима у вас получится только путем отключения питания компьютера с его последующим немедленным возобновлением; при этом могут появляться ошибки деления на ноль. Компьютерам, соответствующим спецификации ACPI, требуются отдельные часы реального времени, которые применяются для регулирования событий, связанных с управлением питанием. Этот таймер (аппаратное устройство на материнской плате) определяет время приостановления и возобновления работы отдельных компонентов компьютера. Если система BIOS скомпонована некорректно, операционная система может проигнорировать показания этого таймера, в результате чего возникнут сбои. Часто они обуславливаются дефектом системы BIOS интерфейса ACPI. Чтобы устранить эту неисправность, свяжитесь с производителем компьютера для получения обновленной версии BIOS для вашей системы.

Симптом 17.5. Хранители экрана OpenGL препятствуют переходу системы в ждущий режим

При включении на компьютере с Windows 2000 заставки OpenGL совместно с функцией системного ожидания (System Standby) при использовании интерфейса APM компьютер может не перейти в ждущий режим. Так происходит в том случае, если заставка OpenGL запускается до перехода в ждущий режим. Дело в том, что ACPI переводит компьютер в ждущий режим только по прошествии определенного периода бездействия процессора. При запуске заставки OpenGL процессор начинает работать, и таймер ACPI, связанный с переходом в ждущий режим, переустанавливается. Избежать такой ситуации можно путем отключения заставок OpenGL.

Симптом 17.6. Не удается отключить управление прерываниями на компьютере с ACPI

В системе Windows 2000 с поддержкой ACPI **Device Manager** (Диспетчер устройств) не поддерживает функцию отключения управления прерываниями. В среде Windows 2000 на компьютере, не поддерживающем спецификацию ACPI, отключение управления IRQ позволяет устранить неисправности, возникающие при загрузке некоторых устройств. Часто при необходимости воспользоваться управлением прерываниями пользователь обнаруживает, что в Windows 2000 установлены старые драйверы, предназначенные для Windows NT 4.0. Вероятно, эти трудности исчезнут, когда производители выпустят версии ACPI BIOS, полностью согласованные с Windows 2000. Как правило, эта неисправность имеет отношение к BIOS, так что для ее

разрешения вам следует обратиться к производителю материнской платы или компьютера для получения обновленной версии BIOS, совместимой с ACPI.

Примечание

На компьютерах, поддерживающих стандарт ACPI в среде Windows 2000, управление прерываниями не требуется.

Симптом 17.7. В среде Windows 2000 происходит сброс установок даты и времени при каждой загрузке

После установки системы Windows 2000 и ее перезагрузки на экране может появиться сообщение о недействительности системной даты и времени. К примеру, может быть принята дата 1 января 1601 года (или другой неверный вариант), а часы могут вести отсчет с 12:00. Если вы переустановите дату и время, а затем загрузите другую операционную систему (например, Windows NT или Windows 9x), установленные дата и время сохранятся. В случае возврата в Windows 2000 произойдет то же самое. Эта ошибка может возникнуть тогда, когда система BIOS компьютера не полностью совместима с ACPI. Дело в том, что Windows 2000 — это единственная операционная система, которая полагается на записи ACPI BIOS. Свяжитесь с производителем компьютера для получения обновления BIOS, которое нужно установить, следуя инструкциям производителя.

Другим способом устранения этой неисправности является переустановка Windows 2000 без поддержки ACPI. Для этого во время первого этапа инсталляции (на экране **Setup is inspecting your computer's hardware configuration** — Программа установки проверяет аппаратную конфигурацию) нужно нажать клавишу <F7>. Этим вы заставите программу установки (Setup) назначить уровень HAL, не связанный с ACPI.

Симптом 17.8. В Windows 2000 появляется ошибка STOP 0x9F

Работая в операционной системе Windows 2000, вы можете столкнуться с сообщением об ошибке "STOP 0X0000009F DRIVER_POWER_STATE_FAILURE". Эта ошибка возникает в случае, если драйверы некорректно обрабатывают запросы об изменении режима энергопотребления. Чаще всего это сообщение об ошибке появляется во время одного из следующих действий:

- прекращение работы;
- вход или выход из ждущего режима;
- вход или выход из спящего режима.

Чтобы не допустить появления этого сообщения, обновите или удалите конфликтующий драйвер. Впрочем, эта неисправность может быть вызвана не только драйверами устройств — она может быть связана и с фильтрующими драйверами файловой системы (к примеру, драйверы, установленные программами защиты от вирусов, удаленного управления или резервирования). Чтобы изолировать драйвер, вызывающий появление этой ошибки, сделайте следующее.

1. Проверьте, присутствует ли ваш компьютер и все его компоненты в списке совместимого оборудования HCL (Hardware Compatibility List); убедитесь в том, что драйверы подписаны и сертифицированы лабораторией по сертификации аппа-

ратных средств для работы в Windows (WHQL, Windows Hardware Qualification Laboratory).

2. Проверьте наличие обновлений драйверов для вашего аппаратного обеспечения.
3. Обновите программное обеспечение, использующее драйверы с фильтрацией (например, антивирусную программу).
4. Удалите все второстепенные устройства и программы — так вы сможете локализовать аппаратное/программное обеспечение, которое является источником сбоя.
5. Установите Windows 2000 в новый каталог. Начните добавлять по одному драйверу, пока не выясните, какой из них служит источником сбоя.

Симптом 17.9. Появляются сбои при сохранении данных в системе Windows 2000, работающей от аккумулятора

Если компьютер полностью теряет источник питания или в течение длительного времени простаивает, несохраненные текущие данные могут быть потеряны. К аналогичному результату может привести сбой системы, из-за которого компьютер отключается при работающих программах с несохраненными данными. Это происходит также, если компьютеры находятся в ждущем режиме, в течение длительного времени работая от аккумулятора, который впоследствии истощается, в результате чего происходит отключение системы. Наконец, это может случиться, если система Windows 2000 не поддерживает пробуждение при малом заряде аккумулятора или события, связанные с пробуждением при работе от аккумулятора. Для того чтобы избежать потери несохраненных текущих данных в случае нарушения энергоснабжения компьютера, сбоя системы или перехода в режим энергосбережения, примите во внимание следующие рекомендации.

- ❒ Регулярно сохраняйте текущие данные.
- ❒ Сохраняйте данные, прежде чем отлучиться от компьютера.
- ❒ Сохраняйте данные, прежде чем переходить в ждущий или спящий режим.
- ❒ Сохраняйте данные, прежде чем отлучиться от компьютера, поддерживающего управление питанием.
- ❒ Настройте функции управления питанием компьютера на применение спящего режима.
- ❒ Используйте первое временное событие, связанное с простоем системы, для перехода к спящему режиму.
- ❒ Настройте аварийные сигналы системного аккумулятора на вхождение в спящий режим (если это возможно).

Симптом 17.10. В стандартном режиме VGA функции управления питанием недоступны

При выключении компьютера или применении утилиты управления питанием панели управления в среде Windows 2000 функции вхождения в ждущий и спящий режим оказываются недоступными. Подобные трудности возникают в том случае, если в компьютере применяется видеодрайвер VGA. Такой драйвер обеспечивает работу лишь основных функций вывода изображения. Драйверы VGA не поддерживают управление питанием. Эти функции зависят от применяемой видеокарты. Чтобы

сделать возможным вхождение в ждущий или спящий режим, вам необходимо установить соответствующий видеодрайвер.

Симптом 17.11. При использовании SYSPREP система зависает

После запуска SYSPREP в среде Windows 2000 с целью создания основной копии жесткого диска может произойти полный отказ системы, сопровождающийся пустым экраном, причем это происходит в компьютере с задействованным интерфейсом ACPI. Чтобы устранить эту неисправность, установите последний служебный пакет для Windows 2000. В английской версии должны быть следующие (или более свежие) атрибуты файла:

```
04/07/2000 04:47p 5.0.2195.2020 45,840 Sysprep.exe
```

Симптом 17.12. Компьютер зависает при работе в режиме ACPI

Если ваш компьютер на базе Windows 2000, работающий в режиме ACPI, в качестве счетчика с высоким разрешением использует таймер управления питанием ACPI (PMTimer, Power Management Timer), есть вероятность появления любой из следующих неисправностей:

- при воспроизведении звуковых или видеопотоков появляются сбои и ухудшается производительность;
- на синем экране появляется сообщение об ошибке, после чего происходит полный отказ системы.

Вероятно, в вашей системе установлен набор микросхем, который заставляет PMTimer действовать так, чтобы течение времени казалось обратным. В компьютерах на базе Windows 2000 к подобным сбоям приводит применение следующих наборов микросхем:

- VIA;
- SIS;
- ALI;
- RCC.

Чтобы исключить такие сбои, установите Windows 2000 Service Pack 1 или более современную версию.

Симптом 17.13. Windows 2000 использует IRQ6 даже при отсутствии контроллеров гибких дисков

Windows 2000 пытается установить прерывания IRQ6, которые обычно резервируются для контроллеров гибких дисков. Так происходит даже в том случае, когда контроллер гибких дисков не предусмотрен системой BIOS, или флоппи-дисковод физически отсутствует. Если отключить контроллер гибких дисков через **Device Manager** (Диспетчер устройств), а затем открыть вкладку **Resources** (Ресурсы) его системных свойств, вы сможете увидеть следующее сообщение:

```
The Device is not using any resources
(Устройство не использует какие-либо ресурсы,)
because it is not currently enabled
(поскольку в настоящее время недоступно)
```

Если воспользоваться инструментом **Computer Management** (Управление компьютером) на панели управления и последовательно выбрать **System Information** (Сведения о системе), **Hardware Resources** (Ресурсы аппаратуры), а затем указать соответствующие прерывания для просмотра их ресурсов, то в установках IRQ6 не будет сказано об его использовании. Впрочем, если попытаться настроить другое устройство ISA на применение IRQ6, вы получите сообщение о том, что данный ресурс уже используется. Дело в том, что системы на базе x86, не поддерживающие ACPI, но применяющие Plug-and-Play BIOS, всегда сообщают о наличии контроллера гибких дисков. В системах стандарта ACPI в файле ACPI.SYS указаны контроллеры гибких дисков из таблиц BIOS, которые передаются в операционную систему (в этом файле сообщается только об установленных устройствах).

Чтобы устранить эту неисправность, обновите BIOS до версии, соответствующей спецификации BIOS. Если система BIOS на базе ACPI уже используется, внесите в нее изменения, необходимые для того, чтобы она не сообщала о контроллере гибких дисков при его отсутствии (отключите контроллер гибких дисков с помощью CMOS Setup). Свяжитесь с производителем вашей системы для получения обновления BIOS. При использовании BIOS на базе ACPI следует удалить аппаратный узел PNP0700 из таблиц ACPI — после этого сообщений о гибком диске, вероятно, не последует.

Симптом 17.14. Не удается обнаружить немаскируемое прерывание в многопроцессорной системе с поддержкой ACPI

Немаскируемое прерывание (NMI, Nonmaskable Interrupt) может не распознаваться в многопроцессорных системах, работающих на базе Windows 2000 с поддержкой ACPI. Эта неисправность может стать результатом того, что процессоры в соответствующих разъемах расположены не подряд (не последовательно). Все дело в Windows 2000. В качестве альтернативного варианта попробуйте перегруппировать процессоры, установив их в смежные разъемы. В настоящее время существует подтвержденное исправление от Microsoft, но оно предназначено исключительно для устранения рассматриваемой здесь неисправности и должно применяться только при ее наличии. У английской версии этого исправления должны быть следующие (или более свежие) атрибуты файла:

```
2/19/2001 05:12p 5.0.2195.3273 81,760 Halaacpi.dll
2/19/2001 05:12p 5.0.2195.3273 82,656 Halmacpi.dll
```

Симптом 17.15. В системе Windows 2000 с поддержкой ACPI появляется ошибка STOP 0xA

Эта ошибка может обнаружиться по прошествии некоторого периода применения драйвера ACPI в среде Windows 2000 SP1. К примеру, ошибка STOP 0x0000000A может появиться после установки драйвера термоконтроллера материнской платы, если это устройство не полностью соответствует стандарту ACPI. Дело в том, что встроенный драйвер контроллера ACPI (ACPIEC.SYS) способен обращаться к драйверу устройства многократно. Если устройство не полностью соответствует стандарту ACPI, эти обращения могут инициировать появление сообщения об ошибке STOP. Эта проблема связана с Windows 2000. Чтобы исправить ее, нужно загрузить и установить последнюю версию служебного пакета для Windows 2000.

Симптом 17.16. Происходит полный отказ системы с набором микросхем OSB4

Если на компьютере с набором микросхем OSB4 от Reliance Computer Corp./ServerWorks, работающем на базе Windows 2000 (SP1 или SP2) в режиме ACPI в качестве счетчика с высоким разрешением применяется таймер управления питанием ACPI, то могут возникнуть следующие неисправности:

- при воспроизведении звуковых или видеопотоков появляются трудности и ухудшается производительность;
- на синем экране появляется сообщение об ошибке, после чего происходит полный отказ системы.

В вашей системе, скорее всего, установлен набор микросхем, который заставляет таймер управления питанием действовать так, чтобы течение времени казалось обратным. Чтобы проверить, действительно ли на вашем компьютере установлен такой набор микросхем, сделайте следующее:

1. Последовательно выберите **Start** (Пуск), **Settings** (Настройка), **Control Panel** (Панель управления).
2. Двойным щелчком выберите пиктограмму **System** (Система).
3. На вкладке **Hardware** (Оборудование) нажмите кнопку **Device Manager** (Диспетчер устройств).
4. Двойным щелчком выберите **System Devices** (Системные устройства).
5. Найдите устройство PCI-to-ISA Bridge. Это устройство должно содержать описание с обозначением набора микросхем.

Рассматриваемая неисправность устраняется с помощью реестра.

Примечание

Неверное редактирование реестра может привести к серьезным сбоям, вплоть до необходимости переустановки операционной системы. Прежде чем вносить в реестр какие-либо изменения, его следует зарезервировать. В среде Windows NT и Windows 2000 нужно обновить диск аварийного восстановления системы (ERD, Emergency Repair Disk).

1. Вы должны работать в системе Windows 2000 SP1 или в более поздней версии (возможно, прежде чем продолжать, вам нужно обновить Windows 2000).
2. Запустите редактор реестра (REGEDT32.EXE).
3. Найдите и щелкните следующий ключ реестра:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\HAL
```

4. Откройте меню **Edit** (Редактировать) и выберите **Add Value** (Добавить значение); затем добавьте следующее значение:

```
Value name: 11660200
Data type: RED_DWORD
Data: 00000001
```

5. Закройте редактор реестра и перезагрузите компьютер.

Источники бесперебойного питания

Работа сети подразумевает беспрерывную работу серверов, рабочих станций и других устройств. Во многих случаях оборудование функционирует постоянно за счет подачи питания через сеть общего пользования (т. е. переменного тока через розетку). К сожалению, подача электропитания не постоянна — время от времени происходят нарушения типа падения, резких скачков и перепадов напряжения и полного отключения питания. Нарушение электроснабжения может привести к ошибочной работе сервера или к перезагрузке. В худшем случае сбои, связанные с электропитанием, могут стать причиной повреждения данных и даже выхода из строя сетевого оборудования. *Источник бесперебойного питания* (UPS, Uninterruptible Power Supply) — это устройство, которое отвечает за обеспечение энергоснабжения в условиях подобных нарушений (рис. 17.5). Источник бесперебойного питания (ИБП) устанавливается на кабеле между розеткой и компьютерным оборудованием, которое предполагается защитить. При сбое в системе энергоснабжения ИБП переключается на аккумуляторный источник питания, который обеспечивает работу оборудования — по крайней мере, на период, достаточный для сохранения данных и штатного отключения. В большинстве случаев ИБП предусматривает защитную схему, которая не допускает влияния перепадов напряжения на компьютерное оборудование.

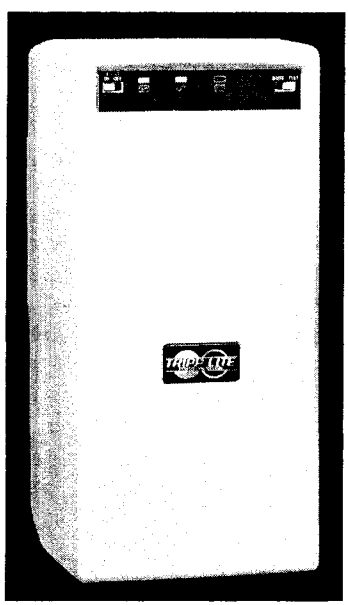


Рис. 17.5. Источник бесперебойного питания Tripp Lite BCPro 600 (публикуется с разрешения Tripp Lite)

Введение

Существует два основных типа ИБП: оперативные (Online) и автономные или интерактивные (Offline, Interactive). *Оперативным ИБП* называют систему, в которой ин-

вертер (схема, которая преобразует постоянный ток в переменный) функционирует постоянно и подает питание на компьютерное оборудование. В результате компьютер постоянно питается от аккумулятора, даже когда переменный ток присутствует и поддерживает заряд аккумуляторов ИБП. Переменный ток, поступающий из розетки, преобразуется в постоянный ток, который и обеспечивает заряд аккумуляторов; затем постоянный ток, накапливаемый в аккумуляторе, преобразуется обратно в переменный, на основе которого и работает компьютерное оборудование. Такие ИБП часто называют системами двойного преобразования, при этом и напряжение, и частота поддаются регулировке. Второй тип оперативных ИБП стал популярен к 1990 г. Такие устройства называют ИБП однократного преобразования, дельта-преобразования или параллельными оперативными системами. В устройствах этого типа только часть выходной мощности проходит через преобразование переменного тока в постоянный, и обратно.

Для сравнения, *автономный ИБП* работает (поставляет электроэнергию от аккумулятора), только если источник переменного тока недоступен. Такие ИБП традиционно обозначаются как системы аккумуляторного резервирования или дежурные ИБП. Когда переменный ток исчезает, в рабочее состояние вступает инвертер ИБП — он обеспечивает работу компьютерного оборудования исключительно за счет заряда аккумулятора. ИБП такого типа немного проще проектировать и обслуживать, но в них могут появляться проблемы, связанные с аккумуляторами — дело в том, что часто они оказываются слишком разряженными и не способными обеспечить нагрузку подключенного компьютера. При выполнении типичных задач дежурный ИБП применяется для защиты менее критичных нагрузок на протяжении небольших периодов времени (т. е. для рабочих станций).

Линейные интерактивные ИБП являются существенным шагом вперед по сравнению с дежурными ИБП, т. к. они способны корректировать скачки напряжения без помощи аккумуляторов. За счет функции повышения напряжения, которая помогает поднять уровень подачи полезного напряжения, или функции компенсирования, снижающей входящее напряжение, линейный интерактивный ИБП откладывает начало применения аккумулятора до того момента, когда напряжение начинает существенно превосходить допустимые пределы. Линейный интерактивный ИБП, как правило, имеет дисплей, на котором отображается процент загрузки, заряд аккумулятора, а также другие данные. Такие устройства помогут справиться практически с любой критической нагрузкой.

Примечание

Работа ИБП почти всегда основана на аккумуляторах. В некоторых расширенных системах ИБП предусматриваются генераторы с бензиновым источником питания — именно они отвечают за заряд аккумулятора и обеспечивают значительное увеличение длительности работы.

Время передачи

Большинство автономных ИБП отвечают не мгновенно. Для того чтобы обнаружить потерю подачи переменного тока, запустить инвертер и убедиться в том, что резервное электропитание поддерживается всем компьютерным оборудованием, требуется некоторое время. Это время отклика называется *временем перехода*, его значение зависит от конкретной модели ИБП. Довольно часто время перехода составляет от 3

до 13 мс. Общей границей этого параметра для компьютерного оборудования является значение 7 мс — это значит, что компьютерное оборудование (и другие устройства с критической нагрузкой) может дать сбой или неожиданно перезагрузиться лишь в том случае, если отключение переменного тока по времени превышает 7 мс. Если вам нужно обеспечить очень быстрое время перехода (приближающееся к 0 мс), попробуйте воспользоваться оперативным ИБП.

Взаимодействие

Потеря мощности обычно считается критическим отказом, а аккумуляторы не могут обеспечивать питание компьютерного оборудования бесконечно. Это значит, что даже самый лучший ИБП — это просто устройство подстраховки, которое позволяет выиграть несколько дополнительных минут работы системы, которые используются для штатного сохранения файлов и отключения компьютера. К сожалению, нет никакой гарантии, что во время потери мощности рядом с компьютером окажется технический специалист или администратор, который сможет выполнить отключение системы. Большинство современных ИБП имеют встроенный контроллер, который отслеживает уровни мощности и взаимодействует с подключенным компьютерным оборудованием (обычно это взаимодействие осуществляется через последовательный кабель). Когда происходит потеря мощности и система начинает работать от ИБП, он может отправить компьютеру сигнал о необходимости запуска автоматического процесса отключения. Для этого необходимо последовательное соединение между компьютером и ИБП, а также определенное клиентское программное обеспечение, способное отслеживать состояние ИБП. Возможен даже вариант отправки соответствующего извещения сетевому администратору (посредством электронной почты или на пейджер). Если при активном состоянии ИБП питание возобновится, ИБП оповестит об этом пользователей и прервет процесс отключения.

Продолжительность работы

Очевидно, что аккумуляторы, которыми оснащен ИБП, не могут бесконечно осуществлять питание. Это означает, что ИБП может питать лишь некоторые компоненты оборудования в течение ограниченного промежутка времени. Точная продолжительность этого периода времени зависит от нагрузки (количества оборудования), подключенной к ИБП, и размера (емкости) самого ИБП. В отношении ИБП произвольной емкости действует правило, в соответствии с которым чем выше нагрузка, тем меньше продолжительность работы. Уменьшение нагрузки (или применение ИБП большей емкости) приводит к увеличению продолжительности работы. Сложнее всего вычислить предполагаемую продолжительность работы исходя из нагрузки, которую вы намереваетесь подключить.

Все ИБП оцениваются в вольт-амперах (ВА) — это специальная единица измерения мощности (которая также измеряется в ваттах, Вт). Требования вашего оборудования, касающиеся мощности, должны быть меньше или равны ВА-емкости вашего ИБП. К примеру, ИБП модели IBM OfficePro 700 имеет емкость 700 ВА. ВА-емкость обычно подразумевает, что питание будет подаваться на указанном уровне в течение 8—10 мин. Следовательно, ИБП емкостью 700 ВА может питать компьютерное оборудование с суммарной мощностью 700 ВА около 10 мин. Если мощность нагрузки в два раза меньше (350 ВА), ИБП будет работать в два раза дольше (т. е. 16—20 мин.). При использовании четверти нагрузки (175 ВА) ИБП должен работать

в четыре раза дольше (т. е. 35—40 мин.) и т. д. На практике, фактическая продолжительность работы будет немного больше, если нагрузка в значительной степени меньше, чем емкость ИБП (т. е. емкость ИБП оценивается с учетом нагрузки).

Определить подключаемую к ИБП нагрузку довольно сложно. Все производители компьютерного оборудования сопровождают свои устройства указанием максимально допустимой нагрузки. Это значение обычно приводится на паспортной табличке или на наклейке, помещаемой рядом с сетевым шнуром на задней плоскости устройства. Значение может приводиться в вольт-амперах (ВА), ваттах (Вт) или в амперах (А). В идеале, все нагрузки следует обозначать в вольт-амперах, чтобы их можно было складывать. Если нагрузка указывается в ваттах, то преобразование ее в вольт-амперы производится по формуле $W \times 1{,}4$. Если нагрузка обозначена в амперах, то ее можно перевести в вольт-амперы, умножив на 120 (для устройства на 120 В) или на 230 (для устройства на 230 В). Предположим, что вы хотите подключить ИБП к монитору, компьютеру и лентопротяжному устройству. Приведем пример такого вычисления.

Компьютер, ВА	=	120 В × 2 А	=	240 ВА
Монитор, ВА	=	100 Вт × 1,4	=	140 ВА
Лентопротяжное устройство, ВА	=	120 В × 1 А	=	120 ВА
Итого				**500 ВА**

На примере становится ясно, что ИБП с емкостью 500 ВА будет питать этот комплект оборудования на протяжении 8—10 мин., ИБП с емкостью 1000 ВА — около 20 мин. В табл. 17.1 приводится сравнение нормативных нагрузок и продолжительности работы для некоторых распространенных значений емкости ИБП.

Таблица 17.1. *Сравнение продолжительности работы ИБП в зависимости от нагрузки*

Нагрузка	250 ВА	400 ВА	450 ВА	600 ВА	900 ВА	1250 ВА
50 ВА	37 мин.	100 мин.	120 мин.	145 мин.	220 мин.	270 мин.
75 ВА	29 мин.	72 мин.	88 мин.	105 мин.	155 мин.	210 мин.
100 ВА	23 мин.	47 мин.	65 мин.	79 мин.	110 мин.	160 мин.
150 ВА	14 мин.	30 мин.	41 мин.	54 мин.	83 мин.	115 мин.
200 ВА	8 мин.	19 мин.	32 мин.	41 мин.	65 мин.	92 мин.
250 ВА	5 мин.	13 мин.	24 мин.	31 мин.	47 мин.	75 мин.
300 ВА	—	9 мин.	18 мин.	22 мин.	40 мин.	64 мин.
350 ВА	—	7 мин.	14 мин.	17 мин.	35 мин.	54 мин.
400 ВА	—	5 мин.	11 мин.	13 мин.	29 мин.	46 мин.
450 ВА	—	—	8 мин.	10 мин.	24 мин.	40 мин.
500 ВА	—	—	—	7 мин.	20 мин.	34 мин.

Таблица 17.1 (окончание)

Нагрузка	250 ВА	400 ВА	450 ВА	600 ВА	900 ВА	1250 ВА
550 ВА	—	—	—	6 мин.	17 мин.	29 мин.
600 ВА	—	—	—	5 мин.	15 мин.	25 мин.
700 ВА	—	—	—	—	13 мин.	22 мин.
800 ВА	—	—	—	—	11 мин.	17 мин.
900 ВА	—	—	—	—	10 мин.	13 мин.
1000 ВА	—	—	—	—	—	10 мин.
1250 ВА	—	—	—	—	—	9 мин.

Примечание

Ни в коем случае не подключайте к ИБП лазерные принтеры! Среднестатистический лазерный принтер потребляет намного больше мощности, чем другие периферийные компьютерные устройства, и может расцепить защитный автоматический выключатель системы ИБП. Подключайте лазерные принтеры к высококачественному ограничителю перенапряжений. При возобновлении питания задания на печать всегда можно вновь поставить в очередь.

Критерии выбора ИБП

Следующие вопросы помогут сетевому администратору определить, какой ИБП лучше других соответствует потребностям сети.

- ❒ Отвечает ли данный ИБП номинальным потребляемым мощностям сети?
- ❒ Сколько компонентов он может питать (количество розеток)?
- ❒ Оповещает ли он сервер о нарушении энергоснабжения и о том, что он питается от аккумуляторов?
- ❒ Поддерживает ли ИБП механизмы защиты от перепадов напряжения?
- ❒ Каков срок службы аккумулятора ИБП?
- ❒ Как долго ИБП может находиться в неактивном состоянии, прежде чем его аккумуляторы начинают портиться?
- ❒ Предупреждает ли ИБП администратора и пользователей о разрядке аккумулятора?

Установка ИБП

Процесс установки ИБП, без сомнения, не является ни сложным, ни трудоемким, но все же здесь можно выделить несколько этапов, которые могут помочь рационализировать этот процесс. В руководстве по эксплуатации ИБП должны приводиться подробные инструкции, а общее руководство представлено ниже.

1. *Подключите коннектор аккумулятора.* Во многих случаях ИБП поставляется так, что аккумулятор находится в отключенном состоянии (часто это делается для то-

го, чтобы обеспечить сохранность оборудования во время его транспортировки). Прежде чем предпринимать следующие действия, аккумулятор необходимо подключить.

2. *Подключите оборудование и электропитание к ИБП.* Подключите оборудование к розеткам ИБП. Подключайте ИБП только к двухполюсной трехпроводной электрической розетке с заземляющим контактом. Избегайте применения удлинителей и штепселей-переходников.
3. *Включите и протестируйте ИБП.* Прежде чем включать ИБП, убедитесь в том, что к нему подключен аккумулятор. Чтобы включить ИБП, нажмите кнопку питания, расположенную на его передней панели, — в результате произойдет включение подсоединенного оборудования (переключатели питания этого оборудования должны быть приведены в положение ON). Во включенном состоянии ИБП осуществляет подзарядку своего аккумулятора. Полная зарядка аккумуляторов производится в течение первых нескольких часов работы в нормальном режиме. В ходе этого первоначального периода зарядки достичь полной продолжительности работы от батареи вам, вероятно, не удастся. ИБП выполняет автоматическое самотестирование при включении, а также через каждые последующие две недели (по умолчанию). Проверьте состояние индикатора ошибочной электропроводки узлов, расположенного на блоке ИБП. Он сигнализирует в случае, если ИБП подключен к неверно смонтированной штепсельной розетке источника переменного тока. Среди дефектов электропроводки встречаются отсутствие заземления, поменянные местами фазовый и нейтральный провод, а также перегрузка нейтрали. При обнаружении дефекта необходимо пригласить квалифицированного электрика.
4. *Установите дополнительное программное обеспечение и оборудование.* Вы можете включить последовательный кабель между ИБП и компьютером (при наличии соответствующего оборудования), а также утилиты питания, необходимые для надлежащего управления компьютером в случае сбоя питания.

Примечание

Для получения специальных инструкций по установке необходимо обратиться к руководству по эксплуатации.

Значение светодиодов

В большинстве ИБП имеется ряд светодиодов, применяемых для обозначения состояния питания, оставшегося заряда, критических ошибок и т. п. (рис. 17.6). При подключении любого ИБП необходимо разобраться в тех светодиодах, которые на нем установлены.

Примечание

Не все ИБП имеют одинаковый набор светодиодов. Более подробную информацию об индикаторах конкретного ИБП вы сможете найти в его документации.

Нагрузка

Индикатор из пяти светодиодов в левой части передней панели показывает процент доступного питания, используемый подключенным оборудованием (т. е. дает сведе-

ния о нагрузке). К примеру, если сигнализируют три светодиода, подключенная нагрузка занимает от 50 до 67% емкости ИБП. Если сигнализируют все пять светодиодов, подключенная нагрузка занимает от 85 до 100% емкости. Чтобы исключить перегрузку ИБП, необходимо тщательно протестировать всю систему. ИБП поддерживает заряд аккумулятора только при условии подключения к источнику переменного тока (и при наличии штатного напряжения).

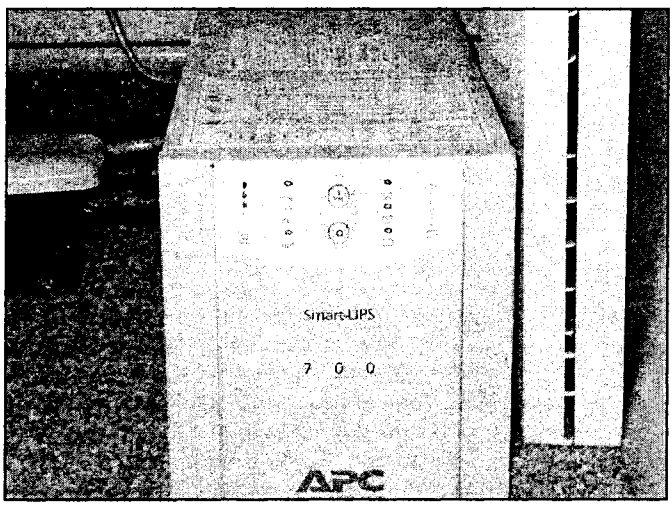


Рис. 17.6. ИБП типа APC Smart UPS имеют комплект светодиодов, которые оповещают о линейном напряжении, оставшемся заряде аккумулятора, аварийных ситуациях и т. п.

Самотестирование

При включении ИБП (а также каждые две недели) он проводит автоматическое самотестирование. Вы можете изменить принимаемый по умолчанию интервал между самотестированием. Автоматическое самотестирование облегчает требования по сопровождению, исключая необходимость в периодических ручных проверках. В ходе самотестирования ИБП в течение непродолжительного времени питает подключенное оборудование от аккумуляторов. Если самопроверка проходит успешно, ИБП возвращается к нормальному режиму работы. Если самотестирование заканчивается неудачей, ИБП сигнализирует светодиодом замены аккумулятора и немедленно возвращается к работе. Неудачный исход тестирования не оказывает никакого влияния на подключенное оборудование. Проведите 24-часовую подзарядку аккумулятора и самотестирование еще раз. Если и в этот раз оно не будет успешным, аккумулятор придется заменить.

Энергоснабжение

Во время нормальной эксплуатации ИБП следит за энергоснабжением и поставляет его подключенному оборудованию. Если в вашей системе наблюдаются чрезмерно длительные периоды повышенного или пониженного электропитания, пригласите электрика для поиска электрических дефектов в сети. Если неисправность сохранится, то вам придется воспользоваться другим источником электроснабжения.

Оперативный режим

Индикатор оперативного режима сигнализирует тогда, когда ИБП поставляет подключенному оборудованию штатное электропитание. Если индикатор перестает сигнализировать, значит, ИБП подключил аккумуляторное питание; в этом случае ИБП подает звуковые аварийные сигналы — по четыре сигнала каждые 30 сек.

Подводимое напряжение (120/230 В переменного тока)

Диагностические возможности ИБП позволяют ему определять подводимое напряжение. Подключите ИБП к обычному штатному источнику питания. Чтобы просмотреть график подводимого напряжения, нажмите и удерживайте соответствующую кнопку. Через несколько секунд на индикаторе, расположенном в правой части передней панели, будет показано входное напряжение. Для интерпретации отображаемых значений обращайтесь к схеме слева (значения в ИБП не приводятся). Частью этой процедуры является самотестирование ИБП. Его выполнение не оказывает воздействия на индикатор напряжения. На нем отображается напряжение, точное значение которого находится между значением в списке и следующим большим значением. К примеру, если светятся три светодиода, входное напряжение больше 114, но меньше 124 В. Если ни один светодиод не светится, но устройство ИБП подключено к работающей розетке переменного тока, линейное напряжение находится на крайне низком уровне. Если горят все пять светодиодов, линейное напряжение очень высоко; в этом случае необходима электротехническая экспертиза.

Понижение/повышение напряжения AVR

Светодиод понижения напряжения AVR указывает на то, что ИБП выполняет компенсацию высокого входного напряжения. Светодиод повышения напряжения AVR обозначает, что ИБП проводит компенсацию низкого входного напряжения.

Питание от аккумулятора

Если штатное питание пропадает, ИБП начинает подводить к подключенному оборудованию питание от своего внутреннего аккумулятора, ресурсы которого ограничены по времени. Во время питания от аккумулятора ИБП издает аварийные сигналы (по четыре сигнала каждые 30 сек.). Когда ИБП возвращается к работе в нормальном оперативном режиме, аварийное сигнализирование прекращается. Когда работает индикатор питания от аккумулятора, ИБП снабжает подключенное оборудование аккумуляторным питанием.

Подзарядка аккумулятора

Индикатор из пяти светодиодов, находящийся в правой части передней панели, демонстрирует текущий заряд аккумулятора ИБП в виде процента от его емкости. Когда светятся все пять светодиодов, аккумулятор полностью заряжен. По мере того как емкость аккумулятора убывает, светодиоды начинают гаснуть (сверху вниз). Предупреждением о низком заряде аккумулятора является мигание светодиодов и аварийные сигналы. Настройки предупреждения о низком заряде аккумулятора, принимаемые по умолчанию, можно изменить на задней панели устройства (или посредством дополнительного программного обеспечения управления питанием).

Перегрузка

В случае возникновения перегрузки (т. е. превышения подключенным оборудованием установленной максимальной нагрузки) ИБП издает продолжительный аварийный звуковой сигнал, а светодиод начинает светиться. Аварийная сигнализация продолжает работать вплоть до устранения перегрузки. ИБП продолжает подавать электропитание, находясь в оперативном режиме, пока не произойдет расцепление прерывателя; в то же время, в случае обрыва подачи штатного напряжения ИБП не сможет обеспечить питание от аккумуляторов. Чтобы устранить перегрузку, следует отключить от ИБП все несущественное оборудование. Если в режиме аккумуляторного питания перегрузка не прекращается, в целях предохранения от возможных повреждений ИБП отключает выходные мощности.

Замена аккумулятора

Если самотестирование ИБП оканчивается неудачей, в течение минуты он издает непродолжительные звуковые сигналы; при этом сигнализирует светодиод замены аккумулятора. Мигание этого светодиода указывает на то, что аккумулятор отключен. ИБП запускает аварийную сигнализацию каждые пять часов. Зарядите аккумулятор и через 24 часа запустите процедуру самотестирования еще раз — это позволит подтвердить состояние аккумулятора. Если аккумулятор успешно проходит самотестирование, аварийные сигналы прекращаются. В противном случае придется заменить аккумулятор.

Тестирование ИБП

После нескольких часов, в течение которых ИБП должен произвести зарядку аккумулятора, следует включить его питание и подсоединить компьютерное оборудование. Индикатор ИБП должен засветиться, а оборудование должно войти в нормальный режим работы. Чтобы протестировать работу ИБП, отключите его входной шнур (или нажмите и удерживайте переключатель Test/Alarm Disable) — так вы сможете имитировать полное отключение энергоснабжения. После этого ИБП должен немедленно перевести все подключенное оборудование на питание от своего внутреннего аккумулятора. В течение этого периода времени ИБП будет каждые несколько секунд издавать звуковой сигнал, напоминая вам о том, что оборудование питается от источника с ограниченным временем работы. Теперь возобновите энергоснабжение ИБП, подключив сетевой шнур (или отпустив контрольный выключатель Test). Убедитесь в том, что во время перехода с переменного тока на аккумуляторное питание и наоборот ваше оборудование работает без сбоев. Чтобы окончательно убедиться в полной работоспособности ИБП, проведите этот тест четыре или пять раз.

Если суммарная потребляемая мощность подключенного оборудования значительно превосходит емкость ИБП, тыловой прерыватель цепи ИБП может расцепиться, что свидетельствует о ситуации перегрузки. После расцепления прерывателя ИБП пытается справиться с нагрузкой с помощью своих внутренних аккумуляторов, но это может привести к непредвиденно малой продолжительности работы. Если перегрузка труднопреодолима, ИБП немедленно отключается и издает громкий звуковой сигнал, извещающий о перегрузке. Если это происходит во время теста, отключите ИБП и отсоедините от него все несущественное оборудование. Прерыватель цепи может быть восстановлен после устранения перегрузки.

Поддержка ИБП и Windows 2000

Применение ИБП особенно важно для серверов, т. к. внезапная потеря питания может привести к обрыву сетевого трафика и непредвиденной потере данных. Как правило, ИБП является ключевым компонентом обеспечения доступа к сети, а некоторые ИБП (например, модель APC Back-UPS Office UPS) способны взаимодействовать с сервером с помощью последовательного кабеля (рис. 17.7) и соответствующего программного обеспечения управления ИБП (например, APC PowerChute for Windows 2000). Такое соединение обеспечивает возможность автоматизированного, штатного отключения сервера при потере питания. Некоторые системы поддерживают ряд интеллектуальных функций — например, таких:

- проведение запланированных или незапланированных процедур самотестирования ИБП;
- планирование отключения или перезагрузки системы;
- регистрация данных;
- отправка оповещений по электронной почте или на пейджер (для администраторов или технических специалистов).

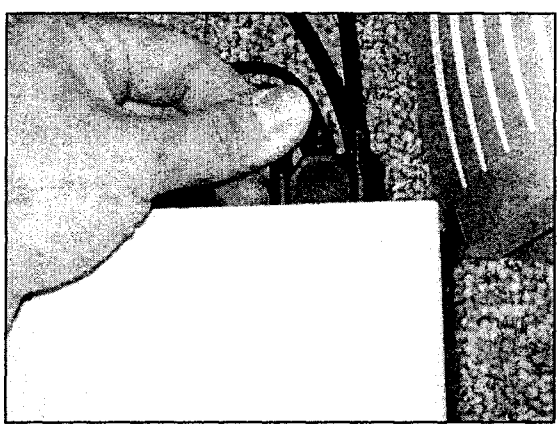


Рис. 17.7. ИБП с последовательным интерфейсом может автоматически тестировать или отключать сервер или персональный компьютер в случае нарушения энергоснабжения

После установки ИБП его последовательный порт нужно подключить к свободному последовательному порту сервера. Предназначенный для этих целей кабель поставляется в комплекте с ИБП. Затем необходимо настроить дополнительные средства управления; в Windows 2000 это делается с помощью Power Options. Откройте **Control Panel** (Панель управления) и дважды щелкните на пиктограмме **Power Options** (Электропитание). Найдите две вкладки: **Hibernate** (Спящий режим) и **UPS** (ИБП).

Примечание

Большинство ИБП поддерживает и другие операционные системы, включая Linux, NetWare, Solaris, OS/2 и др. Если вы работаете не в Windows 2000, для получения

инструкций по установке специального программного обеспечения и его настройке вам следует обратиться к руководству по инсталляции (или к документации от производителя данной операционной системы).

Hibernate (Спящий режим)

Вкладка **Hibernate** (Спящий режим) (см. рис. 17.4) является факультативной — она есть не на всех компьютерах. Если на вашем сервере есть аппаратное обеспечение, поддерживающее работу в спящем режиме (т. е. сохранение состояния системы на диск вместо ее полного отключения), и как минимум 128 Мбайт, вы можете установить флажок **Enable hibernate support** (Разрешить спящий режим) и нажать кнопку **Apply** (Применить). Таким образом, в случае длительных сбоев в подаче электропитания ИБП сможет перевести ваш сервер в спящий режим.

UPS

Вкладка **UPS** (ИБП) (рис. 17.8) содержит основные опции, необходимые для настройки устройства ИБП, к которому подключен ваш сервер. Нажмите кнопку **Select** (Выбор), выберите производителя (например, American Power Conversion), модель (например, Smart-UPS) и COM-порт, подключенный к ИБП (например, COM1). Чтобы завершить настройку и возвратиться на вкладку ИБП, нажмите кнопку **Finish** (Готово). Если вы включили поддержку спящего режима, нажмите кнопку **Configure** (Настройка) и для параметра **Next, instruct the computer to** выберите значение **Hibernate** (вместо **Shutdown**). После этого нажмите кнопку **Finish**, а затем **Apply**; тогда все изменения вступят в силу.

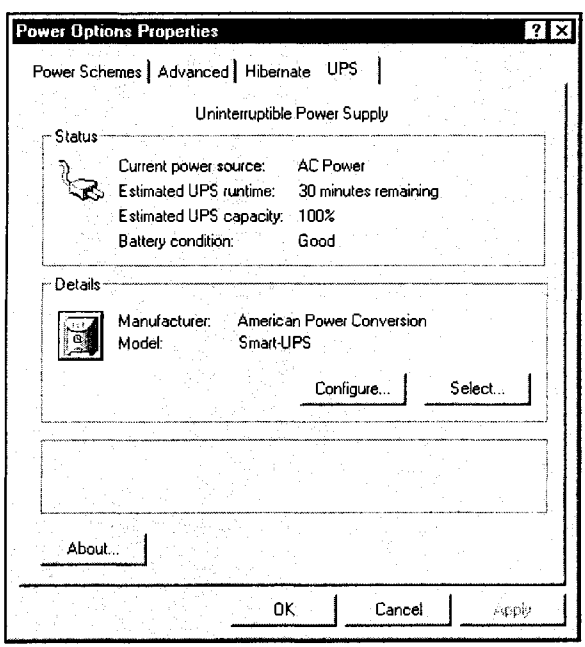


Рис. 17.8. Вкладка **UPS** позволяет настроить сервер на работу посредством ИБП

Обслуживание ИБП

Колебания и сбои в подаче электропитания от сети общего пользования способны помешать работе компьютера и могут приводить к отдельным отказам и перезагрузкам. Если это происходит на персональном компьютере, последствия оказываются довольно незначительными, чего не скажешь о сетевых серверах — для них такая ситуация может обернуться катастрофой. ИБП предназначен как раз для того, чтобы обеспечить продолжение работы сервера в случае перебоев с электропитанием. Вместо того чтобы подключать сервер непосредственно к розетке переменного тока, к ней подключается ИБП, а от него получает питание сервер (или другое периферийное оборудование). Если подача переменного тока прерывается на непродолжительный период времени, ИБП поддерживает постоянный уровень напряжения и предотвращает аварийные отказы сервера. Если же питание от источника переменного тока исчезает полностью, ИБП продолжает подводить питание на протяжении еще нескольких минут. Современные ИБП способны взаимодействовать с сервером так, что системный администратор узнает о событиях, связанных с подачей электропитания, а на компьютере запускается процесс штатного отключения системы.

Примечание

Большинство ИБП поддерживают применение аккумуляторов в качестве источников резервного питания; в то же время некоторые более сложные ИБП дополняют аккумуляторное питание бензиновым генератором, который обеспечивает работу сервера в течение нескольких часов.

Тестирование аккумулятора ИБП

Аккумуляторы — это электромеханические устройства. Следовательно, по прошествии определенного, хоть и достаточно большого, количества циклов зарядки/разрядки они изнашиваются и требуют замены. Как правило, менять аккумуляторы приходится каждые 3—5 лет нормальной эксплуатации. Долговечность аккумулятора также уменьшается под воздействием других факторов, включающих низкое качество источников питания от сети общего пользования, повышенная температура хранения, а также ошибки эксплуатации. Можно предположить, что аккумулятор выходит из строя, если он не держит заряд (т. е. короткая продолжительность работы и оповещения о низком заряде имеют место даже после длительной подзарядки). Внутренние диагностические средства ИБП, как правило, сообщают о неисправности аккумулятора по мере ее развития. К примеру, на блоке ИБП может начать сигнализировать индикатор работы аккумулятора, а на сервере о его неисправности оповещает программное обеспечение ИБП. Во многих случаях протестировать аккумуляторы можно самостоятельно с помощью следующей методики (для аккумуляторов +12 В постоянного тока).

- ❒ Убедитесь в надежности подключения ИБП, а также в том, что к нему подсоединено такое количество устройств, которое составляет по меньшей мере 50% общей нагрузки (системный блок настольного компьютера, монитор, сканер и т. д.).
- ❒ Включите систему и подключенные периферийные устройства, чтобы компьютер загрузился в нормальном режиме.
- ❒ Сымитируйте нарушение электропитания, выдернув сетевой шнур ИБП.

- Для измерения напряжения каждого аккумулятора воспользуйтесь стандартным цифровым вольтметром.
- Напряжение каждого аккумулятора на 12 В постоянного тока должно колебаться между отметками 11,5 и 12,5 В. Любой аккумулятор со значениями, выходящими из этого диапазона, следует считать неисправным и его необходимо заменить.
- Напряжение всех аккумуляторов должно быть примерно равным. Любой аккумулятор, напряжение которого отличается от напряжения остальных более чем на 0,4 В, следует признать неисправным и заменить.
- Подождите около пяти минут и повторите тестирование (так вы сможете обнаружить слабый аккумулятор, который разряжается быстрее остальных). Каждый аккумулятор, разряжающийся быстрее остальных, следует признать неисправным и заменить.

Замена аккумулятора ИБП

При необходимости замены аккумулятора это следует делать в соответствии с представленными ниже инструкциями. Не забывайте, что взамен старых аккумуляторов вы должны либо ставить аккумуляторы того же производителя и той же модели, либо аккумулятор, рекомендованный производителем ИБП. Возможно, если неисправен только один аккумулятор, потребуется замена всех аккумуляторов ИБП. Обязательно свяжитесь с производителем ИБП, чтобы получить квалифицированные рекомендации. Как правило, ИБП поддерживает холодный (с выключением ИБП) и горячий (без выключения ИБП) методы замены аккумуляторов.

Подготовка к холодной замене

Самым безопасным способом замены аккумуляторов ИБП является холодная замена; в этом случае сначала ИБП и все устройства, составляющие его нагрузку, отключаются, и только после этого осуществляется процесс замены. Холодная замена аккумулятора включает следующие этапы.

1. Отключите все нагрузочные устройства (сервер, монитор, принтер и т. д.).
2. Выведите ИБП из рабочего режима (Operate). Для этого нужно нажать кнопку **Standby** (Спящий режим) на ИБП. Светодиод ON гаснет, и подача питания на нагрузочные контактные гнезда прекращается.
3. Отключите ИБП от штатного источника питания (переменного тока).
4. Подождите по меньшей мере 60 сек., пока внутренняя цепь ИБП разрядится.

Подготовка к горячей замене

Как правило, аккумуляторы ИБП можно заменить без выключения самого ИБП (способом горячей замены) — это возможно лишь в том случае, если в данный момент ИБП не заряжает аккумуляторы и не питает от них устройства компьютера, т. е. при доступности штатного источника переменного тока. Чтобы определить, будет ли горячая замена в данных условиях безопасной, проверьте индикаторы ИБП и убедитесь в том, что все аккумуляторы полностью заряжены, а ИБП поставляет не аккумуляторное, а штатное питание.

Примечание

Возможны ситуации, при которых старые аккумуляторы регистрируются как полностью заряженные, но при этом остаются неспособными обеспечить резервное питание нагрузочных устройств. При этом светодиоды заряда аккумуляторов могут обозначать такие аккумуляторы как полностью заряженные, но на самом деле диагностические средства ИБП уже определили, что они нуждаются в замене.

Снятие аккумулятора

Следующие действия должны послужить общей инструкцией по удалению из ИБП старого аккумулятора (ваш ИБП, возможно, устроен по-другому, так что точное руководство по снятию аккумулятора может предоставить только производитель).

1. Чтобы получить доступ к аккумулятору, необходимо открыть корпус ИБП. Для этого ознакомьтесь с документацией к ИБП. Во многих случаях требуется снять несколько винтов, фиксирующих лицевую панель, а затем снять ее, чтобы получить доступ к кабелям светодиодных индикаторов.
2. Отсоедините от лицевой панели кабель светодиодных индикаторов и уберите панель в сторону. При этом будьте осторожны и старайтесь не повредить материнскую плату, которая находится за устройством светодиодной индикации.
3. Открутите винты, фиксирующие аккумулятор.
4. Плавно выдвиньте аккумулятор из ИБП, чтобы получить доступ к его зажимам.
5. Отключите отрицательные (черные) концевые зажимы аккумулятора.
6. Отключите положительные (красные) концевые зажимы аккумулятора.
7. Плавно выдвиньте аккумулятор, чтобы получить доступ к крепежу кабеля аккумулятора. Открутите винт и снимите крепеж кабеля аккумулятора.
8. Осторожно выдвиньте аккумулятор до того момента, пока не получите доступ к пластиковой ручке.
9. Снимите аккумулятор и отложите его для последующей утилизации.

Примечание

Вес аккумуляторов ИБП часто превышает 27 кг. При транспортировке этого блока вам, вероятно, потребуется помощь. Выберите место, куда можно будет положить аккумулятор после его извлечения из ИБП.

Установка нового аккумулятора

После удаления старых аккумуляторов необходимо установить в ИБП новые аккумуляторы — как это делается, показано ниже (точное руководство по установке аккумулятора вам может предоставить только производитель).

1. Плавно поместите новый аккумулятор на шасси — оставьте свободное пространство, достаточное для замены крепежа кабеля.
2. Устанавливая крепеж, расположите кабели так, чтобы они ровно пролегали под пластиковым транспортировочным ремнем (ремнями).
3. Подключите положительные (красные) концевые зажимы аккумулятора.
4. Подключите отрицательные (черные) концевые зажимы аккумулятора.

5. Прикрутите винты, фиксирующие аккумулятор на шасси ИБП.
6. При необходимости установите лицевую панель устройства индикации. Подключите кабель светодиодных индикаторов к устройству светодиодной индикации.
7. Прикрутите винты, фиксирующие лицевую панель на корпусе.

Тестирование аккумулятора

После установки нового аккумулятора следует запустить процедуру самотестирования ИБП или его диагностику (т. е. нажать кнопку Test/Alarm Reset). Инструкции по самотестированию и диагностике можно найти в документации к вашему ИБП. Не забывайте о том, что большинство ИБП не запускают самотестирования до достижения 90% (или даже более полного) заряда новых аккумуляторов, так что, возможно, вам придется подождать, пока новый аккумулятор не зарядится. Если после установки аккумулятора возникнут неисправности, сигнализировать начнет один или несколько предупредительных индикаторов аккумулятора (т. е. индикатор работы аккумулятора). Возможно, вам придется прервать работу и еще раз проверить концевые зажимы.

Утилизация старых аккумуляторов

Из-за применения опасных и едких химических продуктов избавиться от старых аккумуляторов практически невозможно. Большинство производителей составляют инструкции по надлежащей упаковке старых аккумуляторов ИБП и их доставке на утилизационное предприятие. Если производитель вашей модели ИБП не предусмотрел описание подходящих вариантов утилизации, найдите в местном телефонном справочнике утилизационный центр, соответствующий всем местным стандартам защиты окружающей среды.

Увеличение времени закрытия системы

По умолчанию во время отключения системы Windows NT/2000 (т. е. после отключения штатного источника питания и перехода ИБП на аккумуляторы) каждому работающему в системе процессу на завершение работы отводится 20 секунд. Если за это время процесс не ответит, система открывает диалоговое окно **Wait, End Task, Cancel**, которое спрашивает пользователя, нужно ли подождать еще 20 секунд, завершить процесс или отменить отключение системы. Если на корректное отключение приложениям требуется больше времени, вам придется увеличить временной период, отведенный на закрытие системы. Временное значение блокировки по времени, применяемое по умолчанию, хранится в ключе реестра HKEY_CURRENT_USER\Control Panel\Desktop в значении WaitToKillAppTimeout (значение этого периода блокировки для Windows NT 4.0 было неосторожно перемещено в HKEY_USER\.DEFAULT\Control Panel\Desktop). Это значение выражается в миллисекундах. Для его редактирования в реестре вы можете воспользоваться программой REGEDIT.EXE; внесенные в реестр изменения вступают в силу только после перезагрузки системы.

Примечание

Неверное редактирование реестра может привести к серьезным неисправностям всей системы, для устранения которых потребуется переустановка Windows. Прежде чем решиться на внесение изменений в системный реестр, обязательно делайте его резервную копию.

Как правило, увеличение времени отключения системы следует проводить только в том случае, если это действительно необходимо. К примеру, если ваш компьютер теряет источник питания, вполне возможно, что ИБП не сможет обеспечивать резервное аккумуляторное питание столько времени, сколько требуется для корректного завершения всех процессов, а также операционной системы.

Способы устранения наиболее распространенных аварийных состояний ИБП

Многие современные ИБП имеют несколько интеллектуальных функций, которые контролируют такие характеристики, как заряд аккумулятора и автоматическая диагностика. Когда не выполняются важные условия или обнаруживаются ошибки, ИБП издает аварийный сигнал. Средства реализации этого сигнала (т. е. звук, семиполосковые коды или вывод данных на жидкокристаллический индикатор в буквенно-цифровой форме) могут быть различны, но вы должны уметь интерпретировать важнейшие аварийные сигналы и знать, как на них быстро реагировать.

- *Batteries Disconnected* (аккумуляторы отсоединены). Аккумуляторы ИБП неправильно подключены. Проверьте подключение всех аккумуляторов ИБП. ИБП не сможет обеспечить защиту вашей системы, пока эта ошибка не будет исправлена.
- *Batteries Undercharged* (недостаточный заряд аккумулятора). Компьютер получает питание, но заряд аккумуляторов недостаточен, и они не смогут обеспечивать защиту системы в течение длительного времени. Обеспечьте достаточный период времени на подзарядку аккумуляторов. Если такая ситуация сохранится, протестируйте каждый аккумулятор.
- *Check Battery* (проверьте заряд аккумулятора). ИБП выявил возможную неисправность аккумуляторов. Убедитесь в надежности подключения всех аккумуляторов к ИБП. При необходимости вы должны протестировать и заменить все неисправные аккумуляторы.
- *Check Fan* (проверьте вентилятор). Охлаждающий вентилятор внутри ИБП неисправен. Вероятно, вентилятор придется заменить; возможно, ИБП требует заводского ремонта или замены.
- *Check Fuse Board* (проверьте панель предохранителей). ИБП выявил возможную неисправность на внутренней панели предохранителей. Возможно, вам удастся проверить/заменить эту панель, но в большинстве случаев это сообщение означает, что ИБП неисправен и нуждается в заводском ремонте или замене.
- *Check Inverter* (проверьте инвертер). ИБП выявил возможную неисправность, связанную с его инвертирующей схемой (это схема, которая осуществляет непосредственное преобразование аккумуляторного постоянного тока в переменный ток, которым питается компьютер). Как правило, это сообщение означает, что ИБП неисправен и нуждается в заводском ремонте или замене.
- *Check MOVs* (проверьте MOV). ИБП выявил неисправность варистора на основе окиси металла (Metal Oxide Varistor, MOV), находящегося внутри устройства. Как правило, это сообщение означает, что ИБП неисправен и нуждается в заводском ремонте или замене.
- *CHECK POWER SUPPLY* (проверьте источник питания). Устройство выявило возможную неисправность, связанную со своим внутренним источником пита-

ния (который питает элементы микропроцессорного управления ИБП). Как правило, это сообщение означает, что ИБП неисправен и нуждается в заводском ремонте или замене.

- *Circuit Breaker Warning/Shutdown* (предупреждение прерывателя цепи/закрытие системы). ИБП поставляет электрический ток в повышенных объемах. Обычно это происходит из-за того, что избыточное компьютерное оборудование перегружает ИБП. Выключите все компьютерное оборудование и перезапустите ИБП. Затем отключите все несущественные устройства, питание которых через ИБП приводит к его перегрузке.
- *High ac Out/Shutdown* (высокий выходной переменный ток/закрытие системы). ИБП генерирует необычно высокое выходное переменное напряжение и для предотвращения повреждений компьютерного оборудования будет выключен. Как правило, это сообщение означает, что ИБП неисправен и нуждается в заводском ремонте или замене.
- *High Ambient Temperature* (высокая температура окружающей среды). Температура внутри блока ИБП слишком высока. Убедитесь в том, что ИБП стоит в помещении, температурный режим которого находится в пределах диапазона, рекомендованного для его работы (высокотемпературные производственные среды обычно не допустимы). Убедитесь в том, что ничто не блокирует работу охлаждающих вентиляторов внутри ИБП.
- *High Battery* (высокий заряд аккумулятора). Напряжение аккумулятора в ИБП слишком высоко. Возможна ошибка в настройках зарядного устройства аккумулятора, неисправность самой схемы зарядки или дефект одного или нескольких аккумуляторов. Как правило, это сообщение означает, что ИБП неисправен и нуждается в заводском ремонте или замене.
- *Low ac Out/Shutdown* (низкий выходной переменный ток/закрытие системы). ИБП генерирует необычно низкое выходное переменное напряжение и для предотвращения повреждений компьютерного оборудования будет выключен. Как правило, это сообщение означает, что ИБП неисправен и нуждается в заводском ремонте или замене.
- *Low Battery* (низкий заряд аккумулятора). Напряжение аккумулятора ИБП слишком низкое, поэтому ИБП не может работать на аккумуляторном питании и позже будет выключен. В большинстве случаев это связано с ошибкой продолжительности работы. Если заряд аккумуляторов остается на низком уровне, даже когда ИБП работает на переменном токе, то могут быть неисправны схемы зарядки или сами аккумуляторы.
- *Low Runtime* (малая продолжительность работы). Компьютер питается от аккумуляторов, и их оставшийся временной ресурс недостаточен (обычно составляет две минуты или менее). Немедленно выполните штатное выключение компьютерного оборудования. В большинстве случаев отключение ИБП не является обязательным (когда источник переменного тока вновь станет доступен, ИБП сможет выполнить автоматический перезапуск и начать процесс подзарядки аккумуляторов).
- *Memory Error* (ошибка памяти). При запуске ИБП не прошел свой автоматический тест на достоверность памяти (обычно это происходит в интеллектуальных устройствах ИБП, работающих на базе микропроцессоров). Как правило, это со-

общение означает, что ИБП неисправен и нуждается в заводском ремонте или замене.

- *Output Short Circuit* (короткое замыкание выходных цепей). Аналогично перегрузке, рассмотренной ниже. Как правило, на это состояние указывает непрерывный звуковой сигнал; обычно означает возникновение состояния перегрузки при включенном ИБП. Проверьте электропроводку и убедитесь в том, что наличие избыточного оборудования не приводит к перегрузке ИБП.
- *Overload* (перегрузка). Потребляемая компьютерным оборудованием мощность превосходит возможности ИБП. Это может привести к значительному уменьшению продолжительности действия аккумулятора. Вам придется последовательно отключать дополнительное компьютерное оборудование (например, сканеры, принтеры и т. д.) до тех пор, пока эта ошибка не исчезнет.
- *Replace Batteries* (замените аккумуляторы). Эта ошибка обычно генерируется в виде одного или нескольких последовательностей звуковых сигналов и предполагает, что один или несколько аккумуляторов устройства не удерживают достаточный заряд. Вам придется проверить каждый аккумулятор ИБП и заменить все подозрительные аккумуляторы.
- *UPS Fault* (сбой ИБП). Обозначает серьезную ошибку в работе ИБП. В такой ситуации ИБП не может обеспечивать защиту вашей системе. Устраните ошибку или замените ИБП.

Симптомы неисправностей ИБП

Обычно ИБП способны в течение длительного времени обеспечивать надежное обслуживание вашей системы, однако есть некоторые неисправности, которые могут стать препятствием к нормальному функционированию ИБП. В этой части главы рассматривается ряд общих симптомов, с которыми вы можете столкнуться, имея дело с проблемными ИБП.

Симптом 17.17. ИБП не включается

Появление подобной неисправности может быть вызвано несколькими причинами. Для их выяснения нужно проверить следующие факторы.

- Возможно, устройство находится в отключенном состоянии. Нажмите кнопку On один раз, чтобы подвести питание к ИБП, а также к тому оборудованию, которое к нему подключено.
- Проверьте подключение к штатному источнику питания. Возможно, ИБП не подключен к источнику переменного тока. Убедитесь в том, что силовой кабель, проведенный от ИБП до штатного источника питания, надежно закреплен с обоих концов.
- Проверьте прерыватель цепи. Вполне возможно, что входной прерыватель цепи ИБП расцепился. Снизьте нагрузку на ИБП, отключив оборудование и перезапустив прерыватель цепи (на боковой части ИБП) нажатием на плунжер.
- Очень низкое (или отсутствующее) входное напряжение. Проверьте подведение к ИБП источника переменного тока, подключив к нему настольную лампу. Если ее свет окажется очень тусклым, проверьте штатное напряжение.

- ❒ Аккумулятор плохо смонтирован. Убедитесь в том, что аккумуляторные коннекторы полностью зацеплены.

Симптом 17.18. ИБП не отключается

Практически во всех подобных случаях оказывается, что неисправность кроется в самом ИБП, который нуждается в ремонте или замене. Не пытайтесь продолжать эксплуатировать ИБП — отключите его и немедленно сдайте в ремонт.

Симптом 17.19. ИБП использует аккумулятор при наличии нормального напряжения переменного тока

Если в стенной розетке есть переменный ток, но ИБП работает на аккумуляторе, вам следует проверить входной прерыватель цепи. Возможно, из-за резкого скачка напряжения или избыточной нагрузки произошло расцепление прерывателя, в результате чего ИБП был отрезан от источника переменного тока. Если расцепление прерывателя происходит постоянно, снизьте нагрузку на ИБП, отключив от него лишнее оборудование и переустановив прерыватель цепи (на боковой панели ИБП). Другим распространенным источником этой проблемы является искаженное (т. е. высокое или низкое) напряжение на линии передачи переменного тока. Это случается при наличии сбоев на центрах электроснабжения от сети общего пользования. Распространенным примером является понижение напряжения в летнее время, когда электрическая сеть оказывается перегруженной системами кондиционирования воздуха (недорогие бензиновые генераторы также могут искажать напряжение). Подключите ИБП к розетке в другой силовой цепи. Протестируйте входное напряжение с помощью индикатора входного напряжения. Если уровень напряжения в отношении подключенного оборудования является приемлемым, уменьшите чувствительность ИБП.

Симптом 17.20. ИБП не обеспечивает ожидаемого времени резервного питания

Практически во всех подобных случаях причину следует искать в аккумуляторах. Возможно, аккумулятор ИБП слаб из-за недавнего нарушения энергоснабжения (он еще не полностью перезарядился), или его срок службы подходит к концу. Замените аккумулятор. После продолжительных сбоев питания аккумуляторы нуждаются в подзарядке. При частом применении или при работе в условиях повышенных температур они изнашиваются быстрее, чем обычно. Если срок службы аккумулятора приближается к завершению, постарайтесь заменить его (даже в том случае, если светодиод замены аккумулятора еще не начал сигнализировать).

Симптом 17.21. Все индикаторы ИБП светятся, а само устройство постоянно подает звуковые сигналы

В некоторых случаях причина такого поведения заключается в перегрузке ИБП. Проверьте индикатор нагрузки ИБП, отключите лишнее оборудование (например, принтеры) и при необходимости перезапустите ИБП. Если неисправность сохраняется, вероятно, имеет место серьезная внутренняя неисправность самого устройства ИБП. Не пытайтесь продолжать его эксплуатацию. Отключите ИБП и немедленно сдайте его в ремонт.

Симптом 17.22. Панельные индикаторы ИБП сигнализируют один за другим

Обычно в таких ситуациях речь не идет о сбое. Напротив, ИБП был удаленно отключен (посредством программного обеспечения или факультативной вспомогательной платы). При возобновлении штатного энергоснабжения ИБП произведет автоматический перезапуск.

Симптом 17.23. ИБП подключен к штатному источнику питания, но ни один индикатор не работает

ИБП отключился, т. к. аккумулятор был разряжен после продолжительного сбоя питания. В таком случае можно только восстановить штатное питание переменным током. ИБП возобновит работу в нормальном режиме, когда питание будет восстановлено и аккумулятор получит достаточный заряд.

Симптом 17.24. Горит светодиод замены батареи (Replace Battery)

Аккумуляторный источник питания разряжен или неисправен. Дайте аккумулятору, по меньшей мере, четыре часа на подзарядку, а затем запустите процедуру самотестирования ИБП. Если неисправность сохранится и после подзарядки, замените аккумулятор. Иногда в подобных случаях выясняется, что аккумулятор ненадежно закреплен, тогда проверьте, все ли аккумуляторные коннекторы полностью сцеплены.

Симптом 17.25. ИБП указывает на ошибку местной электропроводки

В большинстве случаев это означает, что ИБП обнаружил некорректную электропроводку в розетке переменного тока. К примеру, эта розетка может быть не заземлена (с другой стороны, заземляющий провод может отсутствовать на шнуре питания ИБП). Возможно, вы также обнаружите, что линейный и нейтральный провода в розетке переменного тока (или в шнуре питания ИБП) перепутаны местами. В обоих случаях для устранения неисправности следует пригласить квалифицированного электротехника.

Симптом 17.26. На ИБП начинает сигнализировать предупредительный светодиод высокого напряжения

Обычно это означает, что переменное напряжение слишком высоко (т. е. выходит за пределы рабочего диапазона ИБП). Обычно в таких случаях ИБП, чтобы не повредить компьютерное оборудование, переходит на аккумуляторное питание. Если подобная ситуация будет повторяться регулярно, пригласите квалифицированного электрика для проверки уровня переменного напряжения. Возможно, после возвращения к нормальному уровню переменного тока вам придется сбросить аварийное состояние.

Симптом 17.27. На ИБП начинает сигнализировать предупредительный светодиод пониженного напряжения

Обычно это означает, что переменное напряжение слишком низко (т. е. выходит за пределы рабочего диапазона ИБП). В таких случаях ИБП, чтобы не повредить компьютерное оборудование, переходит на аккумуляторное питание. Если подобная ситуация будет повторяться регулярно, пригласите квалифицированного электрика для проверки уровня переменного напряжения. Возможно, после возвращения к нормальному уровню переменного тока вам придется сбросить аварийное состояние.

Симптом 17.28. ИБП часто переключается со штатного питания на аккумуляторное

Как правило, при этом ИБП работает в нормальном режиме, защищая компьютерное оборудование от высоких/низких уровней переменного напряжения. В первую очередь проверьте уровень переменного тока и убедитесь в том, что он не выходит за пределы допустимого рабочего диапазона ИБП. Если это не так, пригласите квалифицированного электрика для устранения этой неисправности. Если переменный ток не выходит за рамки допустимой нормы, но ИБП продолжает часто переключаться из одного режима в другой, вам, вероятно, придется отрегулировать ИБП так, чтобы сделать его менее чувствительным к изменениям уровня переменного тока. Если неисправность сохранится, возможно, неисправен ИБП.

Симптом 17.29. На ИБП начинает сигнализировать предупредительный светодиод нагрузки

В дополнение к сигнализированию светодиода может обнаружиться расцепление прерывателя цепи. Как правило, это означает, что ИБП подвергается чрезмерной нагрузке (к нему подключено слишком много устройств). Убедитесь в том, что суммарная нагрузка (исчисляемая в вольт-амперах) не превышает емкости ИБП. В случае превышения следует либо отключить ненужные устройства, либо заменить имеющийся ИБП на более мощную модель. Если нагрузка находится в допустимых пределах, то, возможно, ИБП неисправен.

Симптом 17.30. Вкладка *UPS* диалогового окна *Power Options* недоступна

При попытке настройки ИБП может выясниться, что в диалоговом окне **Power Options** (Электропитание) операционной системы Windows 2000 вкладка **UPS** недоступна. Практически во всех случаях это означает, что сервер не смог должным образом идентифицировать ИБП. Поддержка ИБП встроена в Windows 2000, и на большинстве устройств ИБП есть либо последовательный кабель, либо шина USB (Universal Serial Bus — универсальная последовательная шина), с помощью которой и происходит их подключение к компьютеру.

ИБП, подключенный посредством кабеля USB, в Windows 2000 представляется как аккумулятор и настраивается на вкладке **Alarms and Power Meter** (Настройка ИБП) диалогового окна **Power Options** (Электропитание). В ноутбуках и настольных компьютерах с ИБП, подключенным через USB, вкладка **UPS** в диалоговом окне **Power Options** (Электропитание) отсутствует. В этом случае ИБП подает себя как HID-совместимое устройство (Human Input Device — устройство ввода человеком), и Windows 2000 автоматически выполняет установку необходимых драйверов. Убедитесь в том, что на вашем компьютере установлены надлежащие средства поддержки USB, и еще раз проверьте кабель USB, проходящий между ИБП и системой.

ИБП, подсоединенный через последовательный кабель, настраивается во вкладке **UPS** диалогового окна **Power Options**. Windows 2000 не обязательно обнаружит последовательно подключенный Plug-and-Play ИБП. По умолчанию, Windows 2000 поддерживает последовательное подключение следующих устройств ИБП, произведенных компанией American Power Conversion (APC):

- Back-UPS;
- Back-UPS Pro;

- базовый порт на вспомогательных средствах обмена информацией;
- базовое сигнализирование на любой UPS от APC;
- Matrix-UPS;
- PowerStack;
- интеллектуальное сигнализирование любого UPS от APC;
- Smart-UPS;
- Symmetra Power Array.

Чтобы настроить полярность сигнала ИБП, вы можете выбрать **Generic** в окне **Manufacturer**, а затем **Custom** в окне **Model**. За инструкциями по настройке службы **UPS** для вашего ИБП следует обратиться к его документации. Важно не забывать, что устройства ИБП, предполагающие последовательное соединение, могут подключаться посредством различных специализированных кабелей (причем разные кабели обеспечивают разные уровни функциональности). Если при настройке ИБП вы сталкиваетесь с трудностями, свяжитесь с производителем ИБП, чтобы получить информацию о конкретных требованиях к кабелям ИБП.

Симптом 17.31. Во время установки Windows 2000 ИБП входит в аккумуляторный режим

В процессе установки Windows 2000 на компьютере, подключенном к ИБП, система может неожиданно перейти в аккумуляторный режим. Эта неисправность появляется на стадии работы программы установки (Setup), когда драйвер порядковой нумерации (SERUNUM.SYS) пытается выяснить, какие соединения установлены на последовательных портах. ИБП запускается в тот момент, когда этот драйвер контактирует с последовательным портом. К сожалению, это известная проблема, связанная с Windows 2000. Чтобы избежать ее появления, на время работы программы установки Windows 2000 следует отключить последовательный кабель от ИБП, тогда после завершения работы Setup эта проблема больше не появится.

Симптом 17.32. Во время установки Windows 2000 ИБП входит в режим аттестации аккумулятора

В процессе установки Windows 2000 некоторые системы ИБП, работающие в режиме интеллектуального сигнализирования (Smart Signalling), могут переходить в режим калибровки аккумулятора (Battery Calibration). Со временем такое поведение может привести к непредвиденному истощению аккумулятора. Эта неисправность возникает тогда, когда на этапе работы программы установки Windows 2000 пытается обнаружить мышь с последовательным подключением. При этом Windows отправляет на последовательный порт символ "D" ASCII, что и приводит к вхождению некоторых устройств ИБП в режим аттестации аккумулятора. Во всех версиях Windows 2000, начиная с Service Pack 2, эта проблема устранена. Свойства английской версии этого исправления должны быть следующими:

```
06/21/2000  09:40p  229,264  Setupldr.bin
```

Чтобы избежать появления этой неисправности, на время работы программы установки Windows 2000 с CD-ROM ИБП следует отключить. Если вы устанавливаете Windows средствами автоматической инсталляции, необходимо заменить файл

SEUPLDR.BIN в каталоге I386 файлом SETUPLDR.BIN, имеющимся в этом исправлении.

Симптом 17.33. ИБП с "простым сигнализированием" не отключается после отключения системы

Если к вашему компьютеру, работающему на базе операционной системы Windows 2000, подключен ИБП с "простым сигнализированием", может обнаружиться, что после отключения системы это устройство не выполняет отключение питания — таким образом, ИБП продолжает поставлять аккумуляторное питание. Такое поведение не наблюдается при сочетании аналогичного ИБП с операционной системой Windows NT 4.0. Эта проблема обуславливается изменениями в Windows 2000. В Windows NT 4.0 после отключения системы процессы могут работать на ограниченных ресурсах. Это позволяет драйверу службы ИБП под Windows NT 4.0 отправлять на ИБП сигналы на отключение через последовательный порт. В Windows 2000 во время отключения системы все процессы автоматически завершаются операционной системой. Это не позволяет драйверу службы ИБП сигнализировать ИБП о необходимости отключения питания после отключения системы. Обходных путей решения этой проблемы не существует, но некоторые ИБП позволяют устанавливать внутренний таймер, который автоматически отключает ИБП при питании от аккумулятора в отсутствие нагрузки. Чтобы узнать, есть ли такая функция в вашем ИБП, ознакомьтесь с руководством по его эксплуатации.

Симптом 17.34. ИБП не может обратиться к своему COM-порту

Такие случаи известны при работе с операционной системой Windows 2000 (SP1 и SP2). При попытке выбора производителя ИБП с помощью вкладки **UPS** диалогового окна **Power Options** может появиться следующее сообщение об ошибке:

```
The UPS service could not access the specified Comm Port.
```

Возможность возникновения этой неисправности присутствует в том случае, если на вашем компьютере есть лишь один COM-порт, который не настроен как COM1. Значением COM-порта, принимаемым по умолчанию при установке ИБП, является COM1, так что при переходе на вкладку **UPS** именно это значение автоматически заносится в реестр. Чтобы устранить эту неисправность, следует выбрать COM-порт вручную.

1. Последовательно выберите **Start** (Пуск), **Settings** (Настройка), **Control Panel** (Панель управления) и двойным щелчком откройте **Power Options** (Электропитание).
2. Откройте вкладку **UPS** (ИБП), затем нажмите кнопку **Select** (Выбор).
3. В окне **On Port** (Порт) укажите COM-порт. Возможно, в вашем распоряжении будет лишь один вариант.
4. Нажмите кнопку **Finish** (Готово), затем кнопку **OK**.

Симптом 17.35. Отключение Windows происходит сразу после сбоя энергоснабжения

Windows NT/2000 закрывается сразу после сбоя энергоснабжения, несмотря на то, что компьютер питается через работающий ИБП. Обычно возникновение этой неисправности обуславливается неспособностью ИБП отправить компьютеру сигнал

низкого заряда аккумулятора. Когда ИБП не может отправить компьютеру сигнал, оповещающий его о состоянии низкого заряда аккумулятора, Windows NT/2000 основывается на информации, предоставленной пользователем, и исходя из этих данных определяет период времени, в течение которого система может питаться от аккумулятора. Когда заряд аккумулятора снижается настолько, что его хватает лишь на две минуты, Windows запускает процесс отключения системы.

При загрузке Windows NT/2000 операционная система запускается с допущением, что аккумулятор полностью истощен. Эта функция связана с обеспечением защиты; она предполагает, что компьютер был только что включен, а аккумулятор ИБП еще не успел зарядиться. Затем Windows NT/2000 вычисляет период времени, в течение которого возможно питание от аккумулятора, основываясь на настройках **Expected battery life** (Ожидаемое время жизни батареи) и **Battery recharge time per minute of run time** (Время восстановления батареи на минуту работы), значения которых задаются на экране конфигурации службы **UPS** (**UPS Service**). Например, если время перезарядки аккумулятора равно 100 минут, то прежде чем Windows решит, что заряда аккумулятора хватит на 1 минуту резервного питания, должно пройти 100 минут. Чтобы Windows NT смогла вычислить двухминутный заряд, должно пройти 200 минут и т. д.

Windows NT/2000 запускает процесс отключения системы сразу после сбоя энергоснабжения лишь в том случае, если исчисленный ею срок работы от аккумулятора составляет менее двух минут. Таким образом, если последняя перезагрузка компьютера производилась недавно, после сбоя энергоснабжения Windows может отключить систему быстрее, чем предполагалось, несмотря на то, что аккумулятор ИБП полностью заряжен. Это делается намеренно, потому что система Windows NT/2000 при отсутствии данных о состоянии ИБП допускает его наихудшее состояние.

Симптом 17.36. Неисправность связана с последовательным подключением ИБП

Возможно, на вкладке **UPS** (ИБП) диалогового окна **Power Options** (Электропитание) в Windows 2000 появляется сообщение о том, что связь с ИБП потеряна. Прежде чем пытаться настроить ИБП, убедитесь в том, что для подключения к ИБП используется именно тот кабель, который входил в комплект ИБП (а не стандартный последовательный кабель). Проверьте, правильно ли указаны производитель и модель ИБП на вкладке **UPS** (ИБП). Затем откройте **Device Manager** (Диспетчер устройств) и вкладку **COM Ports** (COM-порты). Двойным щелчком выберите COM-порт, применяемый для взаимодействия с ИБП. В диалоговом окне **Port Properties** (Свойства порта) должны быть определены необходимые настройки порта (конкретные настройки должны указываться в руководстве по эксплуатации ИБП). Как правило, подходят следующие настройки:

- Data Rate, bps (Скорость передачи данных, бит/с): 2400;
- Data (Данные): 8-бит;
- Parity (Контроль по четности): none;
- Stop: 1;
- Flow Control (Управление потоком): none.

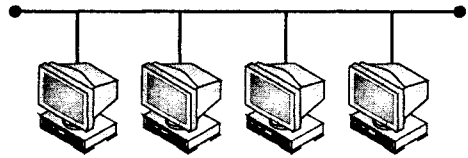
Дополнительные ресурсы

TrippLite: **www.tripplite.com**.

APC: **www.apcc.com**.

Best Power: **www.bestpower.com**.

Microsoft: **www.microsoft.com**.



ГЛАВА 18

Сетевые хранилища данных

Современные сети оперируют не только текстом, электронными таблицами и другими распространенными типами данных, которые мы традиционно ассоциируем с работой в сети — сети с большой пропускной способностью осуществляют обмен высококачественной графикой, голосовыми данными и даже видеосигналами в реальном времени. Такие требования увеличивают связность сети, но, с другой стороны, они обуславливают повышенную нагрузку на сетевые системы хранения данных. Администраторы понимают, что несколько жестких дисков, установленных в сервере, теперь не отвечают потребностям сети по хранению данных. Появляется новое поколение *сетевых устройств хранения данных* (NAS, Network Attached Storage), способных обеспечить значительное дисковое пространство для хранения данных. Устройство NAS — это специализированный файловый сервер, подключаемый к сети через концентратор или коммутатор. Оно позволяет администраторам быстро наращивать память и распределять память по разным областям сети (снижая перегруженность трафика, которая часто случается на файловых серверах). В этой главе подробно рассматриваются некоторые распространенные типы устройств хранения, а также излагаются основы сетей хранения данных (Storage Area Network, SAN).

Серверы жестких дисков

Наиболее распространенным типом сетевого устройства хранения данных является файловый сервер на основе жестких дисков; в качестве примера такого устройства можно привести файловый сервер Maxtor NAS 3000, показанный на рис. 18.1. Это специализированные файловые серверы, содержащие массив дисков (которые можно организовать на разных уровнях RAID), сетевой интерфейс, а также все технические компоненты и программы, необходимые для функционирования устройства. В большинстве случаев применение сервера NAS подразумевает его подключение к сети и последующий запуск программного обеспечения, которое должно инициализировать и настроить характеристики хранения этого устройства. Когда NAS подключен к сети, его управление, как правило, без труда осуществляется через Web-браузер.

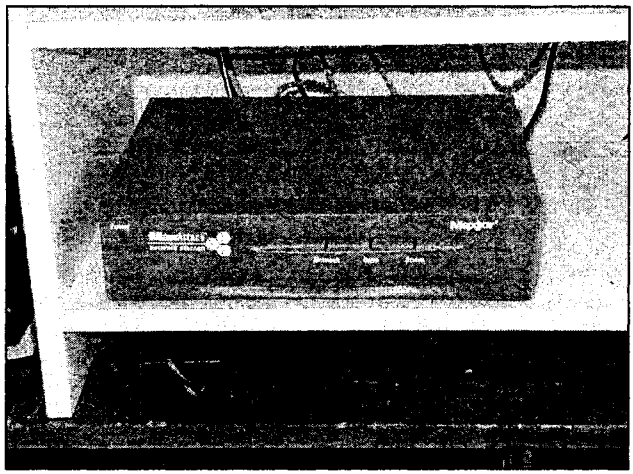


Рис. 18.1. В условиях простого Ethernet-соединения Maxtor NAS 3000 обеспечивает до 40 Гбайт пространства хранения

Назначение индикаторов

Специализированные устройства хранения (типа NAS 3000) имеют комплект индикаторов, которые обозначают состояние устройства и указывают на сбои в его работе. Прежде чем устанавливать устройство хранения, ознакомьтесь с назначением имеющихся на нем индикаторов. Как правило, среди них есть следующие.

- *Светодиод питания* (Power LED). Светодиод питания указывает на подключение устройства к источнику питания. При мигании индикатора устройство запускается или, наоборот, выключается.
- *Светодиод подключения к сети* (Network LED). Светодиод подключения к сети может сигнализировать зеленым или оранжевым светом. Например, зеленый свет обозначает соединение с сетью на скорости 10 Мбит/с, а оранжевый — соединение на скорости 100 Мбит/с. Установленное сетевое соединение обозначается постоянным свечением светодиода. Мигание светодиода указывает на наличие сетевого трафика (аналогично светодиоду связи/активности на многих коммутаторах и маршрутизаторах).
- *Светодиод дисковода* (Drive LED). Светодиод дисковода обозначает его активность. Постоянное свечение указывает на высокую активность диска. В других случаях светодиод мигает, обозначая различные уровни активности.
- *Светодиод состояния* (Status LED). Свечение светодиода состояния указывает на то, что NAS генерирует предупреждение (которое обычно отображается на домашней странице устройства NAS). Свечение может быть постоянным или мигающим; в последнем случае светодиод указывает на конкретную ошибку. В табл. 18.1 приводятся некоторые распространенные предупреждения для Maxtor NAS — другие устройства NAS могут иметь другие индикаторы. Устройства NAS, подобные Maxtor NAS 3000, генерируют кодовые мигания светодиода, которые обозначают состояние и ошибки устройства.

Таблица 18.1. *Обычные предупреждения Maxtor NAS*

Состояние	Описание/решение
Постоянно включен	В устройстве NAS произошел серьезный сбой; устройство нуждается в замене
Мигнул 2 раза	Имя одного из расположенных в сети серверов совпадает с именем NAS. Имя, присвоенное NAS, должно быть уникальным; необходимо назначить устройству новое сетевое имя
Мигнул 3 раза	Обновление операционной системы оказалось неуспешным. NAS возвращается к применению предыдущей версии и выдает предупреждение
Мигнул 4 раза	IP-адрес одного из расположенных в сети устройств совпадает с IP-адресом NAS. IP-адрес, присвоенный NAS, должен быть уникальным; необходимо назначить NAS постоянный IP-адрес
Мигнул 5 раз	Температура внутреннего процессора NAS слишком высока. При появлении этого предупреждения температура все еще на 10% ниже того температурного порога, по достижении которого устройство отключается автоматически. Выключите питание NAS и проверьте вентиляцию
Мигнул 6 раз	Один из двух дисков в составе дублированной пары сталкивается с ошибками или отсутствует
Мигнул 7 раз	Оба диска в составе дублированной пары имеют ошибки
Мигнул 8 раз	NAS фиксирует большое количество ошибок дисков и генерирует соответствующее предупреждение
Мигнул 10 раз	Один из дисков переполнен; в результате издается предупреждение
Мигнул 12 раз	Датчик температуры/напряжения неисправен; устройство NAS следует заменить

Основы установки

Некоторые устройства NAS представляют собой специализированные компьютеры, установка которых, как правило, подразумевает их подключение к свободному сетевому порту и последующий запуск программной утилиты на административной консоли. Впрочем, доступ к устройству NAS и управление им можно с тем же успехом осуществить с любой рабочей станции, поддерживающей интерфейс Web-браузера. Обычно установка NAS состоит из следующих этапов.

1. Чтобы подключить устройство NAS к сети, вставьте кабель Category 6 в сетевой коннектор, находящийся на задней панели NAS (рис. 18.2), а затем поместите другой его конец в коннектор 10/100BaseT Ethernet сетевого концентратора или коммутатора. Подключите устройство NAS к источнику питания через шнур подачи переменного тока или адаптер.
2. Включите питание NAS, нажав кнопку **On/Off** на задней панели устройства. После этого при включении питания в течение нескольких минут расположенная на

передней панели устройства контрольная лампа источника питания будет мигать. Когда эта лампа прекратит мигать, а светодиод сетевого соединения, напротив, начнет сигнализировать, ваше устройство NAS будет готово к проведению настройки.

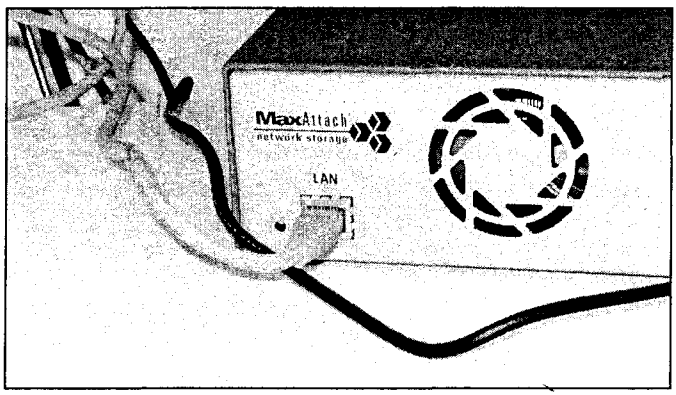


Рис. 18.2. NAS 3000 подключается к сети Ethernet посредством одного кабеля RJ-45

3. Поместите компакт-диск с программным обеспечением устройства NAS в дисковод административного компьютера, зарегистрированного в сети (хотя обычно для этих целей подходит любая рабочая станция). Запуск этого программного обеспечения произойдет автоматически — начнется процесс инсталляции. Чтобы установить программное обеспечение NAS, следуйте приглашениям на экране.

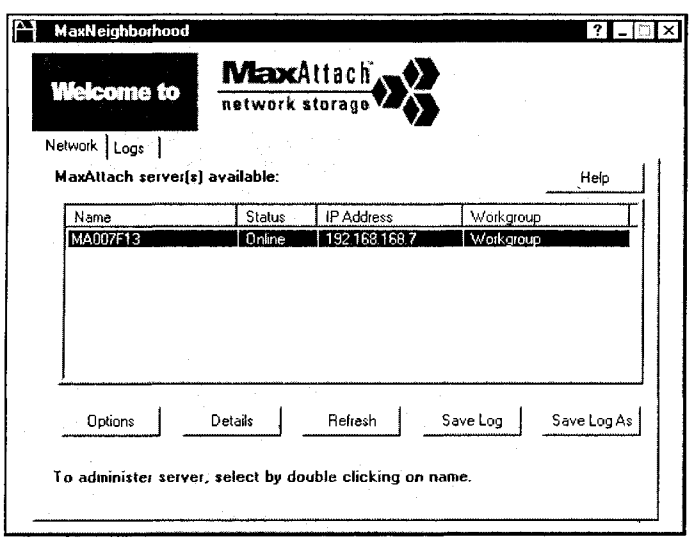


Рис. 18.3. После подключения устройства NAS программа установки автоматически обнаружит все подобные устройства, присутствующие в сети, и сможет сообщить вам их подробные характеристики

4. После завершения процесса инсталляции у вас появится возможность запустить установленное ПО. Чтобы сделать это, нажмите кнопку **Finish**. Появится новое окно, а программа будет искать в сети подключенные устройства NAS. В зависимости от конфигурации сети этот процесс может занять несколько минут.
5. По окончании поиска появится окно со списком устройств NAS, присутствующих в сети. Двойной щелчок на любом из них позволяет просмотреть его состояние, имя, IP-адрес, имя рабочей группы и другие данные (рис. 18.3). Эти данные подтверждают работоспособность данного устройства NAS — следовательно, вы можете приступать к его настройке.

Примечание

Не забудьте включить новое устройство NAS в документацию к вашей сети. Укажите его IP-адрес, MAC-адрес и имя.

Настройка NAS

После подключения устройства NAS и его приведения в работоспособное состояние вам нужно будет выполнить его настройку, а также некоторые административные задачи. При первоначальной настройке NAS вы должны запустить процесс настройки из программного обеспечения этого устройства. Например, чтобы запустить мастер настройки **Maxtor NAS 3000 Configuration Wizard**, выделите имя соответствующего устройства (например, MA007F13) в окне программы, а затем дважды щелкните на нем. После этого мастер **Configuration Wizard** появится в окне вашего Web-браузера (рис. 18.4). Он поможет вам установить часы, назначить пароль администратора, а также имя рабочей группы. Чтобы запустить процесс настройки, нажмите кнопку **Next**, а затем введите следующие параметры.

Примечание

Не забывайте, что данные инструкции приведены только в качестве примера. Возможно, ваша модель NAS поддерживает большее количество опций. Для получения конкретных инструкций по настройке и управлению нужно всегда обращаться к документации устройства.

- *Часы.* При установки часов нужно просто заполнить обязательные поля. Если вы находитесь не в одном часовом поясе с устройством, можно ввести локальное имя, соответствующее местонахождению одного из вас. Чтобы осуществить переход на летнее время, пометьте соответствующий флажок, и в нужный момент устройство переставит часы автоматически. По завершении всех операций нажмите кнопку **Next**.
- *Пароль.* В целях безопасности вам следует назначить устройству NAS пароль администратора. Введите пароль, подтвердите, а затем запишите его в надежном месте.
- *Имя и рабочая группа.* Теперь введите имя устройства и идентификатор рабочей группы, которой соответствует данное устройство NAS. Имя устройства нужно ввести для того, чтобы пользователи сети могли обнаружить его в папке **Network Neighborhood** (Сетевое окружение) или в Windows Explorer (Проводник). При

создании имени устройства (его длина не должна превышать 15 символов) не забывайте, что оно должно быть уникальным — такого же имени не должно быть ни у одного другого устройства в вашей сети. Если вы не изменили имя рабочей группы на настольном или портативном компьютере, по умолчанию принимается имя "Workgroup". Нажмите кнопку **Next**.

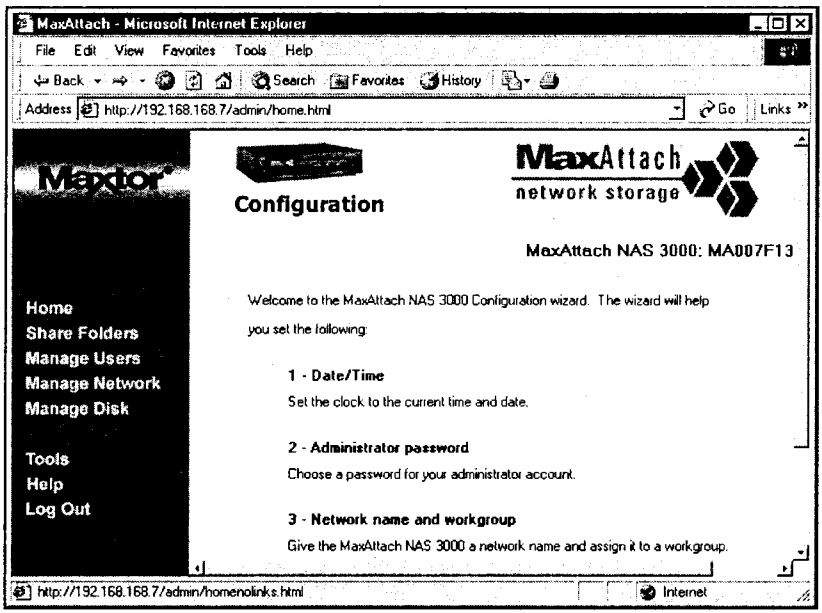


Рис. 18.4. Мастер NAS Configuration Wizard позволяет вам настроить устройство NAS для обеспечения его работоспособности

В большинстве случаев первоначальная настройка на этом заканчивается — чтобы изменения в настройках вошли в силу, устройство NAS нужно перезагрузить. После перезагрузки вы должны будете ввести пароль. Наберите его, а затем нажмите клавишу <Enter> или кнопку **OK**. Теперь NAS готово к работе. Если устройство NAS и рабочая станция, с которой вы его настраиваете, находятся в разных подсетях, то вам придется выделить для NAS временный IP-адрес. Это значит, что ваше устройство действует как DHCP-сервер. Назначьте IP-адрес и маску подсети. После присвоения IP-адреса нажмите кнопку **Next**, а затем **Reboot**. После перезагрузки NAS вам нужно будет ввести пароль. Наберите его, а затем нажмите клавишу <Enter> или кнопку **OK**. Теперь необходимо изменить диапазон IP-адресов, доступный для присвоения средствами NAS. Для этого войдите в меню **Manage Networks**, а затем перейдите на вкладку **DHCP Server**. Измените диапазон в соответствии с новым адресом и нажмите кнопку **Apply**.

Примечание

NAS может обеспечивать поддержку DHCP, но пользоваться этим совершенно необязательно. Так как NAS выполняет функции файлового сервера, ему можно присвоить постоянный IP-адрес.

Об управлении NAS

После первоначальной настройки устройства NAS вы можете создавать пользователей и группы, формировать совместно используемые ресурсы/каталоги и применять средства защиты или, если вы пользуетесь главным контроллером домена, выбрать **NT Passthrough**. Обращение к административной программе производится либо через Web-сервер, либо с помощью программной утилиты NAS. При работе через Web-сервер нужно просто указать в его адресной строке IP-адрес устройства (например, 192.168.1.106) и ввести правильный пароль. В результате в окне браузера появится домашняя страница NAS (рис. 18.5) — в ней будет представлена важная информация о сети, дисках и предупреждениях, связанных с NAS.

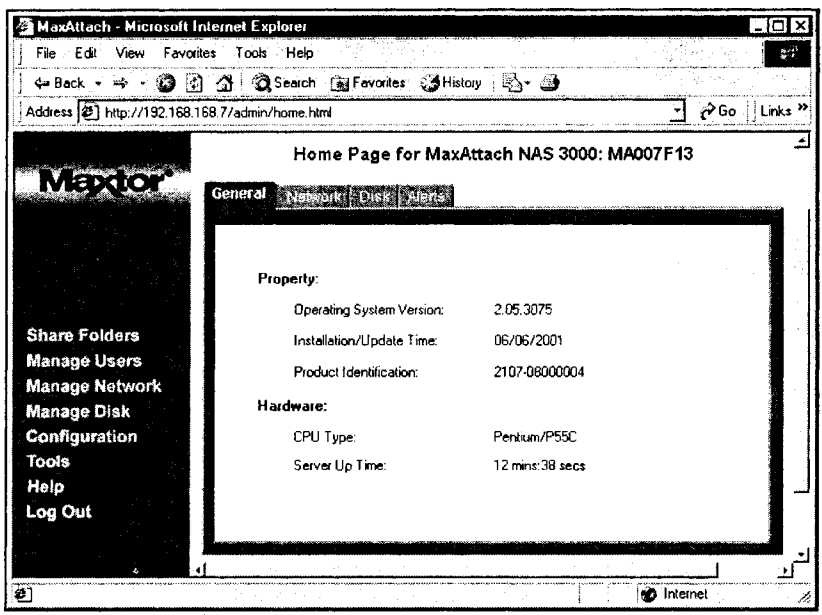


Рис. 18.5. Комплексное управление устройством NAS может производиться через интерфейс браузера

Совместно используемые каталоги

Чтобы создать на устройстве NAS совместно используемые ресурсы, войдите в меню **Share Folders**. К этому моменту на NAS уже должен быть создаваемый по умолчанию общий совместно используемый ресурс (под названием \Public) — если только вы не внесли изменения в заводские настройки дисков. На данном этапе к этому ресурсу имеет доступ каждое устройство, подключенное к сети. Чтобы создать новый совместно используемый ресурс, выберите пункт **Share Folders** на левой панели навигации. В результате появится экран с каталогами по умолчанию (подобный тому, что изображен на рис. 18.6). Если вы уже успели создать какие-либо частные каталоги, они также будут перечислены. Выберите нужный каталог, а затем нажмите кнопку **New Folder**. Введите имя нового каталога. Нажмите кнопку **OK**. Выберите

каталог, который вы только создали. Изначально он не является совместным. Чтобы сделать его таковым, установите переключатель в положение **SMB** или **NFS**. Подтвердите имя совместно используемого ресурса и нажмите кнопку **Apply**. В результате в сети появится новый коллективный ресурс.

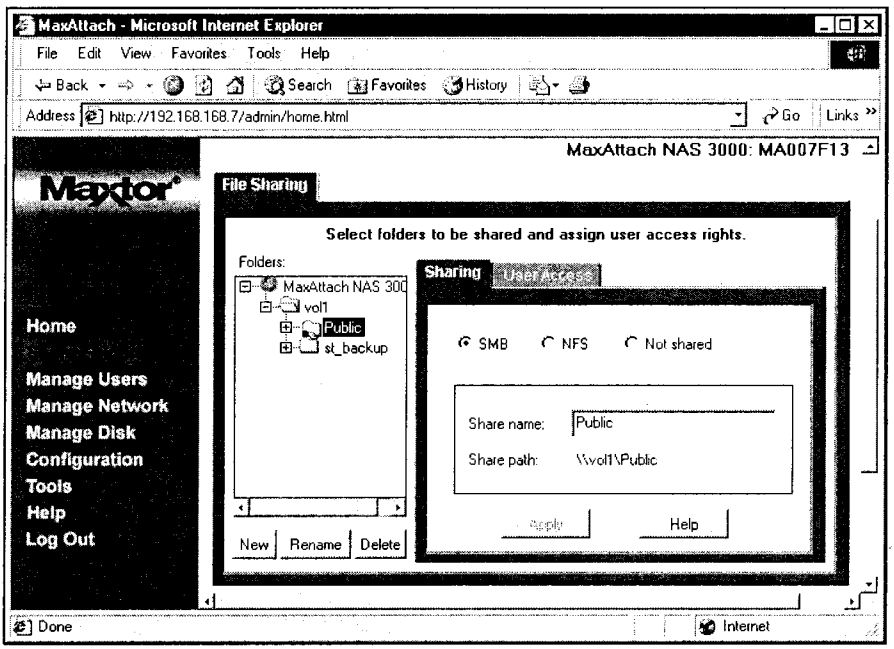


Рис. 18.6. Меню **Share Folders** позволяет управлять каталогами NAS

Устройства NAS, типа Maxtor NAS 3000, позволяют определять для создаваемых совместно используемых ресурсов права доступа и уровни безопасности. Для примера выберите какой-нибудь коллективный ресурс и перейдите на вкладку **User Access**. По умолчанию всем новым совместно используемым ресурсам присваивается статус Read/Write (чтения/записи) для группы AnyOne (т. е. для всех). Чтобы ограничить доступ к данному ресурсу, нужно определить другой статус — None (доступ запрещен) или Read Only (только чтение). Выберите один из этих вариантов и нажмите кнопку **Apply**. Чтобы назначить права доступа пользователю или группе пользователей, выделите соответствующее имя и определите один из статусов. После этого нажмите кнопку **Apply**.

Управление пользователями

У вас есть возможность координировать права пользователей, а также групп, которые обращаются к устройству NAS. Чтобы сформировать права пользователей или групп, выберите пункт **Manage Users** на панели навигации, расположенной в левой части экрана (рис. 18.7). Нажмите кнопку **Add New User**. Введите зарегистрированное в системе Windows 9x/NT/2000 имя пользователя и соответствующий ему пароль. Введите пароль еще раз, чтобы подтвердить его, и нажмите кнопку **OK**. Теперь

вы можете создать для этого пользователя частный или домашний каталог. Для этого установите флажок **Private folder** и нажмите кнопку **Apply** (чтобы создать дополнительных пользователей, нажмите кнопку **Add New User** и пройдите всю процедуру заново).

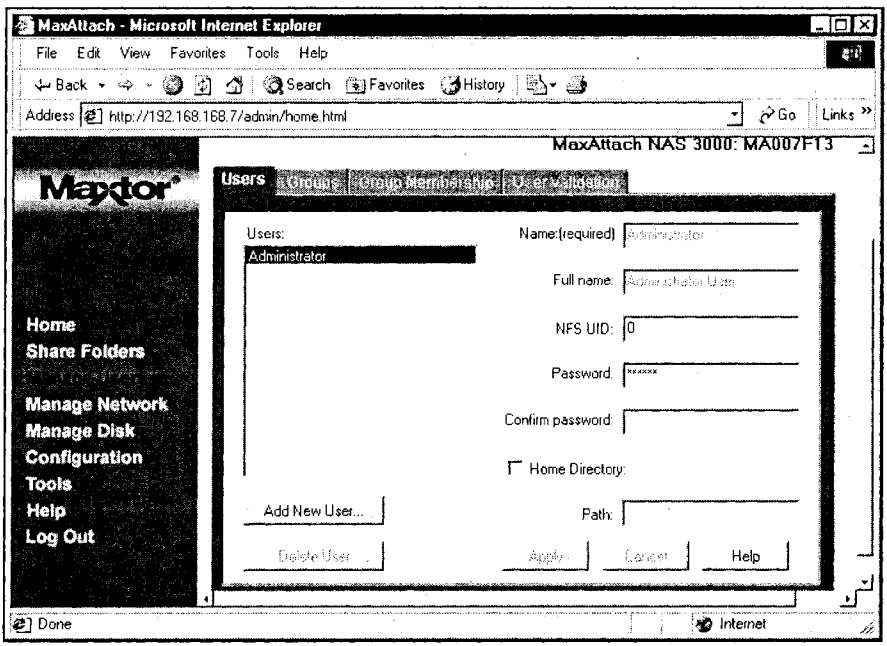


Рис. 18.7. Меню **Manage Users** позволяет координировать пользователей и группы, применяющие устройство NAS

Вы можете создать группу. *Группа* — это совокупность пользователей с одинаковыми правами доступа к каталогам. Распределение по группам особенно удобно, если вы хотите выделить одни и те же ресурсы и права большому количеству пользователей. Чтобы создать группу, перейдите на вкладку **Groups** в верхней части экрана. Нажмите кнопку **Add New Group**. Введите имя группы и нажмите кнопку **OK**. Перейдите на вкладку **Group Membership**, расположенную в верхней части экрана. Выберите пользователя или пользователей, которых вы хотите включить в данную группу. Выберите группу, нажмите кнопку **Add**, затем кнопку **Apply**. На вкладке **User Validation** вы можете выбрать метод проверки паролей.

Управление сетью

Если вам нужно настроить работу NAS в сети, выберите пункт меню **Manage Network** (рис. 18.8). Здесь вы можете изменять IP-адрес устройства, его обозначение (т. е. настройки имени или рабочей группы), настройки WINS и DHCP-сервера (в том случае, если вы хотите, чтобы устройство NAS предоставляло службы DHCP). Если устройство NAS обслуживается другим DHCP-сервером, автоматически получая IP-адрес и подсеть, перейдите на вкладку **Network** и установите флажок **Obtain**

an IP address from a DHCP server. Вкладка **Identification** позволяет задавать имена как самого устройства NAS, так и рабочих групп. Если вы пользуетесь WINS, вкладка **WINS** позволяет задействовать эту службу и ввести IP-адрес WINS-сервера. Если другие DHCP-серверы, которые могли бы обслуживать NAS, отсутствуют, откройте вкладку **DHCP Server** и задайте диапазон IP-адресов, за который данное устройство будет отвечать.

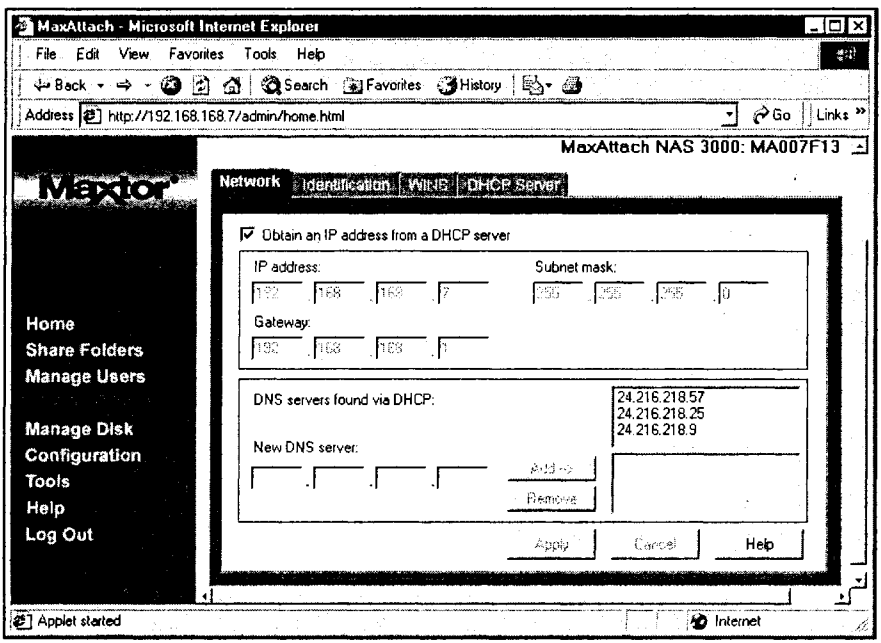


Рис. 18.8. Меню **Manage Network** позволяет вам регулировать поведение устройства NAS в сети

Управление дисками

Устройства NAS типа Maxtor NAS 3000, как правило, содержат несколько дисков для хранения данных. Если ваш NAS относится к этому типу, у вас есть возможность координировать применение дисков. По умолчанию NAS обычно объединяет несколько дисков, в результате чего получается единый, более крупный том. Например, NAS с двумя дисками по 60 Гбайт каждый может выполнить их объединение и получить один логический том объемом до 120 Гбайт. Вы можете воспользоваться меню **Manage Disk** (рис. 18.9) и выбрать одну из возможных конфигураций дисков, среди которых есть, например, такие:

- два отдельных диска (без RAID);
- один активный/один резервный диск (элементарное зеркальное копирование).

Естественно, более сложные устройства NAS с множеством дисков (например, четырьмя, шестью, восемью и более) могут поддерживать дополнительные схемы настройки. Внесение изменений в конфигурацию дисков подразумевает введение их в действие, а также переформатирование.

Поиск неисправностей NAS

Устройства NAS легко установить, они обеспечивают хорошую производительность и долговременную надежную работу в сети. Но у них тоже бывают сбои и неисправности. Как администратор или технический специалист, вы должны иметь представление о важных принципах сопровождения типичных устройств NAS, а также быть знакомым с наиболее распространенными неисправностями.

Службы DHCP

Если ваше устройство NAS поддерживает службы DHCP, то вам нужно учесть несколько специальных требований. Если вы устанавливаете NAS в сети, в которой службы DHCP уже предоставляются (обычно речь идет о сети с сервером или другим устройством со встроенными службами DHCP), то ваше устройство NAS автоматически получит IP-адрес — ничего в этом случае предпринимать не следует.

Если вы устанавливаете NAS в среду без DHCP-сервера, значит, NAS станет таким сервером. Это устройство получит статический адрес по умолчанию (т. е. 192.168.42.252) и подсеть по умолчанию (т. е. 255.255.255.0). Возможно, ваше устройство NAS поддерживает другие настройки по умолчанию, но приведенный пример вполне допустим. Чтобы настроить NAS, вам нужно получить доступ к компьютеру, адрес которого расположен в пределах данного диапазона IP-адресов. Возможно, вам придется временно изменить IP-адрес вашего компьютера. В противном случае при попытке выбора устройства NAS программа конфигурации NAS возвратит ошибку.

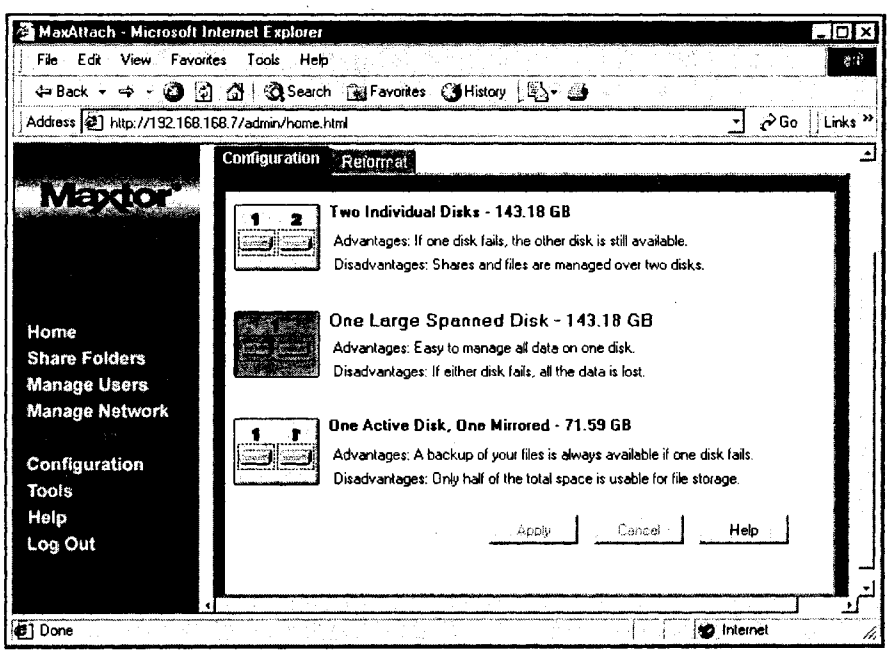


Рис. 18.9. Меню **Manage Disk** позволяет настраивать устройства NAS, содержащие несколько внутренних дисков

Если впоследствии вы решите переместить NAS в среду с DHCP (например, установить это устройство в другой подсети в рамках той же сети), нужно будет выполнить повторный выбор служб DHCP. Для этого откройте NAS в Web-браузере, зайдите в меню **Manage Network** и установите флажок **Obtain IP Address Automatically**. Если настройка перемещенного устройства NAS не будет выполнена заново, оно может вызывать нарушения в работе сети.

Использование предупреждений

При появлении неисправностей большинство устройств NAS генерируют сообщения об ошибке или диагностические сообщения, которые затем сохраняются в регистрационном файле. Если пользователь сообщает об ошибке при обращении к NAS, администратор или технический специалист должен в первую очередь проверить именно этот файл. После этого выбор мер по устранению ошибок можно основывать на сообщениях об ошибках. Maxtor NAS генерирует следующие предупредительные сообщения с низким приоритетом:

- наличие конфликта имени сервера;
- операционная система успешно обновлена;
- том 1 или 2 заполнен на 2%;
- том 1 или 2 заполнен на 90%;
- температура процессора слишком высока;
- напряжение процессора вне диапазона;
- зафиксировано пять неуспешных попыток введения административного пароля.

Maxtor NAS генерирует следующие предупредительные сообщения со средним приоритетом:

- все вышеперечисленные предупреждения с низким приоритетом;
- проходит проверка согласованности файловой системы;
- пользователь вышел за пределы доступного дискового пространства;
- зафиксирован дублированный IP-адрес;
- зафиксирована неисправность датчика температуры/напряжения процессора;
- проходит обновление операционной системы;
- обновление операционной системы было прервано или не удалось;
- зафиксирована ошибка SMART (диагностики диска).

Maxtor NAS генерирует следующие предупредительные сообщения с высоким приоритетом:

- все вышеперечисленные предупреждения с низким приоритетом;
- все вышеперечисленные предупреждения со средним приоритетом;
- высокая частота конфликтов в сети.

Очистка предупреждений

Проверку журнала предупреждений NAS необходимо проводить регулярно — это часть стандартной процедуры сопровождения. Она позволяет администратору выяв-

лять и устранять неисправности до того, как они становятся фатальными. Обычно для проверки и очистки предупреждений нужно сделать следующее.

1. Выберите пункт **Home**.
2. Если вкладка **Alerts** не отображается, нажмите кнопку **Alerts**.
3. Просмотрите предупреждения, перечисленные в окне **Alert**.
4. Чтобы ознакомиться с описанием предупреждения, выберите его и нажмите кнопку **Help**.
5. Чтобы очистить предупреждения, нажмите кнопку **Clear Alerts**.

Почтовые предупреждения

Вместо того чтобы проверять журнал NAS вручную, многие администраторы предпочитают получать предупреждения по электронной почте. Если ваше устройство NAS поддерживает отправку почтовых предупреждений (а в сети применяется почтовый сервер SMTP), то для запроса на отправку предупреждений по электронной почте нужно сделать следующее.

1. Выберите пункт **Tools**.
2. Если страница с вкладкой **E-mail** не отображается, нажмите кнопку **E-mail**.
3. Введите адрес вашего SMTP-сервера.
4. Введите адрес электронной почты, на который нужно отправлять сообщения (например, **John.Smith@yourcompany.com**).
5. Выберите уровень приоритета предупреждений, которые вы хотите получать (или все предупреждения).
6. Чтобы убедиться в том, что введенная информация об электронной почте верна, нажмите кнопку **Test**.
7. При нажатии кнопки **Test** NAS отправляет тестовое сообщение по указанному адресу электронной почты через указанный почтовый сервер. Если это сообщение будет принято, значит, все данные введены верно.
8. После проверки правильности введенной информации нажмите кнопку **Apply**.

Управление операционной системой

NAS является специализированным файловым сервером, на котором установлена собственная версия операционной системы от его производителя. Время от времени производители выпускают новые операционные системы, исправляя дефекты предыдущих версий, совершенствуя совместимость и повышая производительность. Обычно обновить операционную систему можно непосредственно с Web-сайта ее производителя. Прежде чем приступать к обновлению операционной системы, проверьте общее рабочее состояние устройства и получите последние данные о программном и аппаратном обеспечении данного файлового сервера. Например:

1. Обратитесь к программе управления NAS через Web-браузер.
2. Выберите пункт **Home**.
3. Если страница с вкладкой **General** не отображается, нажмите кнопку **General**.

4. Ознакомьтесь с информацией, представленной на этой странице. Среди общих рабочих данных часто указываются следующие:
   - *Версия операционной системы*, установленная в настоящее время.
   - *Дата инсталляции/обновления.* Дата установки (или последнего обновления) операционной системы.
   - *Идентификатор устройства.* Внутренний номер, идентифицирующий данное устройство NAS.
   - *Тип процессора.* Модель и тактовая частота процессора файлового сервера.
   - *Время работы сервера.* Промежуток времени с момента последнего перезапуска NAS.

Обновление операционной системы

Обычно производитель извещает пользователей о появлении новой версии операционной системы (он также указывает адрес файла для загрузки). Процесс обновления ОС, как правило, довольно безопасен, но его нужно запускать с компьютера, на котором установлен Web-браузер и который может получать доступ к сети Интернет. Так как по окончании процесса обновления файловый сервер перезапускается, не следует проводить обновления в то время, когда файловым сервером пользуются другие. Чтобы обновить операционную систему, сделайте следующее.

1. Обратитесь к программе управления NAS через Web-браузер.
2. Выберите пункт **Home**.
3. Если страница с вкладкой **General** не отображается, нажмите кнопку **General**.
4. Запишите идентификационный номер текущей версии операционной системы.
5. Выберите **Tools**.
6. Если страница с вкладкой **Update** не отображается, нажмите кнопку **Update**.
7. Выберите **Update**.
8. После открытия браузера следуйте инструкциям по загрузке новой ОС. Имейте в виду, что во время процесса обновления пользователи сети не смогут обращаться к NAS.
9. После перезагрузки NAS выберите пункт **Home**.
10. Если страница с вкладкой **General** не отображается, нажмите кнопку **General**.
11. Убедитесь в том, что на сервере работает новая версия ОС.

Обновить операционную систему чаще всего не удается по следующим причинам:

- ❒ во время обновления сетевое соединение было прервано;
- ❒ во время передачи файла с обновлением он был поврежден;
- ❒ устройство NAS прекратило получать питание;
- ❒ в NAS уже установлена последняя версия ОС;
- ❒ для загрузки обновления или его активации не хватает места на жестком диске.

Редактирование LMHOST

Если для администрирования NAS вы хотите использовать имена серверов (вместо IP-адресов), вам, вероятно, придется отредактировать или создать файл LMHOSTS. Для редактирования файла LMHOSTS сделайте следующее.

1. Если файл LMHOSTS уже существует (например, он может называться LMHOSTS.SAM), откройте его с помощью Notepad (Блокнот). Если файла LMHOSTS не существует, откройте пустой файл Notepad. Для редактирования файла сначала его нужно открыть и создать резервную копию (под другим именем — например, LMHOSTS.OLD). Таким образом, если в редактируемом файле LMHOSTS обнаружится ошибка, вы сможете восстановить его старую версию.
2. Введите ваш IP-адрес, пять пробелов, а затем предполагаемое имя сервера. Длина имени сервера не может превышать 15 символов. Все это должно выглядеть примерно так:

```
192.168.42.252     имя_сервера
```

3. После редактирования существующего файла LMHOST его следует сохранить под исходным именем. Если вы создали новый файл, сохраните его как LMHOST в подкаталоге Windows 9x (или в подкаталоге WINNT).
4. Перезагрузите компьютер. После перезагрузки файл LMHOST и новое имя сервера должны войти в силу.

Режим транзитной пересылки

Некоторые устройства NAS поддерживают *режим транзитной пересылки*, при котором информация о пользователях и группах берется с сервера главного контроллера домена (PDC, Primary Domain Controller). Это значит, что вам не придется создавать пользователей и группы в системе NAS и управлять ими по отдельности. Вам нужно лишь определить права доступа к локальным коллективным ресурсам и каталогам NAS. Следующие действия служат примером активации транзитного режима.

1. Откройте вкладку **Manage Users**, выберите **User Validation** и нажмите кнопку **Passthrough**.
2. Введите имя сервера NetBIOS.
3. Введите IP-адрес главного контроллера домена и нажмите кнопку **Apply**.
4. В окне предупреждения выберите **Yes**, в результате предыдущая конфигурация и права пользователей будут удалены. После этого появится еще одно окно предупреждения, напоминающее о необходимости перезагрузки системы. Чтобы выполнить перезагрузку, нажмите кнопку **OK**. Транзитный режим активирован.
5. Войдите в меню **Tools** и откройте вкладку **Shutdown**.
6. Определите количество минут до отключения системы (для получения незамедлительной реакции укажите 0) и нажмите кнопку **Restart**. Теперь ваша система находится в транзитном режиме.

Откройте вкладку **Manage Users**. Теперь система должна отображать пользователей и группы в соответствии с данными главного контроллера домена NT. Если списки пользователей и групп отсутствует, значит, обращение к коллективному ресурсу или папке на устройстве NAS разрешено всем. Это должно инициировать загрузку базы

данных. Выберите **Refresh** в окне браузера, после чего появятся обозначения групп. Чтобы изменения вступили в силу, вы должны выйти из системы (выходить из NAS нет необходимости). Чтобы выйти из системы, перезагрузите рабочую станцию.

Примечание

Главный контроллер домена NT не обеспечивает прав доступа к совместно используемым ресурсам NAS; он лишь выполняет проверку правильности паролей пользователей и членство в группах. Права доступа к коллективным ресурсам необходимо устанавливать в NAS

Резервирование/восстановление NAS

Несмотря на то, что NAS можно настроить на выполнение операций RAID, для защиты важных данных все равно требуется полное резервирование. Впоследствии, если в этом возникнет необходимость, на основе резервных данных можно будет провести восстановление. В этом разделе в общих чертах рассматривается процесс резервирования и восстановления файлов на обычном устройстве NAS. Например, чтобы выполнить резервирование существующих данных NAS, необходимо сделать следующее.

1. На рабочей станции зарегистрируйтесь в NAS как администратор.
2. Выберите пункт **Tools** главного меню; в результате появится окно программы **Tools**.
3. Откройте вкладку **Backup** и нажмите кнопку **Backup Now**. Резервная копия будет сохранена как config.dat в каталоге \\vol1\st_backup. После завершения операции появится окно резервирования, сообщающее об успешном резервировании настроек конфигурации. Чтобы продолжить, нажмите кнопку **OK**.
4. Выберите пункт **Share Folders** главного меню; в результате появится программа **Share Folders**.
5. Откройте вкладку **Shares**, выделите каталог \st_backup и установите переключатель в положение **Shared**. В специально предусмотренном окне появится имя каталога \st_backup. Чтобы сохранить изменения, нажмите кнопку **Apply**.
6. Откройте вкладку **User Access**, выберите **User Administrator** и установите переключатель в положение **Read/Write**. Чтобы сохранить изменения, нажмите кнопку **Apply**.
7. Скопируйте каталог \\vol1\st_backup в другой сетевой коллективный каталог или на локальный жесткий диск.
8. Выполните резервирование данных, расположенных в NAS, с помощью стандартной программы резервирования (например, Veritas Backup Exec, Computer Associates ArcServe, Native NT Backup и т. д.). Если у вас нет подобного приложения, можете скопировать данные в другой источник (например, сетевой коллективный каталог или локальный жесткий диск).
9. Выключите устройство NAS.

Восстановление данных в устройстве NAS производится следующим образом.

1. Подключите новое устройство NAS к силовому и сетевому кабелю и подведите к нему питание.

2. Запустите программное обеспечение NAS с системы, на которой оно установлено, и введите всю необходимую информацию. Новому устройству необходимо присвоить старый пароль, сетевое имя и IP-адрес.
3. Войдите в устройство NAS как администратор, затем выберите пункт **Manage Disks** главного меню.
4. Настройте устройство NAS на применение той же конфигурации дисков (зеркальное копирование, простой массив дисков или стягивание), что использовалась на старом устройстве. После завершения конфигурации дисков перезагрузите устройство NAS.
5. Восстановите структуру файлов и каталогов из программы резервирования (или из копии данных). После завершения восстановления перезагрузите устройство NAS.
6. Еще раз войдите в устройство NAS как администратор.
7. Выберите пункт **Tools** главного меню; в результате появится программа **Tools**.
8. Откройте вкладку **Restore** и выберите файл config.dat, который ранее был скопирован в сетевой коллективный каталог (или на локальный жесткий диск). Выбрав этот файл, нажмите кнопку **Restore Now**.
9. После восстановления файла config.dat перезагрузите устройство NAS.
10. На этом этапе структура файлов и каталогов должна быть идентична исходной (в старом устройстве). Полномочия пользователей и групп также должны быть аналогичны тем, что были приняты на старом устройстве NAS. Проверьте возможность доступа. Для этого нужно, чтобы несколько пользователей зарегистрировались на устройстве и обратились к коллективным ресурсам.

Симптомы неисправностей

Большинство устройств NAS были разработаны для того, чтобы обеспечить технологии хранения по модели Plug-and-Play, но при работе с ними могут появляться некоторые неисправности. Большая их часть устраняется посредством визуальных проверок и изменений в конфигурации, но в этой части главы мы сосредоточимся на ряде характерных проблем, для решения которых требуются строго определенные корректирующие действия.

Симптом 18.1. Невозможно администрирование устройства NAS

В первую очередь необходимо проверить питание и соединения. Убедитесь в том, что устройство NAS подключено к источнику питания и его контрольная лампа светится. При необходимости подключите устройство и подведите к нему питание. Если устройство уже включено, проверьте, светится ли светодиод подключения к сети. Если он не работает, проверьте кабельное соединение с сетью. Пользуйтесь только тем кабелем, который входил в комплект данного устройства. Подключите кабель к коннектору с маркировкой "LAN", находящемуся на задней панели NAS. Подключите другой конец кабеля к подходящему сетевому коннектору (например, 10/100BaseT Ethernet) на концентраторе или коммутаторе. Попытайтесь воспользоваться другим портом на концентраторе или коммутаторе или другим сетевым кабелем. Старайтесь не использовать "связной" порт концентратора или коммутатора. Им можно пользоваться только в том случае, если переключатель **Uplink** установлен

в нужное положение. Не подключайте кабель непосредственно к настольному компьютеру или ноутбуку, если у вас нет специального кроссоверного кабеля для NAS (его следует приобрести отдельно). Если неисправность сохранится, перезагрузите NAS. Если она не исчезнет после перезагрузки, возможно, что устройство NAS неисправно и требует замены.

Симптом 18.2. Устройство NAS не удается обнаружить в сети

Например, вам не удается обнаружить устройство в каталоге Network Neighborhood (Сетевое окружение, Windows 9x) или My Network Places (Мое сетевое окружение, Windows 2000). Начните с выполнения предложений, представленных в неисправности 18.1. Если устройство NAS отключено или включено, но ненадежно, или соответствующий порт концентратора или коммутатора неисправен, это устройство не сможет осуществлять обмен информацией по сети (и, соответственно, не будет в ней обнаружено). Убедитесь в том, что NAS находится в той же рабочей группе, что и компьютер, которым вы в данный момент пользуетесь. Для этого откройте каталог Network Neighborhood или My Network Places и дважды щелкните на **Entire Network**. Найдите имя рабочей группы устройства NAS (например, "Workgroup"). Если имя группы NAS есть в списке, дважды щелкните на имени этого устройства, и оно должно появиться. В примере, показанном на рис. 18.10, возможно использование устройства NAS MA007F13, а также сервера SERVER01.

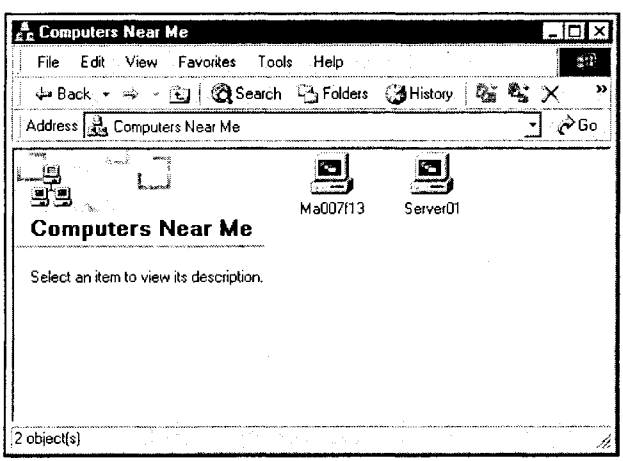


Рис. 18.10. Обнаружение устройства NAS в рамках сети не представляет трудности; перемещаться по нему можно так же, как и по любому другому устройству хранения

Если устройство NAS не отображается в среде Windows 9x, последовательно выберите **Start** (Пуск), **Find** (Поиск), **Computer** (Компьютер). Введите имя устройства NAS (например, MA007F13) и нажмите кнопку **Find Now** (Найти). Компьютер выполнит поиск указанного имени устройства, и в случае, если он его найдет, имя будет отображено. Чтобы просмотреть коллективный ресурс, дважды щелкните на имени. В операционной системе Windows 2000 поиск производится после выбора пункта **Entire Network** (Вся сеть) в диалоговом окне **My Network Places** (Мое сетевое окружение). Если неисправность сохранится, перезагрузите NAS и определите, устранена

ли она. Если она до сих пор присутствует, вполне возможно, что устройство NAS неисправно и требует замены.

Симптом 18.3. Программа администрирования выводится на экран некорректно

Управляете ли вы NAS через Web-браузер? Если нет, то, прежде чем вы сможете обратиться к NAS, вам нужно установить на административной консоли специальную утилиту управления NAS. Если у вас есть возможность управления NAS с помощью Web-браузера, то вы должны пользоваться его соответствующей версией (например, IE 4.01 или более поздней). Если версия Web-браузера, которой вы пользуетесь, подходит для рассматриваемых целей, проверьте, может ли он отображать Java-апплеты и принимать "куки" (Cookies). Если соответствующие настройки не выполнены, административная программа может отображаться некорректно (или не отображаться вообще).

Симптом 18.4. Пароль администратора утерян

Выполните сброс устройства NAS. Некоторые устройства NAS сбрасываются путем нажатия кнопки Reset при подаче питания. Для сброса других устройств их необходимо сначала отключить, а затем с помощью шариковой ручки нажать кнопку Reset, расположенную на задней панели устройства, и уже после этого восстановить подачу питания. Кнопку Reset следует удерживать в течение 3—5 секунд. После сброса файлового сервера все тома данных и база данных безопасности будут сохранены, а все настройки утеряны. При последующей перезагрузке файлового сервера он определяет себя как совершенно новую систему. Устройство должно будет пройти настройку с помощью мастера Configuration Wizard, как и при первоначальной настройке. Нужно также переназначить IP-адрес устройства. Настройкам WINS будет возвращено исходное состояние (т. е. будут отсутствовать). Если вы создали копию настроек конфигурации, теперь, руководствуясь инструкциям производителя, их можно восстановить.

Симптом 18.5. Появляется сообщение об ошибке, в соответствии с которым "дисковое зеркало" находится в вырожденном состоянии

Если ваше устройство NAS настроено на зеркальное копирование дисков, эта ошибка означает, что один из двух дисков в рамках дублированной пары работает с ошибками (или вообще отсутствует). При этом другой диск функционирует и осуществляет сопровождение ваших данных. Если вам известно, что один из дисков физически отсутствует (например, он демонтирован для последующей замены), это предупреждение можно просто проигнорировать, т. к. после замены отсутствующего диска оно не будет появляться. Впрочем, в случае, если оба диска установлены, возможно, вы имеете дело с серьезной неисправностью оборудования. Отключите устройство NAS и перезапустите его. Если неисправность не исчезла, можно предположить, что диск вышел из строя и его нужно заменить.

Симптом 18.6. Появляется сообщение об ошибке, в соответствии с которым дублированный диск неисправен

Это сообщение обозначает, что оба диска из дублированной пары имеют ошибки. Как правило, в этой ситуации можно сделать вывод о том, что данные, хранящиеся

в NAS, скомпрометированы (и, возможно, недоступны). Выключите NAS и перезапустите его. Если неисправность не исчезла, то вам придется заменить неисправные диски или устройство NAS. В любом случае, вы должны восстановить содержимое массива дублированных дисков с помощью недавно созданной резервной копии.

Симптом 18.7. Появляется сообщение об ошибке, в соответствии с которым том диска заполнен

Это простая ошибка. Она означает, что на томе, обозначенном в предупреждении, не осталось свободного места для хранения файлов. Удалите неиспользуемые файлы (например, старые файлы или дополнительные копии рабочих файлов). Имейте в виду, что операции удаления файлов нельзя выполнять через программу администрирования. Для этих целей вам следует воспользоваться Windows Explorer (или другим инструментом управления). Вы также можете переместить некоторые файлы в другое место (например, на резервную магнитную ленту или на другой файловой сервер в сети). Если это предупреждение будет появляться, попробуйте установить в NAS второй диск, воспользоваться дисками большей емкости или поставить в сеть еще одно устройство NAS.

Симптом 18.8. Появляется сообщение об ошибке, в соответствии с которым фиксируется большое количество ошибок дисков

Ошибка этого типа указывает на наличие серьезных неисправностей одного или нескольких жестких дисков, установленных в устройстве NAS. Можете попытаться устранить неисправность путем выключения NAS с его последующей перезагрузкой. Если поступление сообщений об этой ошибке не прекратится, вполне возможно, что NAS нуждается в ремонте или замене у производителя.

Симптом 18.9. Появляется сообщение об ошибке, в соответствии с которым на диске осталось мало места

Как правило, эта ошибка означает, что на диске осталось лишь 10% свободного пространства, пригодного для хранения файлов. Удалите неиспользуемые файлы (например, старые файлы или дополнительные копии рабочих файлов). Имейте в виду, что операции удаления файлов нельзя выполнять через программу администрирования. Для этих целей вам следует воспользоваться Windows Explorer (или другим инструментом управления). Вы также можете переместить некоторые файлы в другое место (например, на резервную магнитную ленту или на другой файловой сервер в сети). Если это предупреждение будет появляться, попробуйте установить в NAS второй диск, воспользоваться дисками большей емкости или поставить в сеть еще одно устройство NAS.

Симптом 18.10. Появляется сообщение об ошибке, в соответствии с которым пользователь с указанным IP-адресом осуществил 5 неудачных попыток введения пароля

Один из пользователей вашей сети (IP-адрес, приведенный в сообщении, должен определить компьютер, за которым он работает) пытался зарегистрироваться как администратор по меньшей мере 5 раз, но в сочетании с именем пользователя "Administrator" вводил неверный пароль. Это серьезная брешь в системе защиты (попытка несанкционированного проникновения), которая должна быть немедленно устранена. Вполне возможно, что указанный пользователь допускал и другие нарушения.

Симптом 18.11. Предупреждения от NAS не приходят на ваш почтовый ящик

Вы настроили NAS на отправку предупреждений по электронной почте, но вы их не получаете. Практически во всех случаях происхождение этой неисправности можно отнести к ошибкам в конфигурации NAS. В первую очередь убедитесь в том, что указанный вами почтовый сервер действительно является SMTP-сервером. Например, чтобы определить, какой сервер вы указали, выберите пункт **Tools** и выведите страницу с вкладкой **E-mail**. Убедитесь в том, что этот почтовый сервер напрямую подключен к вашей сети. Если почтовый сервер становится доступным лишь после дозвона до сети (или установления другого непрямого соединения), вы не сможете получать почтовые предупреждения.

Попробуйте инициировать отправку тестового сообщения для подтверждения правильности введенных данных электронной почты. Чтобы отправить тестовое сообщение, выберите пункт **Tools**, перейдите на страницу с вкладкой **E-mail** и нажмите кнопку **Test**. Определите, какой приоритет предупреждений определен на вкладке — низкий (**Low**), средний (**Medium**) или высокий (**High**). Если вы выбрали **None**, предупреждения отсылаться не будут. Наконец, если почтовый сервер получает свой IP-адрес от DHCP-сервера, убедитесь в том, что он также получает имя хоста. Именно так сервер получает доменное имя DNS.

Симптом 18.12. Пользователь просматривает содержимое NAS, но ему не удается сохранить файлы в определенном каталоге

В большинстве случаев эта неисправность оказывается связанной с совместным использованием ресурсов. Убедитесь в том, что каталог, к которому пользователь пытается обратиться, является совместно используемым (все такие каталоги обозначаются пиктограммой руки). Проверьте, есть ли у пользователя права на чтение/запись (Read/Write) данных в этот каталог (а также в его надкаталоги). Например, чтобы проверить полномочия пользователя, выберите пункт **Share Folder**, выведите страницу с вкладкой **User Access** и укажите в пределах дерева каталогов тот каталог, который вам нужен. Выясните, какие права доступа предоставлены данному пользователю (и к каким группам он принадлежит). Внесите необходимые изменения в полномочия пользователя.

Симптом 18.13. Не удается обновить операционную систему NAS

Обычно обновление операционной системы NAS можно загрузить и установить непосредственно с Web-сайта производителя. Сообщение, подобное следующему:

```
Unit has not been updated successfully with a new operating system
```

означает, что загрузить и инсталлировать операционную систему не удалось. Как правило, после этого NAS возвращается к ОС, установленной в этом устройстве до попытки загрузить новую версию. Вы можете либо продолжать пользоваться текущей версией, либо попытаться провести загрузку еще раз (проверьте, действительно ли вы загружаете нужный файл операционной системы). Если проблема сохранится, проверьте текущую версию ОС и обратитесь к производителю NAS за дополнительной помощью. Возможно, вам придется загрузить другой файл или вернуть устройство производителю для ремонта. Дополнительная информация по этой неисправности представлена ранее в *разд. "Управление операционной системой" данной главы.*

Серверы компакт-дисков

В оживленных сетях часто возникает необходимость в совместном доступе к компакт-дискам. Как правило, эта задача решается посредством дисководов с автоматической сменой компакт-дисков. В то же время в качестве ценной альтернативы позиционируются серверы компакт-дисков (подобные модели Linksys 20GB GigaCD Server, показанной на рис. 18.11). С них пользователи могут загружать часто применяемые компакт-диски, диски с графикой и стандартными аудиоданными, игры и другие востребованные компакт-диски; в результате их не приходится искать и передавать другим пользователям. Применение сервера компакт-дисков приводит к тому, что к данным, расположенным на CD-ROM, может одновременно обращаться множество пользователей сети (через Network Neighborhood). Если на вашем сетевом ПК нет привода CD-ROM, вы можете обратиться к серверу компакт-дисков и воспользоваться хранящимися на нем данными. Например, сервер компакт-дисков позволяет:

- организовывать совместный доступ к компакт-дискам в рамках всей сети;
- запускать приложения, хранящиеся на компакт-дисках, не имея в составе собственной рабочей станции привода CD-ROM;
- хранить до 30 полных (объемом 650 Мбайт) компакт-дисков;
- пользоваться всеми форматами Audio-CD;
- применять функции удаленного мониторинга и закрытия систем;
- обновлять микропрограммное обеспечение любой системы, подключенной к сети;
- выполнять функции DHCP-сервера или клиента.

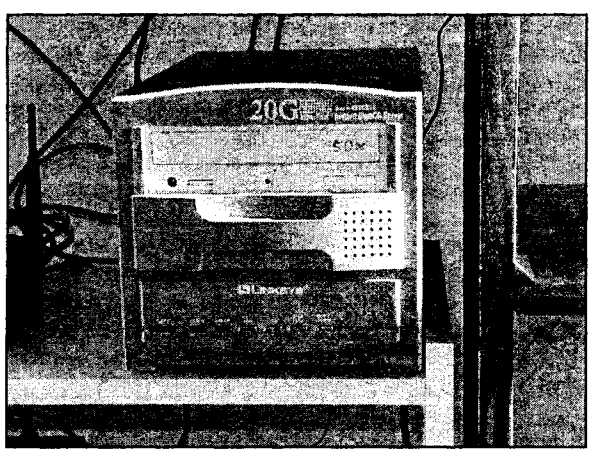


Рис. 18.11. Сервер компакт-дисков Linksys GigaCD позволяет хранить образы компакт-дисков таким образом, чтобы к ним могли обращаться все пользователи сети

Подобно файловым серверам на основе жестких дисков, к которым относится и Maxtor NAS, файловые серверы компакт-дисков представляют собой в высшей степени специализированные сетевые устройства, спроектированные в расчете на инте-

грацию в сеть с минимальными проблемами, связанными с установкой и конфигурацией. Все, что от вас требуется — это вставить компакт-диск в привод и скопировать его на внутренний диск — после этого образ диска будет доступен всем пользователям сети.

Назначение индикаторов

Специализированные устройства хранения (типа Linksys GigaCD Server) содержат ряд индикаторов, сообщающих информацию об их состоянии и любых возможных неисправностях. Прежде чем устанавливать устройство, уделите некоторое время на ознакомление с теми индикаторами, которые на нем установлены. В типичный комплект входят следующие индикаторы.

- *Ready* (готовность). Этот зеленый светодиод мигает во время запуска и отключения устройства, а по завершении этих операций гаснет. В процессе обновления программного обеспечения мигают два светодиода: готовность и ошибка.
- *Error* (ошибка). Этот желтый светодиод мигает во время запуска системы. Если после завершения этой операции он продолжает сигнализировать, значит, в аппаратном обеспечении устройства присутствует неисправность. В процессе обновления программного обеспечения мигают два светодиода: готовность и ошибка.
- *LAN* (подключение к локальной сети). Этот зеленый светодиод начинает сигнализировать при установлении сетевого соединения. В процессе отправки и получения данных по сети он мигает.
- *Disk* (диск). Этот зеленый светодиод мигает при каждом обращении к внутреннему жесткому диску устройства.
- *Disk Full* (заполнение диска). В нормальной ситуации этот зеленый светодиод не светится. Начиная мигать, он сообщает о том, что жесткий диск заполнен на 98%; постоянное свечение обозначает полное заполнение жесткого диска.
- *Copy Error* (ошибка при копировании). В нормальной ситуации этот желтый светодиод не светится. Он загорается, если в процессе копирования образа происходит ошибка и продолжает сигнализировать, пока компакт-диск не будет извлечен из дисковода.

Звуковые индикаторы

В специализированных устройствах хранения типа GigaCD Server часто используются звуковые сигналы. Они оповещают о ключевых событиях и ошибках устройств, требующих внимания. Информационные оповещения и сообщения об ошибках подаются звуковыми индикаторами следующим образом.

- *Один звуковой сигнал.* Произошло нажатие кнопки **Reset IP/Password** или **Power Switch**.
- *Два звуковых сигнала.* Как правило, эта схема повторяется каждые пять секунд в течение одной минуты. Она означает, что сервер является DHCP-клиентом, но на клиентский запрос DHCP не ответил ни один DHCP-сервер.
- *Три звуковых сигнала.* Обычно эта схема повторяется каждые 15 секунд в течение трех минут. Жесткий диск сервера заполнен более чем на 98%.

- *Пять звуковых сигналов.* Как правило, эта схема повторяется каждые 15 секунд в течение трех минут. Произошел перегрев сервера. В таких условиях некоторые серверы автоматически отключаются (через три минуты после первого звукового сигнала).

Основы установки

Так как серверы компакт-дисков, по существу, представляют собой специализированные компьютеры, их установка обычно состоит из подключения устройства к свободному сетевому порту с последующей инсталляцией программной утилиты на административной консоли. Впрочем, доступ к серверу компакт-дисков и управление им через интерфейс Web-браузера может производиться с любой станции. Обычно процесс установки состоит из следующих этапов (возможно, в случае с вашим сервером компакт-дисков это делается по-другому).

1. Проведите сетевой кабель из порта RJ-45 на задней панели сервера к концентратору или коммутатору, к которому этот сервер предполагается подключить. Сервер выполнит автоматическое распознавание скорости соединения (10BaseT или 100BaseT) и его режима (полнодуплексный или полудуплексный).
2. Подсоедините сервер компакт-дисков к источнику переменного тока и включите его.
3. Понаблюдайте за ходом процесса запуска. Во время этого процесса светодиоды устройства (готовности, ошибки, заполнения диска и ошибки при копировании) будут мигать или сигнализировать в течение нескольких секунд. Если после завершения загрузки светодиод ошибки будет продолжать сигнализировать, значит, вы имеете дело с аппаратной неисправностью. В противном случае процесс монтажа аппаратной части можно считать, в основном, завершенным.
4. Теперь нужно установить на административном компьютере все необходимое программное обеспечение. Вставьте в дисковод вашего компьютера соответствующий установочный диск. Программа установки (Setup) должна запуститься автоматически (в противном случае выполните программу setup.exe на компакт-диске).
5. Установите флажок **Administrator Installation** и следуйте приглашениям по установке утилиты управления сервером компакт-дисков, а после завершения этого процесса запустите ее.
6. При появлении главного меню (рис. 18.12) выберите сервер компакт-дисков, который предполагается настроить. При появлении приглашения на ввод пароля нажмите кнопку **OK** (по умолчанию пароль отсутствует). Щелкните на пиктограмме **Setup** и запустите быструю установку (**Quick Setup**). Типичные опции **Quick Setup** приведены в табл. 18.2. После сохранения записей **Quick Setup** сервер компакт-дисков будет приведен в рабочее состояние.

Примечание

Не забудьте добавить сервер компакт-дисков и его характеристики (IP-адрес, MAC-адрес и имя устройства) в сетевую документацию.

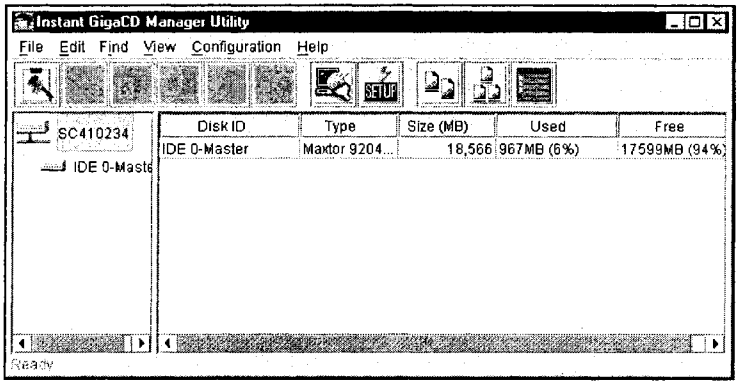


Рис. 18.12. CD Manager перечисляет все серверы компакт-дисков данной сети

Таблица 18.2. *Типичные опции* ***Quick Setup*** *для сервера Linksys GigaCD*

Настройка	**Пояснение**
Свойства сервера:	
Server Name (Имя сервера)	Выводит имя по умолчанию, которое можно изменить на любое другое
Comment (Комментарий)	Здесь можно фиксировать любые комментарии
Date/Time (Дата/время)	Здесь производится установка системного времени
Time Zone (Часовой пояс)	Здесь производится установка вашего часового пояса
Свойства TCP/IP:	
Obtain IP Address Automatically (Автоматическое получение IP-адреса)	Эту настройку можно активировать лишь в том случае, если к вашей локальной сети подключен DHCP- или BOOTP-сервер, который может выделять серверу компакт-дисков IP-адрес. Так как речь все же идет о сервере, лучше всего пользоваться фиксированным IP-адресом
Fixed IP Address (Фиксированный IP-адрес)	Здесь вы можете ввести фиксированный IP-адрес
IP Address (IP-адрес)	**Quick Setup** предложит свободные значения в пределах адресного диапазона, применяемого в данном сегменте локальной сети. Если предложенное значение в данный момент применяется устройством, находящимся в отключенном состоянии, следует изменить адрес на неиспользуемый
Network Mask (Маска подсети)	Здесь должны указываться те значения, которыми располагают все прочие компьютеры в вашей локальной сети. Значение по умолчанию для сервера компакт-дисков — 255.255.255.0

Таблица 18.2 (окончание)

Настройка	Пояснение
Gateway (Шлюз)	Здесь следует использовать те же значения, которые установлены на других компьютерах в вашей локальной сети
Enable DHCP Server (Задействовать DHCP-сервер)	Если этот флажок установлен, сервер компакт-дисков будет выполнять функцию снабжения других компьютеров в данной сети IP-адресами и сопутствующими данными. Компьютеры могут запрашивать такие данные только в том случае, если они настроены как DHCP-клиенты
Start IP Address (Начальный IP-адрес)	Первое значение IP-адреса из тех, что могут назначаться данным DHCP-сервером
Finish IP Address (Конечный IP-адрес)	Завершающее значение IP-адреса из тех, что могут назначаться данным DHCP-сервером. Диапазон между начальным и конечным IP-адресами должен быть достаточным для того, чтобы адресов хватило на всех DHCP-клиентов
Свойства Microsoft Networking:	
Workgroup Name (Имя рабочей группы)	Это имя должно согласовываться с тем именем, которое применяется другими компьютерами в вашей локальной сети
Code Page (Кодовая страница)	Вы можете указать регион, в котором будет работать ваш сервер компакт-дисков

Управление сервером компакт-дисков

После выполнения начальной настройки сервера компакт-дисков вы можете пользоваться утилитой управления сервером. С ее помощью осуществляется выбор сервера и координируется его деятельность. Например, Linksys GigaCD Server поддерживает управляющее ПО, которое позволяет устанавливать пароли, управлять системными настройками, вносить изменения в настройку сети и пользоваться встроенными утилитами. В этой части главы мы рассмотрим примеры опций управления сервером компакт-дисков.

Как правило, администрирование сервера компакт-дисков начинается с запуска управляющего программного обеспечения с административного компьютера (или, если ваше устройство поддерживает этот метод, с обращения к серверу компакт-дисков через Web-браузер). Сначала программа управления автоматически осуществляет поиск серверов компакт-дисков в сети, а после этого выводится ее основной экран (см. рис. 18.12). Перед вами появляется перечень всех серверов компакт-дисков, в данный момент подключенных к вашей сети. Выделите сервер, к которому вы хотите обратиться (если для него установлен пароль, вам придется его ввести). После определения сервера компакт-дисков будут перечислены все его внутренние

"кабинеты"; при выборе одного из этих отделений вы увидите список расположенных в нем образов компакт-дисков.

Примечание

Если ваш сервер компакт-дисков позволяет задавать пароль (большинство подобных устройств поддерживают эту функцию), его лучше определить на этапе первоначальной настройки устройства. Это позволит защитить сервер компакт-дисков от несанкционированных изменений настроек. Обязательно запишите пароль и спрячьте в таком месте, где его никто не сможет увидеть.

Конфигурация системы

Варианты конфигурации системы, как правило, охватывают большую часть рабочих параметров устройства. Общие настройки обеспечивают возможность задать имя, которое будет применяться сервером компакт-дисков в системе. Вы также можете установить дату и время. Настройки копирования позволяют выбрать принимаемое по умолчанию размещение сохраняемых образов компакт-дисков в сети. Почтовые опции дают возможность настроить отправку сообщений по электронной почте. Они будут приходить вам или другому администратору в случае возникновения неисправностей сервера компакт-дисков (если, ваш сервер компакт-дисков поддерживает эту функцию). Наконец, опции отключения системы позволяют задавать время и дату отключения сервера компакт-дисков (или реакцию на события отключения).

Общие настройки

Общие настройки, как правило, задаются на этапе первоначального конфигурирования сервера, но отредактировать их можно и на вкладке **General** (рис. 18.13). Эта возможность оказывается особенно полезной при перемещении сервера компакт-дисков на новое место или в новую сеть, а также при определении летнего времени.

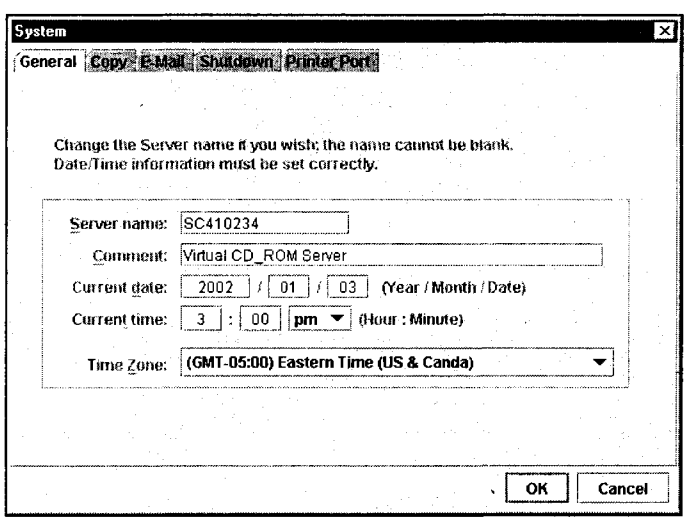


Рис. 18.13. Общие настройки позволяют вносить в конфигурацию сервера компакт-дисков элементарные изменения

- **Server name** (Имя сервера). Здесь вы можете изменить сетевое имя данного сервера компакт-дисков. Не забывайте, что после выполнения этого действия все ссылки, установленные на различные объекты на этом сервере, работать не будут. В состав имени сервера не могут входить знаки пунктуации и специальные символы (например, %#@).
- **Comment** (Комментарий). Это удобное поле позволяет ввести комментарий к серверу компакт-дисков. Ему можно найти практическое применение. Например, можно ввести физическое расположение сервера или контактную информацию администратора.
- **Current date/Current time** (Текущая дата/Текущее время). Внутренний календарь сервера устанавливается в соответствии с данными, вводимыми в эти поля.
- **Time Zone** (Часовой пояс). Найдите и выберите подходящий часовой пояс.

Настройки копирования

Опции копирования позволяют установить принимаемое по умолчанию место нахождения образов CD, копируемых с сервера (рис. 18.14). Эта информация имеет особую важность, т. к. она влияет на расположение информации компакт-дисков.

- **Select disk** (Выбор диска). Выберите внутренний жесткий диск, который вы хотите активировать как принятое по умолчанию место размещения файлов с образами компакт-дисков.
- **Cabinet name** (Имя отделения). Введите имя отделения (или каталога), который предполагается использовать как принятое по умолчанию место размещения образов CD. Если указанного отделения не существует, он будет создан.
- **Image name** (Имя образа). Введите имя, которое предполагается сделать принятым по умолчанию именем образа. Оно будет применяться только в том случае, если имя тома на компакт-диске окажется пустым.

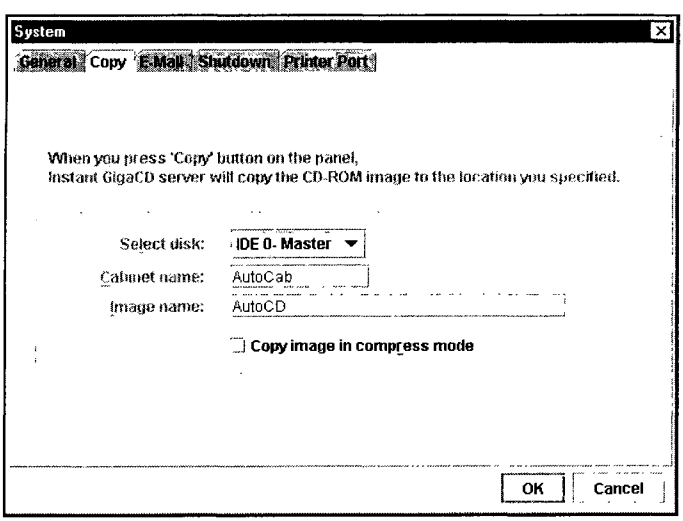


Рис. 18.14. Опции копирования позволяют задавать расположение файлов с образами компакт-дисков

- **Copy image in compress mode** (Копировать образ в сжатом режиме). Чтобы сохранять образы компакт-дисков в сжатом формате, следует установить этот флажок. Впрочем, если образ компакт-диска сжат, совместное использование его файлов становится невозможным, т. к. сжатый файл образа не может считываться другими компьютерами.

Почтовые настройки

Некоторые серверы компакт-дисков поддерживают отправку электронных сообщений для предупреждения администратора или уполномоченного технического специалиста. В загруженных сетях, где неисправности должны быть выявлены и устранены как можно скорее, эта функция может оказаться очень полезной. Чтобы принимать электронные сообщения, вы должны активировать поддержку электронной почты, ввести почтовый адрес и обозначить для них строку темы (например, "CD Server Problem").

Примечание

Если вы решили активировать отправку почтовых сообщений, обязательно протестируйте систему рассылки.

Настройки отключения системы

Некоторые серверы компакт-дисков поддерживают механизм отключения или планируют регулярные отключения в целях сопровождения и обслуживания устройства. С помощью диалогового окна **Shutdown** вы можете при первой необходимости отключить или перезагрузить сервер или определить расписание отключений. После отключения системы вы должны вручную включить сервер. Среди типичных опций есть следующие.

- **Reboot** (Перезагрузка). Чтобы перезагрузить сервер по требованию, выберите этот вариант.
- **Shutdown now** (Немедленное отключение). Чтобы немедленно отключить сервер, выберите эту опцию. После отключения сервер не будет перезапускаться.
- **Start** (Начало). Эта кнопка инициирует выбранное действие.
- **Weekdays/Saturday/Sunday** (Будние дни/суббота/воскресенье). Для того чтобы запланировать отключение, пометьте соответствующий флажок; затем введите время, когда планируется включить сервер.
- **Save** (Сохранение). Эта кнопка сохраняет запланированные данные.

Настройки сети

Возможности настройки сети, как правило, охватывают неисправности, связанные с работой сети. Вкладка **TCP/IP** позволяет редактировать IP-адрес и сопровождающие данные (включая функцию DHCP-сервера). Таблица **DNS** дает возможность настраивать записи DNS. Вкладка **Networking** организует информацию, необходимую для идентификации устройства (например, Workgroup Name и Code Page).

Настройки TCP/IP

Для редактирования настроек DHCP и IP-адреса вы можете воспользоваться диалоговым окном **Network**, вкладка **TCP/IP** (рис. 18.15). Обычно эти параметры задаются

на этапе первоначальной настройки устройства, но при необходимости в них можно вносить изменения.

- **DHCP client** (DHCP-клиент). Сервер DHCP назначает IP-адреса компьютерам и другим устройствам сети. Если в вашей сети есть DHCP-сервер, эту опцию нужно активировать.
- **Fixed IP address** (Фиксированный IP-адрес). Если в вашей сети нет DHCP-сервера, выберите эту опцию и введите соответствующие IP-данные.
- **IP address** (IP-адрес). Выбранный IP-адрес должен быть незанятым и совместимым с другими устройствами, расположенными в сети. Обычно это означает, что первые три поля должны быть такими же, как на вашем компьютере, а последнее поле должно занимать свободный номер между 1 и 254.
- **Network mask** (Маска сети). Указанная здесь маска сети должна быть согласована с другими устройствами в сети.
- **Gateway (Router)** (Шлюз/маршрутизатор). Если в вашей сети есть маршрутизатор или другой шлюз, введите его IP-адрес.
- **Enable DHCP Server** (Задействовать DHCP-сервер). Если этот флажок установлен, данный сервер будет назначать IP-адреса и сопутствующие данные другим подключенным к сети компьютерам по их требованию. Чтобы этой функцией можно было воспользоваться, все остальные компьютеры в вашей сети должны быть настроены как DHCP-клиенты. Если эта функция активирована, вы должны ввести хотя бы одно значение DNS на вкладке **DNS**. Если в вашей сети уже есть DHCP-сервер, активировать эту функцию нельзя.
- **Start IP address** (Начальный IP-адрес). Введите первое число диапазона IP-адресов, выделяемых в вашей сети DHCP-сервером. Это число должно быть между 1 и 254.

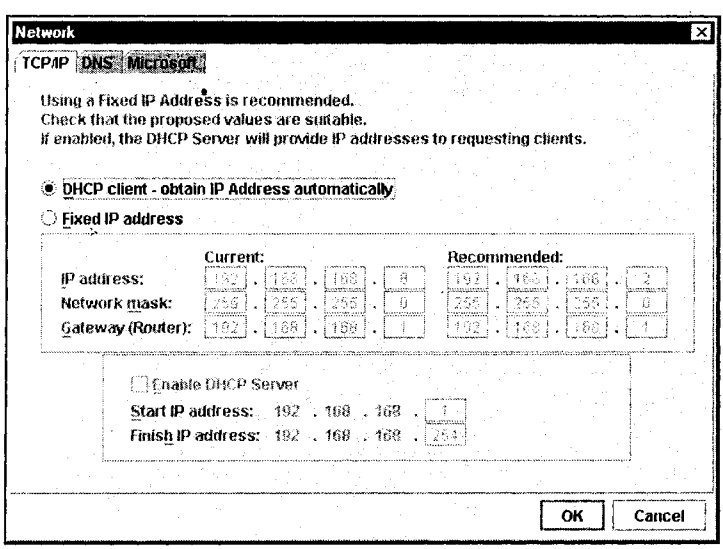


Рис. 18.15. Вкладка **TCP/IP** позволяет настраивать сервер компакт-дисков по отношению к другим сегментам сети и даже автоматически находить IP-адрес

- **Finish IP address** (Конечный IP-адрес). Введите последнее число диапазона IP-адресов, выделяемых в вашей сети DHCP-сервером. Установленный диапазон должен быть настолько широким, чтобы его хватило для всех возможных DHCP-клиентов.

Настройки DNS

Вкладка **DNS** позволяет ввести до трех IP-адресов DNS, чтобы сервер компакт-дисков мог найти в рамках сети DNS-сервер. Первая запись IP-адреса должна соответствовать первому DNS-серверу; второй и третий адреса факультативны. Если вы применяете сервер компакт-дисков как DHCP-сервер, эти IP-данные придется ввести (по крайней мере, для первого IP-адреса). Если же сервер компакт-дисков играет роль DHCP-клиента (соответственно, в сети есть другое устройство, выполняющее функцию DHCP-сервера), вы можете оставить поля для ввода IP-адресов незаполненными.

Настройки сетей Microsoft

Вкладка **Networking** применяется для ввода информации, необходимой для идентификации данного устройства в Microsoft-совместимой сети. Например, имя рабочей группы устройства должно соответствовать имени рабочей группы сети (хотя пользователи из других рабочих групп тоже смогут обращаться к серверу компакт-дисков). Запись кодовой страницы позволяет ввести географический регион, в котором будет работать ваш сервер. На этой вкладке можно подключить WINS-клиента и ввести IP-адрес WINS-сервера (если в вашей сети используется WINS).

Управление образами компакт-дисков

Конечной целью использования сервера компакт-дисков является создание образов CD и их сохранение на внутреннем жестком диске сервера; в результате компьютеры сети получают возможность коллективного использования образов CD, что представляет собой эффективную альтернативу дисководу с автоматической сменой компакт-дисков. Так можно создавать образы компакт-дисков, управлять ими и предоставлять возможность другим пользователям сети обращаться к ним. Для того чтобы справиться с этими задачами, вам понадобится утилита управления сервером компакт-дисков; кроме того, вы должны будете установить клиентское ПО на тех компьютерах, которые будут обращаться к данному серверу.

Отделения

Образы компакт-дисков можно формировать и хранить в каталогах на сервере компакт-дисков (иногда их называют кабинетами или отделениями). Впрочем, отделения нельзя выстраивать в иерархию, т. е. один кабинет не может находиться внутри другого. Например, чтобы создать новое отделение, необходимо запустить программу управления сервером. После этого последовательно выберите ее в меню **File**, **New**, **Cabinet** и введите имя нового отделения (рис. 18.16). Редактирование описания нового отделения производится путем нажатия на пиктограмму **Properties** и ввода нового описания. Вы можете также вырезать, копировать, вставлять и удалять отделения (или образы компакт-дисков), тем самым улучшая структуру данных; но вы не можете копировать образ компакт-диска с одного сервера на другой.

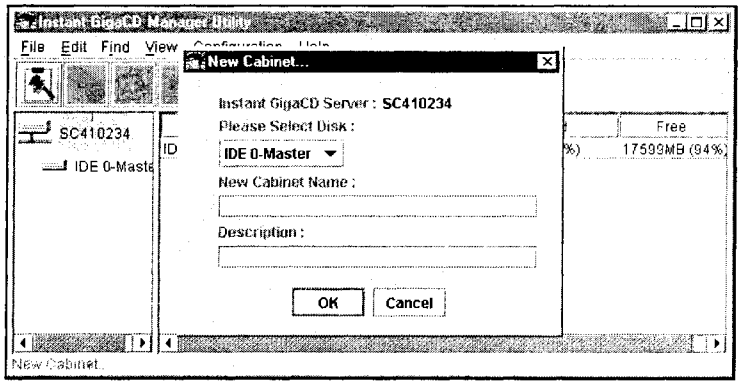


Рис. 18.16. Создание нового отделения для хранения файлов образа компакт-диска

Создание образа

Чтобы создать файл образа CD, поместите этот диск в дисковод. Если программа управления сервером еще не активна, запустите ее сейчас. Процесс формирования запускается по нажатию на пиктограмму или с помощью меню вида **File**, **New**, **CD**. Появится диалоговое окно нового образа компакт-диска (рис. 18.17), после чего вы должны ввести некоторые данные об этом образе.

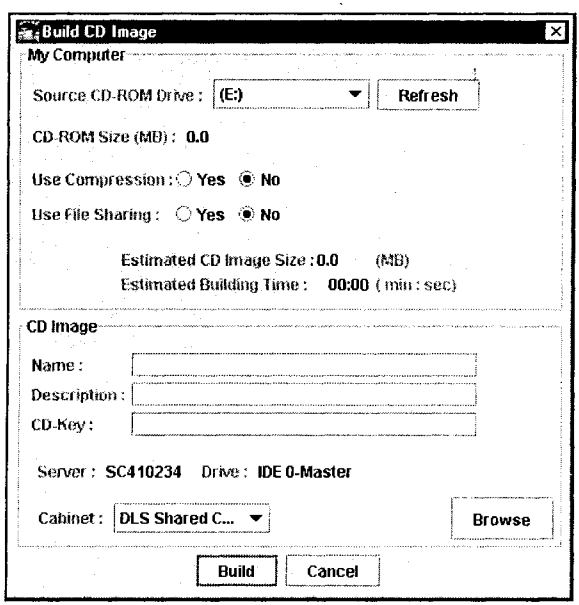


Рис. 18.17. Настройка файла образа компакт-диска с помощью диалогового окна **Build CD Image**

- **Use Compression** (Применение сжатия). Если этот флажок установлен, файл образа компакт-диска будет сохранен в сжатом виде и, следовательно, займет

меньше пространства на жестком диске. Впрочем, сжатие файла не допускает его коллективного использования.

- **Use File Sharing** (Совместное использование файла). Если этот флажок установлен, пользователи вашей сети получат возможность обращаться к образам компакт-дисков, хранящимся на сервере.
- **Name** (Имя). Здесь следует ввести имя образа конкретного CD.
- **Description** (Описание). Здесь нужно ввести описание содержимого образа данного компакт-диска.
- **CD-Key** (Код компакт-диска). Под кодом подразумевается серийный номер или другой идентификатор исходного компакт-диска; он требуется при обращении к образу компакт-диска посредством некоторых программ.
- **Cabinet** (Отделение). Выберите на сервере отделение, в котором будет храниться новый образ компакт-диска.

После завершения всех операций в упомянутом диалоговом окне, для создания образа компакт-диска необходимо нажать кнопку **Build**. Формирование образа CD на сервере компакт-дисков предполагает выполнение им некоторых операций по обработке данных, в результате чего доступ к этому серверу для других пользователей может быть замедлен. Созданием новых образов лучше заниматься в условиях незначительной загруженности сервера. Приостановить процесс формирования можно путем нажатия кнопки **Pause/Resume**, а для его окончательного прерывания следует нажать кнопку **Cancel**.

Применение образа

Для того чтобы все пользователи сети имели возможность обращаться к серверу компакт-дисков, вам придется установить специальное клиентское программное

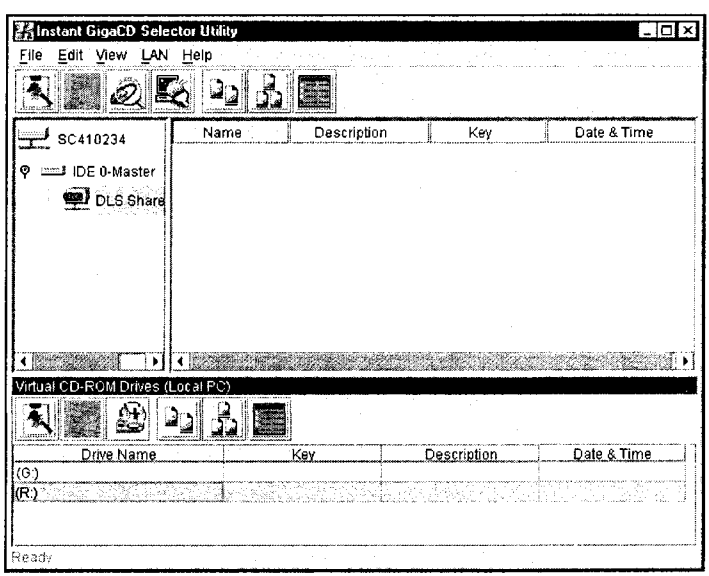


Рис. 18.18. Селекторная утилита сервера компакт-дисков позволяет обращаться к файлам образов CD

обеспечение на каждой рабочей станции. Если быть более точным, вам нужно будет установить на всех рабочих станциях драйвер сервера компакт-дисков, а также селекторную программу, которая обеспечивает возможность обращения к файлам образов CD. С помощью селекторной программы на каждой рабочей станции нужно определить местоположение сервера (рис. 18.18); после этого образы компакт-дисков становятся доступны для данного компьютера. Все происходит так, как будто в локальном приводе CD-ROM установлен настоящий компакт-диск.

Поиск неисправностей сервера компакт-дисков

Серверы компакт-дисков призваны обеспечивать легкость установки, хорошую производительность и долговременную надежность работы в сети (в основном, это обуславливается появлением возможности хранения множества файлов образов компакт-дисков и обращения к ним без использования громоздкого и неуклюжего дисковода с автоматической сменой компакт-дисков). Тем не менее это не означает, что у серверов компакт-дисков не бывает сбоев в работе. Как администратор или технический специалист, вы должны иметь представление о важных принципах сопровождения типичных серверов компакт-дисков, а также быть знакомым с наиболее распространенными неисправностями.

Диагностика дисков

Устройства типа Linksys GigaCD Server хранят файлы образов компакт-дисков на внутренних жестких дисках. Со временем на этих дисках могут появляться дефектные секторы и другие неисправности, способные повредить образы CD или вообще сделать обращение к ним невозможным. Чтобы обеспечить нормальную работу сервера компакт-дисков, технический специалист или администратор должен регулярно

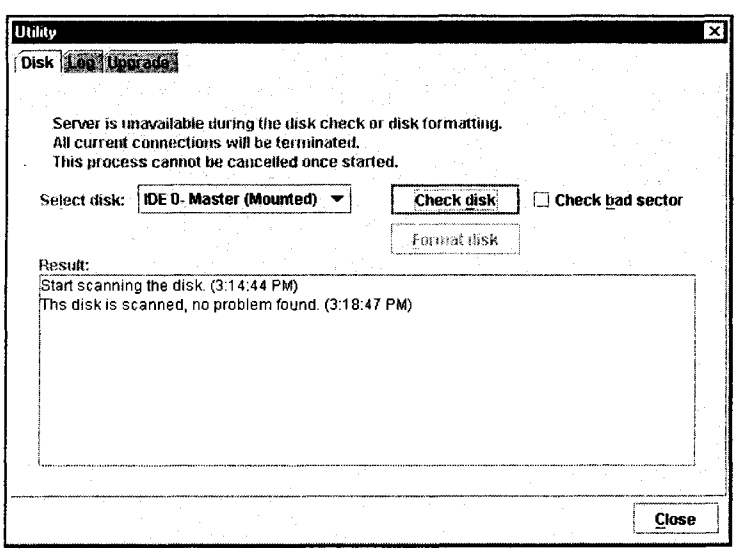


Рис. 18.19. Утилиты позволяют проверять диск(и) и сообщают о зафиксированных неисправностях

проверять состояние диска. Если на вашем сервере поддерживаются средства диагностики диска (рис. 18.19), вы можете контролировать диск, а при необходимости предпринимать корректирующие действия.

Журнал активности

Как правило, серверы компакт-дисков ведут журнал активности, который может оказаться полезным при выполнении задач, связанных с управлением и поиском неисправностей. Некоторые серверы записывают свои журналы активности во внешний текстовый файл; другие ведут внутренний журнал, обращение к которому может производиться через служебное меню устройства. Прежде чем пытаться устранять неисправность, связанную с доступом к серверу или с его производительностью, не забывайте проверить записи в этом журнале.

Обновление микропрограммного обеспечения

Если ваш сервер компакт-дисков содержит утилиту обновления микропрограммного обеспечения, то вы можете ей воспользоваться. В большинстве случаев перед этим необходимо загрузить с сайта производителя обновленный файл с микропрограммным обеспечением. Откройте утилиту обновления, введите полный путь к файлу обновления (например, c:\program files\Virtual CD-Rom Utility\manager\DC36799.rpm) и запустите процесс обновления. Имейте в виду, что в ходе процесса обновления сервер будет недоступен, и все соединения с ним будут разорваны (включая то, через которое обновление инициировалось). Процедура обновления может занимать до десяти минут. По завершении обновления сервер необходимо перезагрузить (если он не перезагрузится самостоятельно); затем, после повторного установления соединения с сетью клиенты вновь получат возможность обращаться к образам компакт-дисков.

Симптомы неисправностей

Большинство серверов компакт-дисков разрабатываются с расчетом на обеспечение хранения данных по модели Plug-and-Play, но при этом могут появиться сбои в работе. Большая их часть устраняется посредством визуальных проверок и изменений в конфигурации, но в этой части главы мы сосредоточимся на ряде характерных проблем, для решения которых требуются строго определенные корректирующие действия.

Симптом 18.14. Не удается подключиться к серверу компакт-дисков с целью его администрирования

В первую очередь необходимо проверить питание и соединения. Убедитесь в том, что сервер компакт-дисков подключен к источнику питания, и его контрольная лампа светится. При необходимости подключите устройство и подведите к нему питание. Если устройство уже включено, проверьте, сигнализирует ли светодиод подключения к сети. Если он не работает, проверьте кабельное соединение с сетью. Пользуйтесь только тем кабелем, который входил в комплект данного устройства. Подключите кабель к коннектору с маркировкой "LAN", находящемуся на задней панели сервера компакт-дисков. Подключите другой конец кабеля к подходящему сетевому коннектору (например, 10/100BaseT Ethernet) на концентраторе или ком-

мутаторе. Попытайтесь использовать другой порт на концентраторе или коммутаторе или попробуйте другой сетевой кабель. При работе с концентратором или коммутатором со связным портом старайтесь не использовать этот порт. Им можно пользоваться только в том случае, если переключатель **Uplink** установлен в нужное положение.

Другим источником неисправности могут быть IP-адреса. Убедитесь в том, что на рабочей станции, с которой производятся попытки доступа, применяется IP-адрес в пределах диапазона, совместимого с сервером компакт-дисков. Например, диапазон (192.168.0.3; 192.168.0.254) совместим с IP-адресом сервера компакт-дисков по умолчанию — 192.168.0.2. Если неисправность сохранится, попробуйте перезагрузить сервер компакт-дисков. Если и это не поможет, вероятно, устройство неисправно и требует замены.

Симптом 18.15. При обзоре сети с вашей рабочей станции не удается обнаружить сервер компакт-дисков

Обычно в таких случаях неисправность имеет отношение к TCP/IP на данной рабочей станции. В первую очередь убедитесь в том, что протокол TCP/IP на ней установлен или установите его. Проверьте, действительно ли протокол TCP/IP привязан к вашему сетевому адаптеру. Выберите сетевой адаптер, нажмите **Properties** (Свойства) и откройте вкладку **Bindings** (Привязки). Если флажок **TCP/IP** не установлен, установите его сейчас. TCP/IP и сетевой адаптер должны быть привязаны к службе **Client for Microsoft Networks** (Клиент для сетей Microsoft). Выделите запись **TCP/IP** сетевого адаптера, нажмите **Properties** (Свойства) и откройте вкладку **Bindings** (Привязки). Если флажок **Client for Microsoft Networks** (Клиент для сетей Microsoft) не установлен, установите его сейчас.

Возможно, неисправность вызвана IP-адресацией. Если в сети нет маршрутизатора, убедитесь в том, что IP-адрес вашей рабочей станции совместим с IP-адресом сервера компакт-дисков. Он должен находиться в том же самом адресном диапазоне (например, от 192.168.0.3 до 192.168.0.254) и использовать ту же маску подсети (например, 255.255.255.0). Если в сети есть маршрутизатор, проверьте правильность настройки IP-адреса шлюза.

Симптом 18.16. Не удается изменить имя дисковода сервера компакт-дисков в Windows 2000

Windows 2000 поддерживает назначение лишь одного имени дисковода компакт-дисков в процессе инсталляции и изменить это имя нельзя (в любом случае будет применяться одно имя дисковода). После первоначальной инсталляции и перезагрузки у вас появляется возможность выбрать функцию настройки (Setup) сервера компакт-дисков и создать новые виртуальные компакт-диски, расставив их имена в произвольном порядке. После этого необходимо произвести перезагрузку. После перезапуска Windows 2000 выведет приглашение на очередную перезагрузку. Делать это необязательно.

Симптом 18.17. Появляется сообщение об ошибке, в соответствии с которым на диске недостаточно места

Файлы образов компакт-дисков хранятся на жестком диске сервера. Эта ошибка, как правило, означает, что свободное пространство, на котором можно сохранять

файлы образов, составляет менее 10% от общего объема жесткого диска. С помощью программы управления сервером компакт-дисков удалите все ненужные файлы (например, старые стандартные иллюстрации или архивные изображения). Если это предупреждение будет появляться и дальше, попробуйте установить на сервер компакт-дисков второй дисковод, воспользоваться дисками большей емкости или добавить в сеть еще один сервер компакт-дисков.

Симптом 18.18. Предупреждения от сервера компакт-дисков не приходят на ваш почтовый ящик

Вы настроили сервер компакт-дисков на отправку предупреждений по электронной почте, и, несмотря на то, что эти предупреждения генерируются, вы их не получаете. Практически во всех случаях происхождение этой неисправности можно отнести к ошибкам в конфигурации сервера компакт-дисков. В первую очередь проверьте, действительно ли вы активировали почтовые предупреждения и ввели правильный электронный адрес для их получения. Убедитесь в том, что вы выбрали получение всех предупреждений и сообщений.

Основы SAN (сеть хранения данных)

В большинстве сетей малого и среднего масштаба реализуются принципы хранения на базе серверов. Это значит, что информация хранится на серверах, локальных машинах или на устройствах хранения (подобных Maxtor NAS 3000 или Linksys GigaCD Server, рассмотренных ранее в этой главе). Этот подход несложен для понимания и легок в реализации, но тот объем данных, который проходит через сетевую среду (по кабелю) может создавать узкие места в производительности систем хранения, причем эта проблема становится тем серьезнее, чем больше разрастаются сети. В некоторых сетях эффективность хранения повышается за счет применения методик выравнивания нагрузки и агрегирования. Например, вместо одного порта сетевого адаптера на сервере их может быть несколько; в таком случае получается, что взаимодействие с сервером (и его пространством хранения) может производиться по нескольким каналам. Если одно или несколько соединений прервутся, сервер все равно останется досягаемым. Этот принцип развивается в методике кластеризации серверов, которая предполагает объединение нескольких серверов и совместное предоставление ими услуг (например, связанных с хранением файлов).

Тем не менее крупные сети сталкиваются с тремя трудноразрешимыми проблемами. Они связаны с базами данных с коллективным доступом со стороны приложений, загруженными приложениями и необходимостью постоянной доступности. База данных с коллективным доступом со стороны приложений (application-shared database) выполняет функции поддержки различных типов программ посредством общей для всех них информации. Когда разделяемая база данных используется приложениями, размещенными на нескольких серверах, она сама должна быть распределена, а это, в свою очередь, может привести к появлению сбоев ее синхронизации.

К трудностям аналогичного характера приводит и совместное использование загруженных приложений. На большинстве предприятий есть несколько основных приложений, к которым должна обращаться большая часть пользователей. Зачастую активность этих критических приложений слишком высока, что приводит к чрез-

мерной перегрузке отдельного сервера; в то же время распределение такого приложения по нескольким серверам приводит к появлению базы данных с коллективным доступом. Другой важный фактор, который нужно принять во внимание, это наличие постоянной доступности. Возможно, отдельный сервер и сможет выдержать полный объем нагрузки по хранению данных, но он все равно не может защититься от неисправностей аппаратного/программного обеспечения. Если для резервирования первичного сервера применяется параллельный сервер, между ними должна производиться синхронизация баз данных. Здесь мы опять возвращаемся к неисправностям, связанным с базами данных с коллективным доступом.

Введение в SAN

Разработчики сетей нашли решение описанной проблемы в виде SAN. SAN — это отдельная сеть для серверов и устройств хранения, существующая параллельно с локальной сетью, и дублированные *серверы хранения*, подключенные через выделенные высокоскоростные коммутаторы (рис. 18.20). Данные могут перемещаться между устройствами SAN без обработки со стороны хост-сервера. Архитектура SAN поддерживает универсальный механизм "любой к любому", в соответствии с которым многочисленные серверы могут обращаться к разнообразным дисковым ресурсам — в результате получается своеобразная технология совместного использования диска, реализуемая без участия сервера. На стороне SAN каждый сервер подключается к коммутационной структуре (как правило, по волоконному каналу Fibre Channel или через Gigabit Ethernet), которая, в свою очередь, представляет доступ к отдельным массивам хранения, настраиваемым как узлы в рамках SAN.

В типичную SAN обычно входят серверы, подключенные к ней через сетевой адаптер SAN, который эмулирует стандартный дисковый интерфейс (типа SCSI) сервера. Кроме того, SAN содержит устройства хранения (ленты и массивы дисков), мосты и мультиплексоры. Все они подключаются к коммутаторам Fibre Channel (или высокоскоростного соединения Ethernet). Как и в случае с локальными или глобальными сетями, коммутаторы завершают магистраль для всех подключенных устройств, причем один или несколько коммутаторов действуют как коммутирующая структура канала Fibre Channel. Коммутирующая структура SAN допускает подключение тысяч узлов, обеспечивающих обширные пространства хранения.

SAN на базе волоконного канала может содержать в себе шлейф волоконно-оптического канала с арбитражной логикой (Fibre Channel Arbitrated Loop, FC-AL) — вид сети с разделяемой пропускной способностью. Архитектура FC-AL поддерживает до 126 устройств на каждом шлейфе (подключенных напрямую к коммутаторам волоконного канала или к концентраторам, которые, в свою очередь, подсоединены к коммутаторам). Более того, SAN на базе Fibre Channel способствуют разгрузке серверов, т. к. на них возлагалась дополнительная нагрузка по передаче данных устройствам хранения и в локальную сеть. Теперь же серверы могут передавать обязанности по передаче данных архитектуре SAN и быстро возвращаться к своим первоначальным функциям обработки. В условиях SAN сервер лишь следит за процессом хранения, но не осуществляет прямого управления им.

Примечание

Планируя использование Ethernet в качестве архитектуры соединений SAN, не следует разделять устройства или магистрали Ethernet между SAN и локальной/гло-

бальной сетями. Уровни сетевого трафика, связанные с хранением, очень высоки. Они способны в значительной степени снизить производительность сети для других приложений. Состязания между трафиком SAN и LAN/WAN создают серьезные неисправности, связанные с согласованием по времени, и практически не поддаются восстановлению и устранению.

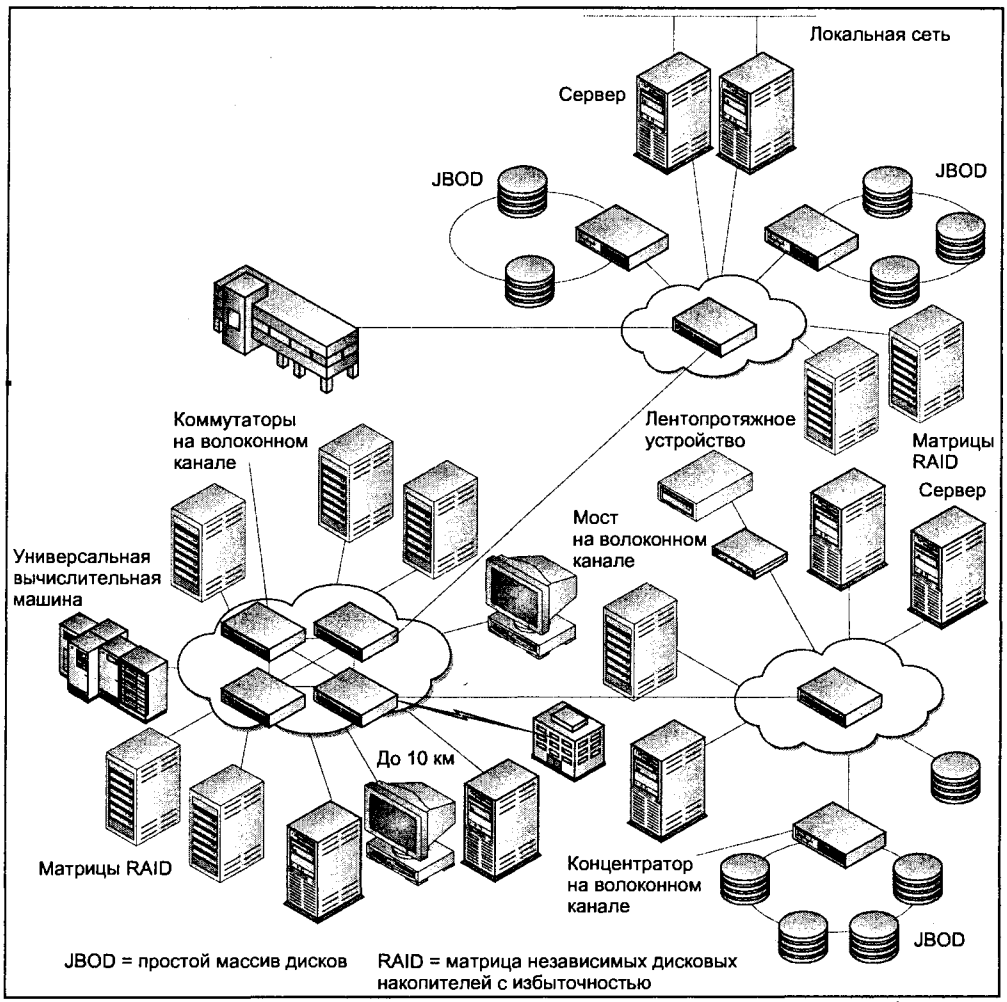


Рис. 18.20. Упрощенный пример SAN в действии (публикуется с разрешения NetworkMagazine.com)

Применение оптоволоконных каналов

SAN на базе Fibre Channel реализуется в виде сетей с разделяемой пропускной способностью или с коммутируемым доступом (иногда применяется сочетание этих двух типов). В SAN с разделяемой пропускной способностью все устройства поль-

зуются одним гигабитовым шлейфом. К сожалению, чем больше добавляется устройств, тем меньше пропускная способность. Этот вариант приемлем для очень небольших сред, однако магистраль на основе коммутаторов Fibre Channel повышает суммарную пропускную способность SAN. При организации коммутационной структуры Fibre Channel может быть задействован один или несколько коммутаторов. Обращение к службам коммутационной системы возможно лишь в том случае, если сетевой адаптер на каждом устройстве хранения может подключаться как к структуре, так и к операционной системе и приложениям. Таким образом, сетевой адаптер становится частью сети хранения после входа в коммутационную структуру. Эта функция называется регистрацией в структуре — при формировании SAN важно пользоваться такими сетевыми адаптерами, которые ее поддерживают.

Другим важным принципом для устройств, подключенных к SAN, является способность обнаруживать все устройства в рамках коммутационной системы. Стандарт Fibre Channel определяет механизм обнаружения (который называется службой SNS — Simple Name Service, простая служба имен), поддерживающий сбор данных об адресе, типе и символическом имени каждого устройства в пределах коммутационной системы. Информация SNS хранится в коммутаторах волоконного канала — именно у них ее запрашивают сетевые адаптеры и контроллеры хранения. Проектировщики сетей, желающие организовать волоконный канал, должны выбирать сетевые адаптеры на основе стандарта Fibre Channel и контроллеры хранения, поддерживающие SNS.

Что касается восстановления после ошибок и локализации неисправностей, то в Fibre Channel поддерживается факультативная функция под названием оповещения об изменении зарегистрированного состояния (RSCN, Registered State Change Notification). При изменениях в конфигурации она отсылает устройствам обновления. Функция RSCN часто применяется в условиях, когда матрицы RAID, диски вне RAID, лентопротяжные устройства и хосты подключены напрямую к коммутационной структуре, а не к шлейфам с разделяемой пропускной способностью (поскольку неисправные узлы не оказывают влияния на все прочие устройства, подключенные к коммутационной структуре). Коммутируемые сети восстанавливаются после ошибок намного быстрее, чем сети с разделяемой пропускной способностью. Так происходит за счет того, что неисправные устройства или каналы поддаются локализации.

Управление SAN

В условиях SAN сетевые администраторы должны иметь возможность пользоваться все теми же инструментальными средствами и системами, которые применяются в локальных и глобальных сетях. Это означает, что вам следует искать такие устройства SAN, которыми можно управлять средствами SNMP или через Web-интерфейс. Эти устройства должны поддерживать Telnet (для удаленной диагностики или обслуживания). Все эти средства управления должны предоставлять подробную информацию о состоянии устройства, уровнях производительности, изменениях в конфигурации и топологии, а также статистические данные. Среди основной информации о состоянии и производительности должны предусматриваться подробные данные о пропускной способности и задержках. В некоторых устройствах SAN даже могут присутствовать инструментальные средства настройки и оптимизации.

В сетях FC-AL концентратор FC предоставляет административную информацию обо всех устройствах в рамках шлейфа, но при этом он не может предоставлять отчеты об устройствах, которые находятся вне этого шлейфа. Естественно, когда шлейфы подключены к базе коммутации, средства удаленного управления и диагностики доступны для всех устройств.

Дополнительные ресурсы

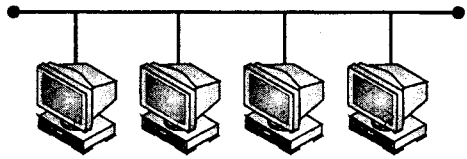
Chi Storage Solutions: **www.chicorporation.com**.

Fibre Channel Association: **www.fibrechannel.com**.

Linksys: **www.linksys.com**.

Maxtor: **www.maxtor.com**.

Ассоциация производителей устройств сетевого хранения (Storage Networking Industry Association, SNIA): **www.snia.org**.



ГЛАВА 19

Защита сетей от вирусов

Большинство современных программных продуктов полезны по своему назначению, но есть и другие программы, служащие более низким целям. Они называются *компьютерными вирусами*. Подобные злонамеренные программы разрабатываются с расчетом на внедрение в сеть таким образом, чтобы пользователь об этом не узнал. Часто они спрятаны в нормальных программах или в электронной почте. Вирусы выполняют свои функции, не спрашивая у пользователя разрешения, они не предупреждают о потенциальной опасности, грозящей системе, и не генерируют сообщения об ошибках. Компьютерный вирус представляет собой фрагмент исполняемого кода, запускаемого втайне и способного к клонированию себя в других программах.

С технической точки зрения, в представленном определении нет ничего, что отражало бы разрушительный характер вируса. Это лишь хитрость, придуманная людьми, занимающимися написанием вирусов. Но легальному программному обеспечению нет нужды запускаться незаметно, прятаться в других программах или заниматься саморазмножением без оповещения об этом пользователей и без получения их разрешения. Таким образом, сам характер компьютерного вируса делает его идеальным средством распространения хаоса. В современном компьютерном мире, когда все локальные сети нуждаются в доступе к сети Интернет, компьютерные вирусы обладают наибольшим проникающим потенциалом. Эта глава посвящена сущности и деятельности компьютерных вирусов, способам их распространения и проявления. Здесь вы также сможете ознакомиться с некоторыми процедурами, направленными на защиту пользователей вашей сети от воздействия вирусов.

Основные сведения о вирусах

Термин *вирус* мы применяем для описания практически любых типов программного обеспечения разрушительного характера. Однако это определение не совсем точное. На самом деле, вирус — это лишь один из многих типов разрушительных программ. Существует множество известных видов злонамеренного программного обеспечения, большая часть которых считается не менее опасными, чем вирусы. Для каждого из этих видов характерен особый режим работы. Как технический специалист, вы должны иметь представление о том, как именно действуют типичные виды вирусов.

Примечание

Сегодня для обозначения разрушительного программного обеспечения часто применяется термин *вредоносные программы* (malware — плохое средство).

Программные дефекты

Программный дефект — это ошибка (Bug -баг), допущенная при кодировании или формировании логики программы, результатом которой является неправильное или неожиданное ее поведение. Дефекты редко допускаются намеренно, причем подавляющее большинство серьезных дефектов, способных вывести систему из строя, обнаруживаются разработчиками на этапах альфа- и бета-тестирования. Чтобы серьезные дефекты смогли проникнуть в готовый продукт (имеются в виду те дефекты, которые могут вызвать серьезные ошибки памяти или привести к потере данных на жестком диске), разработчик должен практически (или совсем) не тестировать продукт на различных компьютерных платформах. Серьезные дефекты, естественно, не злонамеренны, но они предполагают недостаток внимания к продукту со стороны его разработчика. Есть два признака, по которым можно определить наличие программных дефектов: во-первых, в качестве источника сбоя выступает только одна программа (обычно та, которую вы только что установили и запустили), а во-вторых, ее не удается обнаружить с помощью антивирусных средств (они сообщат о том, что данное приложение ничем не заражено). Программы, содержащие серьезные или устойчивые дефекты, часто называют дефектными (bugware). К счастью, дефекты обычно устраняются с помощью программных заплат или обновлений, создаваемых производителем.

Троянские кони

Обычно *троянский конь* считается предшественником современных вредоносных программ. Именно так называется разрушительная компьютерная программа, скрытая под маской полезного и вполне заурядного продукта типа текстового процессора или графической программы. Тщательно проработанные пользовательские оболочки и на вид нормальные операции заставляют пользователя поверить в то, что такая программа совершенно безобидна. Это убеждение сохраняется вплоть до запуска вредоносного кода, и тогда программа показывает свое настоящее лицо. Тактика троянского коня является наиболее популярным средством внедрения вирусов путем распространения на первый взгляд безвредных программ, которые на самом деле содержат вредоносный код. К счастью, такой код можно обнаружить с помощью проверки нового программного обеспечения перед его первым запуском. Чтобы не допустить распространения троянских коней, нужно критически и с опаской относиться к нежелательному или ненужному программному обеспечению, приходящему по электронной почте в виде вложений. Следует остерегаться программ, свойства которых слишком хороши, чтобы быть правдой (в качестве примера можно привести резидентную программу, которая, по заявлению отправителя, способна повысить производительность Windows в 100 раз, обеспечить графику SVGA при видеоадаптере стандарта EGA, разрешить бесплатное использование AOL и т. д.).

Программные бомбы

Сущность *программной бомбы* (Bomb — бомба)[1] полностью соответствует ее названию. Вредоносный код программной бомбы исполняется и начинает вредить системе почти сразу после запуска инфицированной программы. Программные бомбы, как правило, не содержат никаких лишних функций. В отличие от вируса, они пытаются спрятаться и почти не стремятся к размножению. Следовательно, разработка программной бомбы производится быстро и не представляет сложности. В некотором отношении такие бомбы примитивны, и поэтому их довольно просто обнаружить с помощью антивирусных средств.

Логические бомбы

Если программная бомба создается с расчетом на немедленное и беспорядочное разрушение, *логическая бомба*, напротив, настраивается на "взрыв" лишь при определенном логическом условии. Например, логическая бомба может сработать (стереть файлы, неверно рассчитать очередные платежные ведомости, переформатировать диск и т. д.) в том случае, если обнаружит, что ее автор уволен или временно освобожден от работы, а его счета не пополняются более четырех недель. Пуском для логической бомбы может послужить практически любое системное условие. Впрочем, логическую бомбу тоже довольно просто разоблачить методами антивирусной защиты.

Бомбы замедленного действия

Вместо незамедлительного запуска или запуска при определенных условиях состояния системы, *бомба замедленного действия* основывается на временных и повторяющихся условиях. Бомбу замедленного действия можно настроить на "взрыв" по истечении определенного количества запусков программы, по достижении некоей даты (например, 1 апреля или пятницы 13-го) или времени (например, запустить ее в полночь). Бомбы замедленного действия часто используются как средства заявления об определенной дате и времени. Такие бомбы довольно легко поддаются обнаружению антивирусными средствами. Узнать о новых датах активации можно по адресу **www.mcafee.com/anti-virus/**. Преимущество календаря вирусов заключается в том, что у вас появляется возможность оперативно обратиться к возможным повреждениям системы вирусами, а затем найти более подробную информацию в библиотеке вирусов типа **vil.mcafee.com**.

Репликаторы

Назначение *репликатора* (которого иногда называют кроликом) заключается в том, чтобы истощить ресурсы системы. Он выполняет эту задачу путем создания собственных копий. Каждая подобная точная копия запускается родительским элементом, который ее создал. Вскоре после этого огромное количество копий репликатора на диске и в памяти начинают потреблять столько ресурсов, что система вынуждена

---

[1] Здесь и далее "бомба" — это компьютерный сленг, обозначающий вредоносный программный код. — *Ред.*

прекратить работу. Таким образом, система остается непригодной вплоть до удаления копий и устранения воспроизводящего их вируса. Такое поведение приводит к особенно впечатляющим результатам, когда злоумышленник ставит целью организовать сбой многопользовательских систем или сетей. Так как вредоносный код самовоспроизводится, его довольно просто обнаружить средствами антивирусной защиты.

Черви

Червь — это один из самых первых типов вредоносных программ, применявшихся для организации атак на компьютерные сети. Червь переходит из одного компьютера в другой, причем, как правило, не наносит им никакого ощутимого вреда. Обычно черви самовоспроизводятся, чтобы продолжить путь по сети, и пытаются устранить все следы своего присутствия. Червь — это еще один вид сетевого присутствия, применяемый для поиска и выборочного изменения или удаления ограниченного количества файлов или программ. Например, червь может проникнуть в сеть, чтобы изменить или удалить сетевые пароли. Так как черви могут приспосабливаться для выполнения определенных задач, их обнаружение часто связано с некоторыми трудностями, в особенности если данный червь неизвестен.

Вирусы

Наиболее очевидным и динамическим видом злонамеренного программного обеспечения является *вирус*. Вирус модифицирует другие программы, помещая в них исполняемый вредоносный код. В некоторых случаях такой код мутирует и корректируется по мере своего копирования. Профессионально спроектированные вирусы не вносят никаких изменений в дату зараженного файла, его временные метки, размер, свойства и контрольную сумму. Следовательно, вирусы очень сложно обнаружить, но еще труднее устранить. Эта задача оказывается тем сложнее, чем более мощными и изощренными становятся сами вирусы. В современных операционных системах с большим количеством служебных данных, типа пользовательских систем Windows 9x/ME/XP и сетевых систем Windows NT/2000, вирусы обычно могут прятаться и довольно быстро воспроизводиться в любом из многочисленных файлов с расширениями DLL, VXD и других модулях, активированных в нормальном режиме. Учитывая их склонность к маскировке и воспроизведению, вирусы стремятся укрепиться в системе, чтобы переходить с жестких дисков на гибкие, распространяться по сетевым соединениям, попутно разрушая данные, инициировать системные ошибки и всеми способами снижать производительность системы. В конечном итоге большинство вирусов самоуничтожаются, но при этом удаляют и другие файлы, расположенные на жестком диске.

Типы вирусов

Как вы могли предположить, не все вредоносные коды одинаковы. Вирусы не менее разнообразны, чем легальное прикладное программное обеспечение, причем каждая методика создания вируса предоставляет его разработчику ряд преимуществ и недостатков. Некоторые способы создания вирусов предпочтительны потому, что их продукты сложнее обнаружить и устранить, но при этом они требуют дополнительных ресурсов при разработке. Другие вирусы проще создавать, но по параметрам маски-

ровки и уровня сложности они уступают более мощным вариантам. Третьи вирусы имеют более серьезные шансы инфицировать множество систем.

Загрузочные вирусы

На старых компьютерах операционные системы загружались с гибких дисков. Создатели вирусов быстро поняли, что могут подставлять собственные программы вместо исполняемого кода, присутствующего в загрузочном секторе каждого DOS-форматированного гибкого диска вне зависимости от того, есть ли в нем системные файлы. Таким образом, ни о чем не подозревающие пользователи загружали такой вирус каждый раз при запуске компьютера с инфицированного диска. Находясь в памяти, такой вирус получает возможность воспроизводить себя в загрузочных секторах других гибких и жестких дисков. Например, те пользователи, которые непреднамеренно загружали с зараженного гибкого диска вирус Brain, читали рекламу компьютерной службы, расположенной в Пакистане. С этим объявлением в Brain было связано еще одно нововведение, ставшее характерной чертой современных вирусов — полезная нагрузка. *Полезная нагрузка* — это оригинальное или вредоносное поведение, которое (после запуска) может приводить к различным последствиям, от появления раздражающих сообщений до уничтожения данных. Именно это свойство вируса привлекает к себе наибольшее внимание. Сегодня многие разработчики вирусов создают свои творения исключительно затем, чтобы распространить свои полезные нагрузки на максимальное количество компьютеров.

Некоторое время усложненные потомки этого первого загрузочного вируса представляли наиболее серьезную угрозу для пользователей компьютеров. Варианты загрузочных вирусов инфицируют главную загрузочную запись (Master Boot Record, MBR), в которой хранится информация о разделах. Практически каждый этап процесса загрузки (от считывания MBR до загрузки операционной системы) подвержен вирусным диверсиям. Некоторые наиболее мощные и разрушительные вирусы до сих пор способны заражать загрузочный сектор или MBR вашего компьютера. Активация загрузочного вируса в процессе загрузки дает ему возможность сделать свое черное дело еще до того, как сможет заработать антивирусная программа. Некоторые антивирусные программы учитывают эту возможность и поддерживают создание специального "аварийного диска", который, в крайнем случае, можно использовать для загрузки компьютера и устранения инфекций.

Файловые вирусы

Примерно в то же самое время, когда авторы Brain обнаружили слабые места в загрузочном секторе DOS, другие разработчики нашли способ применения уже установленного программного обеспечения в целях воспроизведения их творений. Один из первых файловых вирусов обнаружился в компьютерах университета Lehigh (Пенсильвания). Этот вирус инфицировал часть интерпретатора команд DOS (COMMAND.COM) и с его помощью загружался в память. Оказавшись в ней, он распространялся на другие, незараженные файлы COMMAND.COM при каждом вводе пользователем любой стандартной команды DOS, предполагавшей обращение к диску. Ранние версии этого вируса ограничивали его распространение гибкими дисками, на которых содержалась операционная система.

Довольно быстро вирусы преодолели это ограничение посредством искусного программирования. Например, разработчики могли сделать так, чтобы их вирус вставлял свой код в начало исполняемого файла. При запуске программы код вируса ис-

полнялся немедленно, а затем возвращал управление легальной программе (которая работала так, как будто ничего необычного не произошло). После своей активации вирус перехватывал запросы легального программного обеспечения к операционной системе и подставлял свои собственные ответы. Особенно изощренные вирусы могут даже препятствовать попыткам удаления их из памяти, перехватывая сочетание клавиш <Ctrl>+<Alt>+<Del>, выполняющее горячую перезагрузку, и выполняя фальшивую перезагрузку. В некоторых случаях единственным внешним признаком неисправности системы (до активации какой-нибудь полезной нагрузки) могло быть незначительное изменение размера файла инфицированной легальной программы.

Вирусы-невидимки, мутирующие, зашифрованные и полиморфные вирусы

Какими бы незаметными ни казались эти вирусы, изменения размера файла и другие малозначительные свидетельства вирусных инфекций обычно предоставляют большинству антивирусных программ данные, достаточные для успешного обнаружения и удаления вредоносного кода. Одна из основных задач, стоящих перед создателем вируса, заключается в том, как найти способы скрыть свою работу. В ранних вариантах вирусов применялась смесь новаторских средств программирования с очевидными хитростями. Например, вирус Brain перенаправлял запросы на просмотр загрузочного сектора с реального местоположения его зараженного варианта в новое место размещения загрузочных файлов, которые вирус предусмотрительно переместил. Эта способность к маскировке позволила ему и другим вирусам скрываться от традиционных методик их обнаружения.

Поскольку вирусы не должны повторно заражать одни и те же хосты (в результате таких действий инфицированный файл разросся бы до размеров, при которых его можно было бы с легкостью обнаружить, или был бы вынужден потреблять такой объем системных ресурсов, который сразу указал бы на виновника происходящего), авторы вирусов также должны были указать вирусам на определенные файлы, видоизменять которые нельзя. Они справились с этой задачей, заставив вирус ставить кодовые подписи, которые маркировали зараженные файлы программным эквивалентом объявления "не беспокоить". Это позволяло вирусу отсрочить момент своего обнаружения, но, с другой стороны, антивирусные программы получали возможность найти вирус по этим подписям.

В ответ авторы вирусов нашли способ маскировки кодовых подписей. Некоторые вирусы мутировали или ставили разные кодовые подписи при каждом новом случае заражения. Другие зашифровывали большую часть кодовой подписи или самого вируса, оставляя лишь несколько байт в качестве ключа для дешифровки. Наиболее сложные современные вирусы поддерживают применение огромного количества новых сочетаний маскировки, мутации и шифрования, обнаружить которые почти невозможно. Задача выявления таких полиморфных вирусов заставляет разработчиков программного обеспечения проектировать сложные, досконально продуманные антивирусные программы.

Макровирусы

Примерно к 1995 г. вирусная война вошла в пассивную стадию. Новые вирусы появлялись постоянно (к их созданию отчасти побуждала доступность готовых вирусных комплектов, которые позволяли даже людям, не связанным с программированием, создать вирус за минимальный срок). В то же время большинство существовавших на тот момент антивирусных программ можно было без труда обновить

с целью обнаружения и устранения новых вариантов вирусов, которые, в основном, представляли собой незначительные модификации хорошо известных шаблонов.

Но 1995 год ознаменовался появлением концептуально нового вируса, благодаря которому направление развития вирусов неожиданного переменилось. До появления концептуальных вирусов большинство специалистов, их исследовавших, считали, что файлы данных (текст, электронные таблицы или чертежные документы, создававшиеся пользовательским программным обеспечением) защищены от инфицирования. В конце концов, они полагали, что вирусы — это программы и что они должны запускаться таким же образом, как любое другое исполняемое программное обеспечение. С другой стороны, файлы данных — это всего лишь сохраненная информация, которая вводилась при работе с программой.

Это разграничение потеряло всякие основания, когда компания Microsoft начала встраивать возможности написания макросов в Word и Excel. С помощью упрощенной версии языка Visual Basic пользователи получили возможность создавать шаблоны документов, которые выполняли автоматическое форматирование и добавление других функций в документы, созданные с помощью Word и Excel. Авторы вирусов ухватились за представившуюся возможность и стали маскировать и распространять вирусы в документах, которые создавались самим пользователем. Нарастающая популярность сети Интернет и почтовых клиентов, позволявших прикреплять файлы к сообщениям электронной почты, обеспечивала быстрое и очень широкое распространение макровирусов. К концу 1990-х гг. макровирусы представляли собой самую серьезную вирусную угрозу.

Java и ActiveX

Программы на основе Java и ActiveX очень многообразны. Некоторые из них представляют собой специализированные миниатюрные приложения (апплеты), написанные на Java — сравнительно новом языке программирования, первоначально разработанном в компании Sun Microsystems. Другие программы проектируются с помощью ActiveX — технологии от Microsoft, позволяющей выполнять примерно аналогичные задачи.

Как в Java, так и в ActiveX широко применяются готовые программные модули (объекты), которые программисты могут составлять самостоятельно или заимствовать из существующих источников и приспосабливать к сменным модулям, апплетам, драйверам устройств и другим программным средствам, повышающим эффективность сети Интернет. Объекты Java называются *классами*, а объекты ActiveX — *элементами управления*. Основное различие между ними заключается в том, как они работают на хосте. Java-апплеты запускаются в виртуальной Java-машине, предназначенной исключительно для интерпретирования программного кода Java и приведения его в действие на хосте; в то же время элементы управления ActiveX работают как собственные программы Windows, компонуя данные и передавая их между действующими программами.

Подавляющее большинство этих объектов являются полезными (и даже необходимыми) компонентами любого интерактивного Web-сайта. Однако, несмотря на все усилия, приложенные разработчиками из Sun и Microsoft для встраивания в упомянутые объекты механизмов защиты, некоторые программисты способны пользоваться средствами Java и ActiveX для размещения на Web-сайтах вредоносных объектов, которые остаются незамеченными до тех пор, пока пользователь, действуя совершенно непреднамеренно, не предоставит им доступ к уязвимой компьютерной сис-

теме. В отличие от вирусов, опасные объекты Java и ActiveX обычно не рассматривают в качестве первоочередной цели воспроизводство. Интернет предоставляет им много возможностей для распространения по конечным компьютерным системам, в которых их небольшой размер и на первый взгляд безобидный характер позволяет избежать обнаружения. На самом деле, если вы специально не настроите Web-браузер на их блокировку, объекты Java и ActiveX будут автоматически загружаться в вашу систему при обращении к любому Web-сайту, на котором они используются.

Опасные объекты нацелены на доставку в пользовательские системы своего эквивалента полезной нагрузки вирусов. Например, программисты могут составить объекты, которые будут считывать данные с вашего жесткого диска и отправлять их обратно на посещенный вами Web-сайт. Эти объекты способны похитить вашу почтовую учетную запись, чтобы затем отправлять оскорбительные сообщения от вашего имени или наблюдать за данными, которые передаются от вашего компьютера на другие компьютеры.

Полезные антивирусные компоненты

На сегодняшний день антивирусные программы вышли далеко за рамки простых утилит с управлением из командной строки. Современное антивирусное программное обеспечение (особенно сетевое) представляет собой сочетание мощных взаимосвязанных инструментальных средств, каждое из которых выполняет в системе определенную функцию. В этой части главы рассматриваются компоненты современных антивирусных программных пакетов типа Norton AntiVirus Corporate Edition.

Примечание

Приведенные здесь данные являются лишь примером. Возможно, в вашем антивирусном пакете поддерживается большее или меньшее количество компонентов, но базовый комплект функций, скорее всего, аналогичен рассматриваемому

- Symantec System Center (консольный апплет и система управления предупреждениями) применяется для централизованного управления продуктами и функциями предупреждения Symantec.
- Интегрируемая программа управления (Snap-in) для Norton AntiVirus Corporate Edition, расширяющая консоль Symantec System Center и таким образом предоставляющая возможность управлять Norton AntiVirus Corporate Edition на серверах и клиентских машинах.
- Norton AntiVirus Corporate Edition (включает поддержку серверов Windows NT/2000 и NetWare, клиентов Windows NT/2000, Windows 9x/ME/XP и Windows 3.x/DOS).
- LiveUpdate Administration Utility позволяет загружать обновления на внутрисетевой FTP-сервер или на другой внутренний сервер. Впоследствии серверы и клиенты получают обновления именно с этого сервера.
- Central Quarantine — средство централизованного управления инфицированными файлами, обнаруженными на серверах и клиентских машинах.
- Norton AntiVirus Corporate Edition включает интегрируемое приложение Microsoft Management Console. Применяется для управления Norton AntiVirus Corporate Edition с консоли Symantec System Center.

- Инструмент Importer для импортирования компьютеров, расположенных вне среды WINS.
- Roaming Client Support можно использовать для проверки прикрепления клиентов Norton AntiVirus Corporate Edition (включая мобильных клиентов) к лучшему серверу (по параметрам скорости и близости).
- ACL Fix Tool — инструмент, ограничивающий на платформе Windows NT права записи в реестр для всех, кроме администратора.

Поиск вирусов

Естественно, даже самое лучшее антивирусное программное обеспечение не принесет никакой пользы, если его не настроить на поиск вирусов и активную защиту сети. Современные антивирусные средства позволяют выполнять несколько типов операций поиска, как в обычных ситуациях, так и по требованию. Например, консоль Symantec System Center (управляющая Norton AntiVirus) позволяет настроить на серверах и компьютерах клиентов следующие операции поиска.

- *Чистка вирусов.* Позволяет проанализировать все диски на всех серверах и компьютерах клиентов, принадлежащих к выбранному объекту (как правило, к группе систем в определенной сети). Операции чистки вирусов обеспечивают немедленные результаты поиска в крупных областях сети (или в рамках всей сети).
- *Ручной поиск* (по требованию). Эта функция позволяет анализировать выбранные каталоги и диски на определенных компьютерах. Ручные операции поиска обеспечивают немедленные результаты анализа небольшой области сети или локального жесткого диска; они особенно полезны при тестировании только подозрительных компьютеров без задержек на крупных областях сети.
- *Регулярный поиск.* Эта функция позволяет анализировать выбранные каталоги и диски на определенных компьютерах в определенное время или по стандартному расписанию (например, каждый день или каждую неделю). Регулярные операции поиска идеально подходят для крупных областей сети, потому что в данном случае у вас появляется возможность запуска поиска в нерабочее время в условиях низкого уровня сетевого трафика.
- *Поиск в реальном времени.* Эти операции поиска в реальном времени анализируют файлы, считываемые или записываемые на сервер или клиентский компьютер. Norton AntiVirus позволяет настроить собственные операции поиска в электронной почте 32-битовым компьютерам клиентов.

Вы можете настроить ручные, регулярные и проводящиеся в реальном времени операции поиска в отношении каталогов и папок на компьютере клиента Norton AntiVirus Corporate Edition, а также выбрать два дополнительных типа операций поиска.

- *Специальный поиск.* Ручной запуск операции поиска в дальнейшем.
- *Поиск при запуске.* Автоматический поиск при запуске компьютера клиента.

Чистка вирусов

Мгновенный запуск операций поиска вирусов на серверах и компьютерах клиентов из управляющей антивирусной программы (например, из консоли Symantec System

Center) производится нажатием одной кнопки. Чистка вирусов может осуществляться применительно ко всей системе, одной или нескольким группам серверов или одному или нескольким серверам в древовидной схеме консоли Symantec System Center. Через несколько минут после запуска чистки вирусов в системе вы сможете убедиться, что во всей вашей сети нет ни одного вируса (и вам не придется отправлять пользователям сети сообщения с просьбой провести поиск вирусов в их компьютерах). Операция чистки вирусов обеспечивает отсутствие вирусов на серверах или рабочих станциях.

Примечание

Прервать операцию чистки вирусов в масштабах всей сети после ее запуска нельзя. Она должна завершиться.

Ручной поиск

Операция ручного поиска позволяет вам быстро обследовать целевую область сети. В отличие от операции чистки вирусов, в ходе которой анализируются все файлы на всех дисках, вы можете настроить ручной поиск на сужение области анализа. Пользуясь управляющей антивирусной программой (например, консолью Symantec System Center), вы можете запустить немедленный поиск на одном или нескольких серверах Norton AntiVirus Corporate Edition, находящихся в одной группе серверов, либо на одном или нескольких клиентах, управляемых одним сервером Norton AntiVirus.

Регулярный поиск

Пользуясь управляющей антивирусной программой (например, консолью Symantec System Center), вы можете настроить запуск операций поиска в определенное время дня каждый день, каждую неделю или каждый месяц. Регулярные операции поиска для серверов и клиентских машин необходимо задавать отдельно. Например, вы можете запланировать операции поиска на сервере, выбрав в древовидной структуре консоли Symantec System Center определенные группы серверов, или единственный сервер, или поиск на клиентских машинах, указав в той же структуре сервер или только одного клиента. Очень удобно планировать регулярные операции поиска таким образом, чтобы они происходили через некоторое время после предусмотренных графиком обновлений файлов определений вирусов. Так вы сможете добиться эффективного устранения недавно появившихся вирусов.

Операции поиска в реальном времени

Пользуясь управляющей антивирусной программой (например, консолью Symantec System Center), вы можете настроить защиту файловой системы в реальном времени как на серверах Norton AntiVirus Corporate Edition, так и на компьютерах клиентов Norton AntiVirus. Можно настроить защиту почтовых данных в реальном времени по отношению к известным почтовым приложениям, установленным на определенном компьютере клиента Norton AntiVirus. Защита сервера и компьютеров клиентов в реальном времени должна производиться по отдельности. После настройки защиты в реальном времени вы должны будете изменить ее лишь в случае изменения сетевой среды или политики безопасности.

Основы поиска вирусов на сервере

Регулярные операции поиска на серверах особенно важны постольку, поскольку вирусы могут быстро распространиться на клиентов и нанести ущерб загруженной сети. Вы можете провести поиск или настроить один или несколько серверов Norton AntiVirus Corporate Edition. Количество серверов, настраиваемых или подвергающихся поиску, зависит от выбранного объекта.

- *Все серверы сети.* Например, если выбрать в древовидной схеме консоли Symantec System Center всю сеть, вы сможете запускать операции чистки вирусов в отношении всех сетевых серверов Norton AntiVirus Corporate Edition. Операция чистки вирусов распространяется не только на сам сервер Norton AntiVirus, но и на всех клиентов Norton AntiVirus, которыми он управляет.
- *Все серверы в пределах выбранных групп серверов.* Если выбрать в древовидной схеме консоли Symantec System Center всю сеть, а затем на правой панели указать несколько групп серверов, вы сможете либо запустить операцию чистки вирусов, либо настроить регулярный поиск. При выполнении операции чистки вирусов проверка распространяется не на серверы Norton AntiVirus Corporate Edition и на их клиентов в рамках выбранных групп серверов, а регулярный поиск распространяется только на серверы.
- *Все серверы в пределах одной группы серверов.* Если выбрать объект группы серверов, вы сможете запустить операцию чистки вирусов или настроить регулярный поиск в отношении всех серверов, участвующих в определенной группе.
- *Некоторые серверы в группе серверов.* Если выбрать объект группы серверов, а затем указать несколько серверов из списка, вы сможете запустить на всех выделенных серверах операцию чистки вирусов или ручной поиск (но, если вы хотите настроить регулярный поиск, выбрать несколько серверов вам не удастся).
- *Один сервер.* Если выбрать в качестве объекта единственный сервер, вы сможете запустить на нем и на всех его клиентах операцию чистки вирусов, выполнить ручной поиск или настроить регулярный поиск на сервере или на его клиентских компьютерах.

Основы поиска вирусов на компьютере клиента

С помощью управляющего антивирусного программного обеспечения (типа Symantec System Center) вы можете выполнить поиск или настроить один или несколько клиентских компьютеров Norton AntiVirus Corporate Edition. Уровень настройки зависит от выбранного объекта.

- *Все клиенты сети.* Если выбрать всю сеть, вы сможете запустить операцию чистки вирусов в отношении всех присутствующих в сети 32- и 16-битовых клиентских компьютеров Norton AntiVirus Corporate Edition. В этом случае операция чистки вирусов будет распространяться на все серверы Norton AntiVirus, которые управляют клиентскими компьютерами.
- *Все клиенты в рамках выбранных групп серверов.* Если выбрать в древовидной схеме консоли Symantec System Center всю сеть, а затем на правой панели указать несколько групп серверов, вы сможете запустить операцию чистки вирусов. Эта операция распространится на все серверы Norton AntiVirus Corporate Edition, а

также на их 32- и 16-битовые клиентские компьютеры в рамках выбранных групп серверов.

- *Все клиенты в рамках одной группы серверов.* Если выбрать объект группы серверов, вы сможете запустить операцию чистки вирусов для поиска на всех 32- и 16-битовых клиентских компьютерах в рамках одной группы серверов.
- *Все клиенты, подключенные к одному серверу.* Если выбрать в качестве объекта отдельный сервер, вы сможете запустить операцию чистки вирусов или настроить регулярный поиск. Чистка вирусов будет производиться на всех 32- и 16-битовых клиентских компьютерах, управляемых данным сервером. Регулярный поиск распространится лишь на 32-битовые компьютеры клиентов, управляемых сервером.
- *Отдельные 32-битовые клиентские компьютеры на одном сервере.* Если выбрать в древовидной схеме консоли отдельный сервер, а затем на правой панели указать несколько 32-битовых клиентских компьютеров, вы сможете выполнять операцию ручного поиска.
- *Один 32-битовый клиентский компьютер.* Если выбрать в качестве объекта один 32-битовый клиентский компьютер, вы сможете выполнить ручной поиск или настроить регулярный поиск только для этого компьютера.
- *16-битовые серверы.* Провести независимую настройку и выполнить поиск на каждом 16-битовом компьютере невозможно. Впрочем, 16-битовые компьютеры участвуют в операциях чистки вирусов, а задать настройки защиты 16-битовых клиентов в реальном времени вы можете на уровне сервера или группы серверов.

Введение в "ложные обнаружения"

Ложное обнаружение (иногда оно называется ошибочным результатом анализа) представляет собой такую ситуацию, когда ваша антивирусная программа отправляет сообщение с предупреждением о вирусе, которого на самом деле не существует (или добавляет запись в журнал регистрации). Ложные обнаружения наиболее вероятны в случае применения на одном компьютере антивирусных программ от нескольких производителей, т. к. некоторые такие программы оставляют незащищенными в памяти кодовые подписи, применяемые для обнаружения. Столкнувшись с предупреждением или записью в журнале, безопаснее всего рассматривать эти данные как реальную угрозу инфицирования и предпринять все действия, необходимые для удаления вируса из системы. Но если вы считаете, что антивирусная программа сгенерировала ложное обнаружение (например, она маркировала файл, которым вы безо всяких последствий пользуетесь уже много лет, как инфицированный), не спешите связываться с производителем этой программы, а проверьте, не оказались ли вы в одной из следующих ситуаций.

- На вашем компьютере работает несколько антивирусных программ. Если это так, то одна из них могла обнаружить незащищенные кодовые подписи, применяемые другой программой, и сообщить о них как о вирусах. Чтобы избежать появления подобного сбоя, настройте вашу сеть на применение одной антивирусной программы. Возможно, для этого придется деинсталлировать ненужное антивирусное программное обеспечение на всех серверах и клиентских машинах.
- Вы пользуетесь микросхемой BIOS с функциями защиты от вирусов. Во многих современных версиях BIOS поддерживаются антивирусные функции (предназна-

ченные для защиты от инфицирования загрузочного сектора). Они могут инициировать ложные обнаружения во время работы программного антивирусного обеспечения. Если на каком-либо клиентском компьютере или на сервере фиксируются ложные обнаружения, вы можете попробовать отключить антивирусную защиту в CMOS Setup этой системы.

- В сети есть старые компьютеры. Некоторые устаревшие компьютеры (от производителей типа HP) корректируют загрузочные секторы на своих жестких дисках при каждой загрузке. Антивирусное программное обеспечение может рассматривать эти изменения как вирусы, хотя на самом деле они ими не являются. Чтобы устранить такой сбой, обновите компьютеры, на которых фиксируется эта ошибка, или воспользуйтесь версией антивирусной программы с командной строкой, чтобы добавить прямо в загрузочные файлы информацию о правильности данных. При использовании этого метода информация о загрузочном секторе или главной загрузочной записи не сохраняется.
- Установлено программное обеспечение с защитой от копирования. В зависимости от типа применяемой защиты от копирования, ваша антивирусная программа может обнаруживать вирусы в загрузочном секторе или в главной загрузочной записи на некоторых гибких дисках или на других носителях. Свяжитесь с разработчиком подозрительного программного обеспечения и узнайте, существует ли заплата или обновление (возможно, какой-то другой устанавливаемый вариант), с помощью которого эту неисправность можно было бы устранить.

Примечание

Если ни одно из упомянутых условий в вашей ситуации не соблюдается, вам следует связаться с производителем антивирусного программного обеспечения и проинформировать его о ложном обнаружении. После этого производитель сможет разобраться в его причинах и внести необходимые исправления в последующие заплаты и обновления данных.

Установка антивирусных средств

Не считая некоторых мощных брандмауэров, которые поддерживают проверку на наличие вирусов (типа Sonic Wall SOHO2), все антивирусные продукты реализуются в качестве программного обеспечения (как и пакет Symantec Norton Internet Security на рис. 19.1), которое нужно устанавливать на отдельные компьютеры. Что касается сетевого применения, средства антивирусной защиты должны устанавливаться как на серверах, так и на клиентских компьютерах. После установки антивирусного ПО его следует регулярно обновлять, чтобы обеспечить наличие самых свежих определений вирусов и других методик защиты. В этой части главы мы рассмотрим базовые вопросы установки антивирусных программ на компьютерах конечных пользователей и в масштабах сети.

Установка на отдельных компьютерах

Обычно процесс установки антивирусного программного обеспечения на отдельных компьютерах проходит автоматически под управлением мастера установки, приводимого в действие с помощью файла автоматической загрузки, который открывается

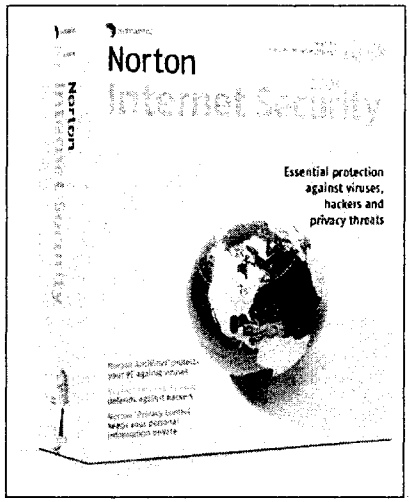


Рис. 19.1. Norton Internet Security является ведущим антивирусным средством/брандмауэром для компьютеров и рабочих станций (публикуется с разрешения Symantec)

при помещении компакт-диска в привод CD-ROM. После этого для завершения инсталляции нужно всего лишь следовать указаниям мастера, который выполняет первоначальную операцию поиска в системе, копирует на компьютер файлы, вносит в конфигурацию системы необходимые изменения, а затем перезагружает компьютер, после чего антивирусная программа начинает работать в фоновом режиме. В одноранговой сети копия антивирусной программы должна быть установлена на каждом узле.

Примечание

Для установки антивирусного программного обеспечения на нескольких компьютерах в одноранговой сети вам понадобится многопользовательская лицензия. В более крупных серверных сетях применяется корпоративная (для предприятий) версия антивирусной программы, включающая узловую лицензию.

Установка в сети

При администрировании сети, содержащей один или несколько серверов и множество клиентских компьютеров, установка антивирусного ПО становится несколько более сложным процессом. Вам, естественно, придется установить антивирусные утилиты на серверах и клиентских компьютерах, но значение имеет сам порядок установки этих продуктов. Например, Symantec рекомендует следующую последовательность установки корпоративной версии Norton AntiVirus.

1. Установку Symantec System Center следует выполнять до инсталляции управляющего интегрируемого приложения Norton AntiVirus Corporate Edition.
2. Попытки управлять Norton AntiVirus Corporate Edition из консоли Symantec System Center должны производиться после установки управляющего интегрируемого приложения Norton AntiVirus Corporate Edition.

3. Установка Norton AntiVirus Corporate Edition должна производиться сначала на серверах, а потом на клиентских компьютерах. Если сначала провести инсталляцию на клиентских компьютерах, они не смогут подключиться к серверу Norton AntiVirus Corporate Edition и будут работать в "неуправляемом" режиме.
4. Остальные продукты и утилиты можно устанавливать в любом порядке.

Лабораторное тестирование на серверах

Один из рисков, связанных с установкой важного сетевого программного обеспечения, заключается в возможности появления непредвиденных сбоев (сетевых отказов) вследствие неожиданных проблем с новыми программами. Например, если новое антивирусное ПО несовместимо с другими программами, установленными на сервере или клиентских компьютерах, существует возможность снижения производительности, сбоев и других трудностей. Прежде чем приступать к полномасштабной установке, имеет смысл на время обучения и на оценочный период установить новое антивирусное программное обеспечение в удаленной (некритической) лабораторной среде. Это позволит вам изучить новые программы более подробно, ознакомиться с их возможностями и отработать любые проблемы, связанные с совместимостью или производительностью, до их полной установки в масштабах всего предприятия.

Наилучшие результаты тестирования достигаются при установке антивирусного программного обеспечения как минимум на двух серверах. При необходимости вы сможете проверить его как в Windows NT/2000, так и в NetWare. Протоколы обмена данными в испытательной среде должны соответствовать тем, что установлены в рабочей сетевой среде. В испытательную среду следует включить маршрутизаторы (в особенности это касается смешанных протокольных сред). Выполните полную инсталляцию (включая все необходимые утилиты управления) на каждом сервере. После установки ПО на испытательных серверах сделайте следующее.

1. Настройте операции поиска вирусов на максимальную защиту (т. е. поиск во всех файлах, на всех дисках и т. д.)
2. Протестируйте вспомогательные функции типа загрузки файлов определений вирусов и обновлений по схеме "с сервера на сервер".
3. Создайте тестовый инфицированный файл (но не настоящий вирус), чтобы проанализировать работу механизмов обнаружения вирусов без необходимости внедрения в систему реального вируса.
4. Регулярные операции поиска и другие автоматизированные функции должны проработать в течение нескольких дней.
5. Убедитесь в том, что управляющее программное обеспечение (например, Alert Management System от Symantec) способно обнаруживать серверы с обеих сторон от маршрутизаторов (если это необходимо).
6. Убедитесь в том, что в журналах регистрации и отчетах ожидаемые данные фиксируются достаточно точно.

Тестовые инфицированные файлы

Важно протестировать антивирусное программное обеспечение, чтобы оценить его поведение, но испытывать его с применением настоящего вируса опасно. Впрочем, вы можете создать текстовый файл, который должен быть интерпретирован как ви-

рус. С его помощью вы сможете проверить работу механизмов обнаружения вирусов, регистрацию и предупреждения. Скопируйте нижеследующую строку в отдельный текстовый файл и сохраните его как TestVirus.com. Это не вирус, но он должен быть обнаружен и интерпретирован как вирус EICAR Test String.70 (возможно, перед сохранением этого файла вам придется на время отключить защиту файлов в реальном времени).

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Примечание

Не ставьте пробелы перед или после этой строки. Наличие пробелов может предотвратить обнаружение вируса.

Лабораторное тестирование на клиентских компьютерах

Как и в случае с серверами, клиентские компьютеры и предназначенное для них новое антивирусное программное обеспечение также следует протестировать до его установки в рабочей среде. Испытания клиентских программ нужно проводить в некритической среде. Возможно, вы обнаружите потенциальные проблемы, связанные с совместимостью или производительностью, которые способны понизить уровень эффективности. Как бы то ни было, набор аппаратного и программного обеспечения в испытательной среде должен быть максимально приближен к условиям рабочей сетевой среды. Ниже приводятся некоторые инструкции по тестированию.

- ❒ Установите антивирусное ПО во всех операционных системах, которыми планируете пользоваться.
- ❒ Установите антивирусное ПО как на подключенные, так и на автономные клиентские компьютеры (если это необходимо).
- ❒ Обеспечьте соответствие всех сочетаний протоколов IP/IPX с условиями рабочей среды.
- ❒ Обеспечьте соответствие всех сочетаний операционных систем по схеме "от клиента к серверу" (например, предоставьте рабочим станциям Windows NT возможность регистрироваться на серверах NetWare и т. д.)
- ❒ Наборы аппаратного обеспечения должны отражать минимальную и максимальную конфигурации.

После установки нового антивирусного программного обеспечения на клиентские компьютеры сделайте следующее.

1. Настройте антивирусную программу на максимальную защиту (т. е. на поиск вирусов во всех файлах, на всех дисках и т. д.).
2. Попробуйте загрузить файл с определениями вирусов.
3. Предоставьте тестовому инфицированному файлу (процесс создания которого описывался выше) возможность инициировать работу системы предупреждений.
4. Регулярные операции поиска и другие автоматизированные функции должны проработать в течение нескольких дней.
5. Убедитесь в том, что управляющее ПО способно обнаруживать клиентские компьютеры по обе стороны от маршрутизаторов.

6. Убедитесь в том, что подключенные клиенты фиксируются управляющим ПО в связке с соответствующим родительским сервером.
7. Воспользовавшись управляющим ПО, просмотрите параметры операций поиска на одном из клиентских компьютеров и убедитесь в том, что клиенты не имеют возможности изменять эти настройки.
8. Запустите операцию чистки вирусов и убедитесь в ее выполнении на всех клиентских машинах.
9. Убедитесь в том, что в журналах регистрации и в отчетах фиксируются ожидаемые данные.

Поэтапная установка

После завершения лабораторных испытаний вам может понадобиться провести тестирование и поэтапную установку новых антивирусных средств, чтобы обеспечить непрерывность сетевых операций. Метод поэтапной установки широко применяется в крупных организациях. Он поддерживает установку антивирусной программы на тестовый сервер с последующим систематическим ее распространением на дополнительные группы серверов; это делается в несколько стадий в течение некоторого периода времени, и тем самым любые проблемы, которые потенциально могут возникнуть в вашей среде, выявляются до полномасштабной установки антивирусного программного обеспечения в рамках всей сети. Решение о том, как именно провести этот процесс, в основном, остается за вами. Например, вы можете приступить к установке антивирусных средств на управляемых клиентских машинах после их инсталляции на одном или нескольких серверах или же начать с установки этих средств на всех серверах и продолжить их инсталляцию на всех клиентских компьютерах. В числе других примеров можно привести поэтапную установку на серверах Windows NT/2000, затем на серверах NetWare или только на клиентах Windows. После этого можно приступать к другим операционным системам, чтобы проработать все возможные трудности для каждой платформы в отдельности. Основная идея заключается в том, чтобы переходить от одного небольшого, тщательно продуманного этапа к другому, а не подвергать сеть риску возникновения серьезных проблем при полной одновременной установке.

Типичные примеры установки на сервере

Теперь пришло время изучить процесс инсталляции типичного антивирусного программного пакета для предприятий. В нашем примере мы рассмотрим серверное программное обеспечение Symantec Norton AntiVirus Corporate Edition и служебную программу Alert Management System. При установке любого программного обеспечения необходимо ознакомиться с конкретными рекомендованными процедурами. Как правило, вместе с антивирусным ПО устанавливаются средства поддержки и управляющие средства. Например, при инсталляции Norton AntiVirus Corporate Edition на серверах и рабочих станциях Windows NT/2000 (или на серверах NetWare) вы можете установить программу Alert Management System (AMS), которая будет работать на всех первичных серверах. Несмотря на то, что наличие AMS требуется лишь на первичном сервере, где она обеспечивает настройку и просмотр предупреждений, ее следует установить на все компьютеры с серверным вариантом Norton AntiVirus. Это позволяет сделать первичным сервером каждый из этих компьютеров.

Если вам придется сделать вторичный сервер первичным, то события AMS не будут потеряны.

Примечание

Если вы пользуетесь другими операционными системами (например, Linux/UNIX или MacOS), обратитесь к инструкциям производителя по установке конкретной версии антивирусного программного обеспечения.

Серверы Windows NT/2000

Ниже приведены типичные этапы установки Norton AntiVirus Corporate Edition на серверах Windows NT/2000:

1. Запустите мастер установки. Нажмите **Install Norton AntiVirus To Servers** и проверьте, установлен ли флажок **Install Norton AntiVirus Server**. Если сначала вы установили дополнения Symantec System Center, выберите пункт **AV Server Rollout** меню **Symantec System Center Tools**.
2. Нажмите кнопку **Next**. Прочтите лицензионное соглашение и гарантийные обязательства, выберите **I Agree** и еще раз нажмите кнопку **Next**.
3. Проверьте, установлены ли флажки **Server Program** и **Alert Management System (AMS)**, и нажмите кнопку **Next**. Файлы AMS применяются только на первичном сервере. Если вы установите флажок **AMS**, эта служба будет установлена на всех серверах, на которых пройдет инсталляция серверной программы Norton AntiVirus. Это позволит вам изменить первичный сервер без необходимости переустановки AMS на новом первичном сервере. Если вы не планируете менять первичный сервер, удалите файлы AMS с непервичных серверов.
4. Двойным щелчком выберите **Microsoft Windows Network**.
5. Укажите сервер, на котором планируется выполнить инсталляцию, и нажмите кнопку **Add**.
6. Повторите предыдущий этап для всех необходимых серверов.
7. Если вы создали текстовый файл с указанием IP-адресов для импортирования компьютеров, расположенных вне сред WINS, переходите к шагу 8. Если вы не создавали такого файла, переходите к шагу 12.
8. Чтобы импортировать список серверов, нажмите кнопку **Import**. Функция Import предназначена для применения только в системах на базе Windows NT. Она не рассчитана на NetWare.
9. Укажите местоположение и двойным щелчком выберите текстовый файл с указанием имен компьютеров. В результате появится сводный перечень компьютеров, которые будут включены в список **Available Computers**. В ходе процесса аутентификации вам, возможно, придется предоставить имена пользователей и пароли для тех компьютеров, которые требуют выполнения аутентификации.
10. Нажмите кнопку **OK**.
11. В ходе аутентификации программа установки проводит проверку на наличие различных сбойных ситуаций. У вас будет выбор: либо просмотреть эту информацию в интерактивном режиме на каждом из компьютеров, либо зафиксировать ее в журнале регистрации для последующего ознакомления. В случае соз-

дания журнала регистрации вы должны знать его местоположение (например, c:\Winnt\Navsecrv.txt).

12. Чтобы создать запись в журнале регистрации, нажмите кнопку **Yes**; чтобы просмотреть интерактивные данные, нажмите кнопку **Next**.
13. Нажмите кнопку **Next**.
14. Согласитесь с принимаемым по умолчанию путем установки антивирусной программы или измените его (укажите компьютер и нажмите кнопку **Change Destination**); затем нажмите кнопку **Next**.
15. Введите имя новой группы серверов и нажмите кнопку **Next**. Вам будет предложено подтвердить создание новой группы серверов. С другой стороны, вы можете выбрать существующую группу серверов, к которой планируете присоединиться, затем нажать кнопку **Next** и при появлении соответствующего приглашения ввести пароль этой группы серверов.
16. Выберите вид запуска: автоматический (**Automatic**) или ручной (**Manual**). Если вы выберите **Automatic**, службы Norton AntiVirus (а также службы AMS, если вы их установили) будут запускаться автоматически после каждой перезагрузки сервера. Если выбрать **Manual**, то после каждой перезагрузки эти службы нужно будет запускать вручную.
17. Нажмите кнопку **Next**. В результате появится экран **Using the Symantec System Center Program**.
18. Нажмите кнопку **Next**. Появится экран **Setup Summary** с указанием пароля по умолчанию, применяемого для разблокировки группы серверов (в нашем примере по умолчанию принимается пароль `symantec`).
19. Нажмите кнопку **Finish**. На экране **Setup Progress** будет показано состояние процесса установки программы на серверах.
20. После того как пакет Norton AntiVirus будет установлен на всех указанных серверах, проверьте, не поступало ли сообщений об ошибках. В нашем примере следует указать нужный сервер и для получения дополнительной информации нажать кнопку **View Errors**.
21. По завершении процесса инсталляции нажмите кнопку **Close**. На этом инсталляция программного обеспечения на серверах должна быть закончена.

Серверы NetWare

При установке Norton AntiVirus в службе каталогов NetWare (NetWare Directory Services, NDS) желательно, чтобы компьютер, на котором проходит процесс инсталляции, использовал клиентскую программу Novell Client для NetWare. Если вы встретитесь с трудностями при установке антивирусного ПО в NDS с Microsoft Client для NetWare, установите Novell Client для NetWare и запустите процесс инсталляции еще раз. Ниже приведены типичные этапы установки Norton AntiVirus Corporate Edition на серверах Novell NetWare.

1. Зарегистрируйтесь на всех серверах NetWare, на которых планируется установить Norton AntiVirus Corporate Edition.
2. Запустите мастер установки. Нажмите **Install Norton AntiVirus To Servers**. Вы также можете перейти на консоль Symantec System Center и выбрать **Tools**, **AV Server**

Rollout (этот пункт доступен лишь при условии предварительной установки дополнений Symantec System Center).

3. Проверьте, установлен ли флажок **Install Norton AntiVirus To Servers**, и нажмите кнопку **Next**.
4. Прочтите лицензионное соглашение и гарантийные обязательства, выберите **I Agree** и нажмите кнопку **Next**.
5. Проверьте, установлен ли флажок **Server Program**, и нажмите кнопку **Next**.
6. Если вы пользуетесь Novell Client для NetWare, двойным щелчком выберите **NetWare Services**. В случае применения Microsoft Client для NetWare следует двойным щелчком выбрать **NetWare Or Compatible Network**.
7. Выберите используемого клиента.
   - *Novell Client для NetWare*. Чтобы установить антивирусные средства на сервер Bindery, двойным щелчком выберите **NetWare Servers** и укажите сервер (он обозначается пиктограммой сервера).
   - *Novell Client для NetWare*. Чтобы установить антивирусные средства в NDS, двойным щелчком выберите **Novell Directory Servers**, а затем укажите объект тома SYS, в котором вы намереваетесь провести инсталляцию Norton AntiVirus.
   - *Microsoft Client для NetWare*. Чтобы установить антивирусные средства на сервер Bindery, укажите его (сервер обозначается пиктограммой сервера).
   - *Microsoft Client для NetWare*. Чтобы установить антивирусные средства в NDS, выберите объект тома SYS, в котором вы намереваетесь провести инсталляцию Norton AntiVirus.
8. Нажмите кнопку **Add**. Если вы проводите инсталляцию в NDS, на экране появится приглашение на выбор контейнера, ввод имени пользователя и пароля. В случае ввода на этом этапе неверного имени пользователя и пароля процесс инсталляции, несмотря ни на что, будет продолжен в нормальном режиме. Впрочем, в дальнейшем при попытке запустить Norton AntiVirus на сервере NetWare вы получите сообщение об ошибке аутентификации, а также приглашение на ввод правильного имени пользователя и пароля.
9. Повторите шаги 7 и 8 по отношению к томам всех серверов, на которых планируете установить антивирусное программное обеспечение.
10. Нажмите кнопку **Next**.
11. Согласитесь с принимаемым по умолчанию путем установки Norton AntiVirus Corporate Edition, а при необходимости измените его; затем нажмите кнопку **Next**.
12. Введите имя новой группы серверов, нажмите кнопку **Next**, а затем (для подтверждения) кнопку **Yes**. Вы также можете указать существующую группу серверов, к которой планируете присоединиться; после этого следует нажать кнопку **Next** и при появлении соответствующего приглашения ввести пароль этой группы серверов.
13. Выберите вариант запуска: автоматический (**Automatic Startup**) или ручной (**Manual Startup**) и нажмите кнопку **Next**. В случае выбора **Automatic Setup** vpstart.nlm будет автоматически запускаться после каждой загрузки сервера

(прежде чем это положение вступит в силу, вы должны завершить процесс инсталляции). Если выбрать **Manual Setup**, то после каждой загрузки сервера вам придется запускать vpstart.nlm вручную.

14. Последовательно нажимайте кнопку **Next**, пока не перейдете к последнему диалоговому окну, а затем нажмите кнопку **Close**.

15. После завершения процесса инсталляции запустите vpstart.nlm на всех серверах NetWare, на которые этот процесс распространялся. Это можно сделать через серверную консоль (или, при наличии соответствующих полномочий, через RConsole). При первом после инсталляции запуске vpstart.nlm вы должны указывать ключ `/Install` — например, `load Sys:Nav\Vpstart.nlm /Install`. На этом процесс серверной инсталляции должен быть завершен.

Примечание

Помните, что все эти процедуры приводятся исключительно в качестве примеров. Вы в любом случае должны следовать инструкциям по установке, приведенным в вашей программе антивирусной защиты.

Типичные примеры установки на клиентских компьютерах

После инсталляции антивирусного ПО на серверах вы должны будете установить его клиентские версии на каждой рабочей станции. Распространенные антивирусные продукты поддерживают возможность установки клиентских программ с клиентского образа диска, расположенного на сервере, а также дают возможность применения установочного компакт-диска локально, т. е. на каждом клиентском компьютере в отдельности. В нашем примере мы рассмотрим установку Norton AntiVirus (но вам в любом случае следует ознакомиться с процедурами установки, рекомендуемыми в отношении вашего программного обеспечения).

Размещение образа диска

В процессе инсталляции Norton AntiVirus Corporate Edition на серверах программа установки (Setup) создает клиентские образы диска (или установочный каталог) на каждом защищенном сервере. Впоследствии пользователи клиентских компьютеров могут запускать программу установки Norton AntiVirus напрямую с серверов, к которым они подключены. Антивирусный клиент будет установлен в управляемом (Managed) режиме; он будет отображаться в управляющем ПО (например, Symantec System Center) при выборе в древовидной схеме консоли связанного с ним сервера. Когда клиент работает в управляемом режиме, у вас появляется возможность настраивать автоматические обновления файлов определений на клиентских машинах и администрировать их через управляющее программное обеспечение.

На серверах Windows NT/2000, например, совместно используемым каталогом по умолчанию является \\Server\Vphome\Clt-inst, и каждый пользователь имеет полномочия для его чтения. На серверах NetWare по умолчанию принимается совместно используемый каталог \\Server\Sys\Nav\Clt-inst. Программа установки (Setup) создает группу под названием nortonantivirususer. При добавлении в эту группу новых пользователей они получают все необходимые полномочия для запуска программы клиентской инсталляции с клиентского образа диска, расположенного на сервере. С другой стороны, если вы разместите установочный компакт-диск на совместно

используемом сетевом диске, пользователям придется подключать его к своим рабочим станциям. Только таким образом они смогут обеспечить успешную инсталляцию всех компонентов. Чтобы установить клиентский образ диска с сервера, выполните следующие действия.

1. Убедитесь в том, что пользователи наделены полномочиями на обращение к клиентскому образу диска, расположенному на сервере.
2. Предоставьте пользователю путь и (при необходимости) подключение к клиентскому образу диска. На серверах NetWare по умолчанию принимается путь \\Server\Sys\Nav\Clt-inst. На серверах Windows NT по умолчанию принимается совместно используемый каталог \\Server\Vphome\Clt-inst.
3. Убедитесь в том, что пользователь знает, версию для какой платформы он должен установить. В случае с Norton AntiVirus в каталоге Clt-inst на каждом сервере имеются следующие установочные каталоги:
   - Clt-inst\Win32\Setup.exe;
   - Clt-inst\Win16\Setup.exe;
   - Clt-inst\Dos\Install.bat.

Удаленная инсталляция

У вас есть возможность провести удаленную инсталляцию клиентской версии Norton AntiVirus на любом компьютере Windows NT/2000 или NetWare, подключенном к сети. Вы также можете провести одновременную инсталляцию на нескольких клиентских компьютерах, во время которой физически обращаться к каждой из них не придется. Преимущество удаленной инсталляции заключается в том, что пользователям перед ее выполнением не нужно регистрироваться на своих компьютерах в качестве администраторов (все это возможно лишь в том случае, если у вас есть административные полномочия по отношению к домену, к которому принадлежат данные пользовательские компьютеры). Чтобы установить Norton AntiVirus, сделайте следующее.

1. Запустите программу установки антивирусного программного обеспечения и выберите **Install Norton AntiVirus To NT Clients**. В результате появится экран **Welcome**.
2. Нажмите кнопку **Next** и двойным щелчком выберите **Microsoft Windows NT Network**.
3. Выберите нужный компьютер, а также сервер, на котором установлена программа Norton AntiVirus, и нажмите кнопку **Add**.
4. Повторяйте предыдущий шаг в отношении всех клиентских компьютеров, которыми предполагаете управлять.
5. Если вы создали текстовый файл с указанием IP-адресов для импортирования компьютеров, расположенных вне сред WINS, переходите к шагу 6. Если вы не создавали такого файла, переходите к шагу 10.

Примечание

Функция Import предназначена для применения исключительно в операционных системах Windows NT/2000/XP. Она не рассчитана на NetWare.

6. Чтобы импортировать перечень компьютеров, нажмите кнопку **Import**.
7. Укажите местоположение и двойным щелчком выберите текстовый файл с указанием имен компьютеров. В результате появится сводный перечень компьютеров, которые будут включены в список **Available Computers**. В ходе процесса аутентификации вам, возможно, придется предоставить имена пользователя и пароли для тех компьютеров, которые требуют выполнения аутентификации.
8. Нажмите кнопку **OK**.
9. В ходе процесса аутентификации программа установки проводит проверку на наличие разнообразных сбойных ситуаций. У вас будет выбор: либо просмотреть эту информацию в интерактивном режиме на каждом из компьютеров, либо зафиксировать ее в журнале регистрации для последующего ознакомления. В случае создания журнала регистрации имейте в виду, что он расположен на диске C: (например, c:\Winnt\Navsecrv.txt).
10. Чтобы создать запись в журнале регистрации, нажмите кнопку **Yes**; чтобы просмотреть интерактивные данные, нажмите кнопку **No**.
11. Нажмите кнопку **Finish**.

Образы вирусов

Антивирусные средства сравнивают содержимое файлов с перечнем известных "образов" — признаков, которые указывают на наличие вируса. На сегодняшний день в файле образов может быть зафиксировано свыше 50 000 образов, причем каждый день выявляются все новые образы. Это означает, что для обеспечения оптимальной защиты сети вам нужно регулярно обновлять файлы образов вирусов. В большинстве случаев у вас есть возможность загрузки новых файлов образов вирусов непосредственно с Web-сайта производителя антивирусной программы (часто это делается автоматически); после этого вам нужно передать новые файлы образов вирусов всем клиентам вашей сети. Этот процесс значительно упрощает задачу устранения вирусов, позволяя администратору обновлять средства защиты в масштабе всей сети без необходимости в загрузке или передаче обновлений образов на каждый компьютер в отдельности.

Устранение инфекций

Вирусы далеко не безобидны, но большинство из них в случае заражения вашей сети не будут уничтожать данные или приводить ваш компьютер в нерабочее состояние. Даже те сравнительно редко встречающиеся вирусы, которые содержат разрушительную полезную нагрузку, обычно делают свое черное дело в ответ на какое-либо инициирующее событие. В большинстве случаев (если вы не наблюдаете свидетельств активизированной полезной нагрузки) у вас будет время на то, чтобы должным образом разобраться с инфекцией. Впрочем, в силу самого своего присутствия эти небольшие фрагменты нежелательного компьютерного кода могут препятствовать нормальной работе вашего компьютера, потреблять системные ресурсы и оказывать другие виды отрицательного воздействия, так что их нужно принимать всерьез и обязательно устранять, как только вы с ними встретитесь.

Необходимо принять во внимание и тот факт, что странное поведение компьютерной системы, ее необъяснимые отказы и другие непредсказуемые события не обязательно обуславливаются зараженностью этой системы вирусами. Если на основании подобных случаев вы считаете, что на вашем компьютере присутствует вирус, его поиск, возможно, не приведет к ожидаемым результатам, но он поможет исключить одно из предположений о причинах неисправности компьютера.

При инсталляции антивирусного ПО программа установки запускает антивирусное приложение, которое обследует память вашего компьютера, а также загрузочные секторы на его жестком диске и в результате убеждается, что может безо всяких рисков инфицирования копировать свои файлы на жесткий диск. Если это приложение не обнаруживает инфекций, доведите процесс установки до завершения, а затем, после перезагрузки компьютера, проведите детальный поиск вирусов в масштабах всей системы. Вирусы, инфицирующие файлы, которые не загружаются в память компьютера и не прячутся в блоках начальной загрузки на вашем жестком диске, могут, тем не менее, присутствовать в других местах в вашей системе.

Обнаружение инфекций во время установки

Если в ходе процесса инсталляции антивирусное приложение все же обнаруживает вирусы, вы должны удалить их из системы. Только после этого вы сможете установить программу. Ниже приводится пример устранения вирусов во время первоначальной инсталляции антивирусных средств.

1. Немедленно выйдите из программы установки (Setup) и выключите компьютер. Обязательно полностью отключите питание вашей системы. Не пользуйтесь сочетанием клавиш <Ctrl>+<Alt>+<Del> и производите сброс компьютера для перезагрузки системы, т. к. во время такой горячей перезагрузки некоторые вирусы остаются в силе.
2. Если во время инсталляции вы создали антивирусный аварийный загрузочный диск, обеспечьте его защиту от записи и вставьте его в дисковод. Некоторые антивирусные средства поддерживают загрузочную CD-версию аварийного диска. Если вы не создали аварийный диск (а ваш компьютер настроен на запуск с загрузочного компакт-диска), поместите установочный компакт-диск в дисковод CD-ROM; теперь вы можете переходить к следующему шагу.
3. Подождите по меньшей мере 15 секунд, после чего снова включите компьютер.
4. Во время перезагрузки вашего компьютера аварийный диск запускает командный файл, который помогает вам выполнить операцию аварийного поиска вирусов. В первую очередь командный файл спрашивает, выполнили ли вы выключение компьютера с его последующим включением. Чтобы продолжить, нажмите клавишу <Y>.
5. Прочтите выведенное на экран предупреждение; затем, чтобы продолжить, нажмите любую клавишу.
6. Аварийный диск загрузит в память все необходимые файлы.
7. Механизм поиска вирусов на основе командной строки, расположенный на аварийном диске (например, в файле BOOTSCAN.EXE), выполнит поиск четыре раза, обследуя загрузочные секторы вашего жесткого диска, главную загрузочную

запись, системные каталоги, программные файлы и другие вероятные точки инфицирования на всех жестких дисках локального компьютера.

Примечание

Аварийный диск не будет пытаться обнаружить макровирусы, сценарные вирусы и троянских коней; он будет проверять систему на наличие вирусов, инфицирующих файлы, и вирусов, расположенных в загрузочном секторе.

8. Если программа BOOTSCAN.EXE обнаружит вирус, она попытается очистить инфицированный файл. Если ей это не удастся, она запретит доступ к этому файлу и продолжит операцию поиска. После завершения всех повторов этой операции она выведет на экран краткий отчет обо всех действиях, предпринятых ею по отношению к каждому жесткому диску. Если механизм поиска обнаруживает вирус, он издает звуковой сигнал и сообщает имя и местонахождение вируса.
9. Когда механизм поиска завершает обследование жесткого диска, вы должны извлечь аварийный диск из дисковода, а затем еще раз выключить компьютер.
10. После того как BOOTSCAN.EXE завершит анализ вашей системы, вы можете либо еще раз попытаться установить антивирусную программу, либо попробовать очистить все оставшиеся вирусы и продолжить работу.

Обнаружение инфекций после установки

Когда антивирусная программа обнаруживает вирус, она оповещает вас об этом, выводя на экран предупредительное сообщение. В этом случае лучше всего попытаться очистить инфицированный файл. При очистке вирус удаляется с вашего сервера, клиентского компьютера или беспроводного устройства, после чего проводится попытка восстановления инфицированного файла. Как правило, обойтись с вирусом можно одним из следующих способов.

- *Попытаться провести восстановление.* Возможно, вам будет предложено восстановить файл. При этом подразумевается устранение инфекции с сохранением файла и продолжением его использования. Этот процесс не всегда проходит гладко, и многие пользователи предпочитают лишний раз предпринять меры предосторожности и удаляют инфицированный файл.
- *Наложить на файл карантин.* Чтобы изолировать инфицированный файл, нужно выбрать опцию **Quarantine**. После наложения на файл карантина следует воспользоваться Instant Updater, чтобы загрузить самые свежие файлы с образами вирусов. Затем вы можете предпринять еще одну попытку очистки инфицированного файла.
- *Удалить файл.* Нажатие кнопки **Delete** приводит к тому, что с вашего компьютера удаляется и вирус, и инфицированный им файл. Выбирать опцию **Delete** следует лишь в том случае, если у вас есть резервная копия данного файла.
- *Прекратить работу.* Если все остальные средства не позволяют достичь желаемого результата, выберите опцию **Stop**, чтобы прекратить поиск, и воспользуйтесь методом восстановления с помощью аварийного диска, рассмотренным выше.

Поиск неисправностей антивирусных средств

Правильное применение антивирусных средств является залогом успеха в борьбе с вирусами. Ассортимент компьютерных магазинов включает огромное количество продуктов антивирусной защиты. Научиться правильно и успешно пользоваться этими продуктами не всегда просто. В этой части главы мы рассмотрим некоторые методики, помогающие разобраться в трудностях, связанных с антивирусным программным обеспечением.

Вопросы установки

В большинстве случаев процесс установки антивирусных средств (в том числе их корпоративных вариантов) проходит вполне гладко, но случаются и трудности. Неудачная инсталляция может привести к возникновению программных неисправностей, локализовать которые бывает очень сложно. Среди наиболее распространенных причин сбоев при установке стоит упомянуть ошибки, связанные с жесткими дисками, временные файлы (TMP), конфликтующие с установкой, а также попытки установить антивирусное ПО во время работы других программных средств. Чтобы минимизировать возможные последствия распространенных ошибок при установке, попробуйте выполнить следующие действия.

Выполните очистку диска

Неисправности диска вполне могут воспрепятствовать успешной установке новых программ. Если с момента последнего применения стандартных диагностических средств уже прошло некоторое время, воспользуйтесь утилитами Disk Cleanup и Disk Defragmenter. Они помогут очистить пространство и реорганизовать файлы на вашем жестком диске:

1. Последовательно выберите **Start** (Пуск), **Programs** (Программы), **Accessories** (Стандартные), **System Tools** (Системные), **Disk Cleanup** (Очистка диска).
2. Укажите нужный диск. Windows 2000 выполнит расчет пространства, которое можно освободить (рис. 19.2).
3. Выберите компонент(ы) для очистки с помощью соответствующих флажков.
4. Windows перейдет к стиранию выбранных файлов. В зависимости от размера вашего жесткого диска, очистка может занять несколько минут.
5. По окончании всех операций диалоговое окно **Disk Cleanup** закроется автоматически.
6. Последовательно выберите **Start** (Пуск), **Programs** (Программы), **Accessories** (Стандартные), **System Tools** (Служебные), **Disk Defragmenter** (Дефрагментация диска).
7. Нажмите кнопку **Analyze** (Анализ). Через несколько мгновений на экране появится подробный отчет о диске (рис. 19.3), содержащий рекомендации о целесообразности его дефрагментации. Ознакомившись с отчетом, закройте его.
8. После закрытия отчета на экране появится графическое представление диска (рис. 19.4).

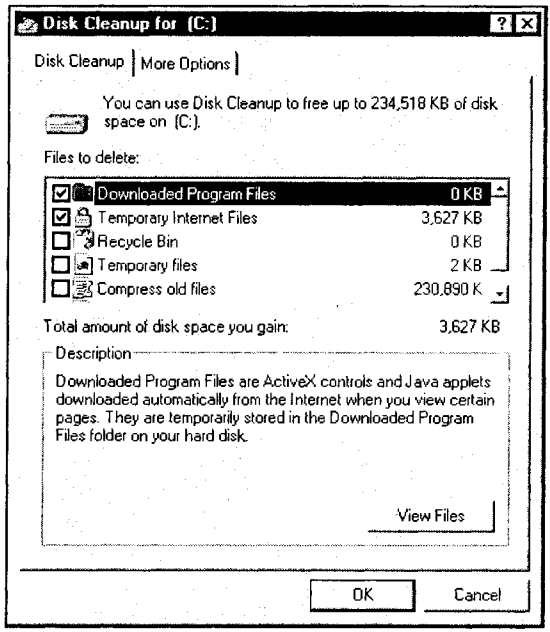


Рис. 19.2. Утилита Disk Cleanup операционной системы Windows 2000 позволяет увеличить свободное пространство на жестком диске

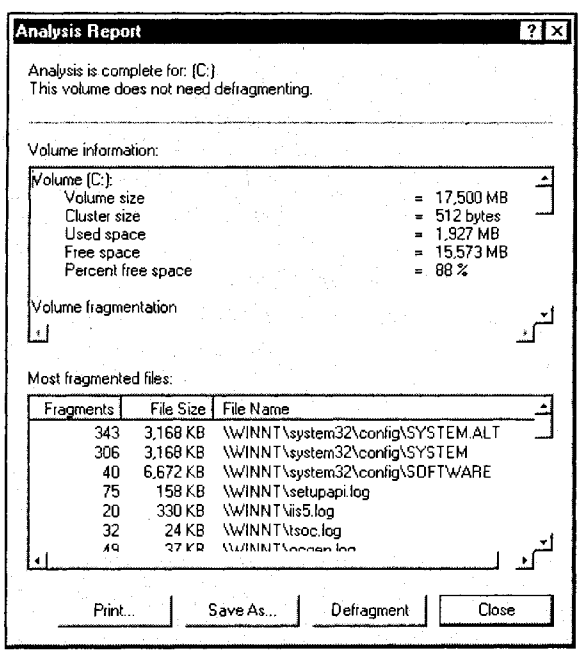


Рис. 19.3. Windows 2000 создает подробный отчет о применении диска и его дефрагментации

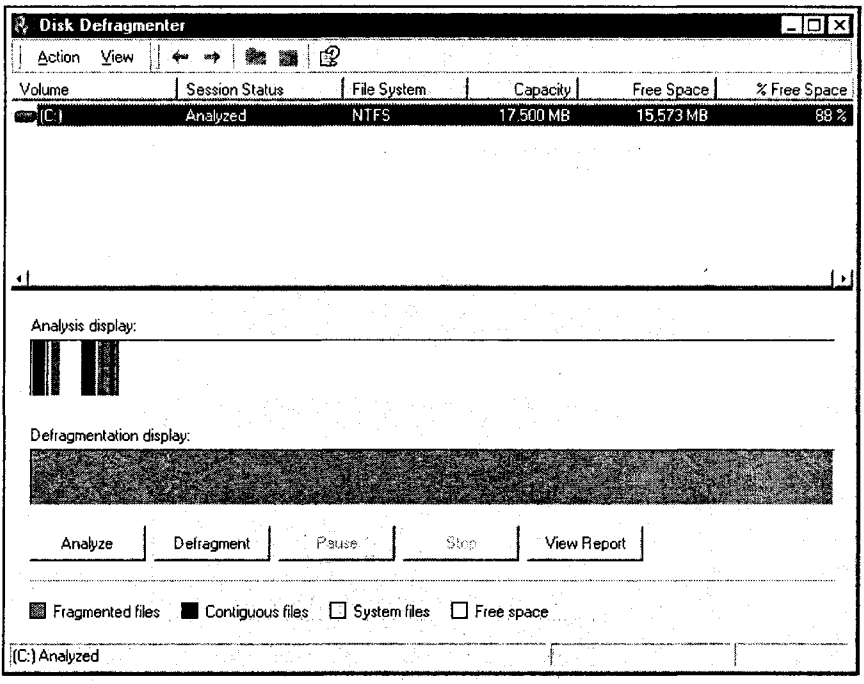


Рис. 19.4. В Windows 2000 у вас есть возможность просмотреть графическое представление дефрагментации диска

9. При необходимости дефрагментации диска нажмите кнопку **Defragment** (Дефрагментация). В зависимости от скоростных характеристик вашего компьютера и размера жесткого диска для завершения этой операции может потребоваться несколько минут.
10. По завершении дефрагментации диска закройте диалоговое окно **Disk Defragmenter**.

Закройте прочее программное обеспечение

Мешать работе программы установки антивирусных средств может и другое программное обеспечение, работающее на вашем сервере или клиентском компьютере в фоновом режиме. Прежде чем повторно пытаться установить ПО, закройте все ненужные программы.

1. Нажмите сочетание клавиш <Ctrl>+<Alt>+<Del>. В результате появится диалоговое окно **Windows Security** (Безопасность Windows). Нажмите кнопку **Task Manager** (Диспетчер задач) (рис. 19.5).
2. Выбирайте ненужные элементы списка и по отношению к каждому из них нажимайте кнопку **End Task** (Завершить задачу).
3. Повторите шаги 2 и 3 вплоть до закрытия всех неиспользуемых программ.
4. Закрыв все ненужные приложения, закройте **Task Manager** и попробуйте установить антивирусную программу еще раз.

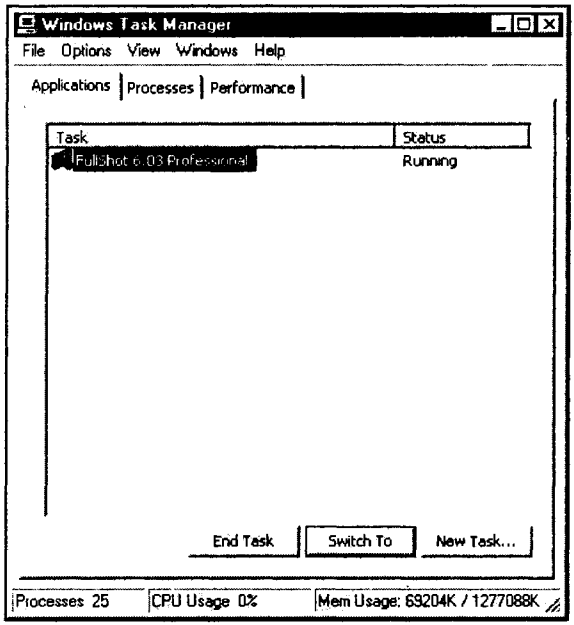


Рис. 19.5. Task Manager операционной системы Windows 2000 позволяет вам закрывать активные процессы, чтобы изолировать приложения тогда, когда они могут помешать установке антивирусных средств или их операциям

Защита от вирусов в макросах

Макровирусы обнаруживаются большинством современных антивирусных средств (причем операцию поиска макровирусов по документам следует проводить регулярно), но, возможно, вам удастся снизить риск последствий деятельности макровирусов, если вы последуете следующим рекомендациям.

- Пометьте файл шаблона NORMAL.DOT как годный "только для чтения". Как правило, это поможет предохранить NORMAL.DOT от инфекций.
- Пользуйтесь редактором Microsoft Word 7.0a или более поздней версии. В этих версиях при попытке открыть файл, содержащий макрос или специальную информацию о настройке, появляется окно предупреждения **Alert**. У вас также появляется возможность отключить неизвестные макросы еще до того, как они начнут действовать.

Удаление макровируса

Вполне возможно, что вы сталкивались с предупреждениями о макровирусах в одном или нескольких документах Microsoft Word или Excel. Возможно также, что вы пытались восстановить эти документы с помощью антивирусной программы, но вам это не удалось; в таком случае вы можете попробовать удалить макровирус вручную. В ходе выполнения представленных ниже шагов должно произойти удаление вирусов из существующих документов; эти действия следует понимать только как сред-

ство аварийного восстановления. Если вирус, создающий инфицированный макрос, все еще присутствует в вашей системе или сети, при следующем открытии зараженного документа произойдет его повторное инфицирование. Как правило, следует избегать применения макросов в приложениях типа Word, Excel или PowerPoint (если это возможно). Ни в коем случае нельзя разрешать автоматическое открытие/исполнение макросов. Чтобы вручную удалить макровирус из документа и восстановить исходный текст, выполните следующие действия.

Примечание

Прежде чем продолжать, создайте резервную копию подозрительных документов и сохраните ее на явно маркированном носителе типа гибкого диска.

1. Последовательно выберите **Start** (Пуск), **Find** (Найти), **Files or Folders** (Файлы и папки). В результате появится диалоговое окно **Find**.
2. Введите NORMAL.DOT и нажмите кнопку **Find Now** (Найти).
3. Когда этот файл будет найден, щелкните на его имени правой кнопкой мыши и в появившемся меню быстрого вызова выберите пункт **Rename** (Переименовать).
4. Переименуйте файл в NORMAL.OLD и нажмите клавишу <Enter>.
5. Закройте диалоговое окно **Find**.
6. Запустите программу Word. Она воссоздаст шаблон NORMAL.DOT.
7. Выберите **File** (Файл), а затем **Open** (Открыть).
8. Найдите каталог, в котором содержится инфицированный файл, и выделите его.
9. Удерживая клавишу <Shift>, нажмите кнопку **Open**. Продолжайте удерживать <Shift> до тех пор, пока зараженный файл не откроется в Word (удерживание клавиши <Shift> во время открытия файла предотвращает запуск макросов).
10. Последовательно выберите **Tools** (Сервис), **Macro** (Макрос), **Macros** (Макросы).
11. В окне списка **Macros In** (Макросы из) выберите пункт **All active templates and documents** (Активных шаблонов).
12. Выберите подозрительный макрос и нажмите кнопку **Delete** (Удалить). Чтобы подтвердить удаление, нажмите кнопку **Yes**.
13. Повторите предыдущий шаг по отношению ко всем подозрительным макросам.
14. Нажмите кнопку **Close** (Закрыть).
15. Выберите **Edit** (Правка), а затем **Select All** (Выделить все).
16. Чтобы снять выделение с последнего в документе символа конца абзаца, нажмите сочетание клавиш <Shift>+<Left Arrow>.
17. Выберите **Edit** (Правка), а затем **Copy** (Копировать).
18. Выберите **File** (Файл), **New** (Создать). Укажите нужный шаблон и нажмите кнопку **OK**.
19. Выберите **Edit** (Правка), **Paste** (Вставить).
20. Чтобы убедиться в том, что инфицированный макрос не воспроизвелся, повторите действия, указанные в шагах 10—14.

21. Сохраните документ.
22. Повторите все приведенные действия по отношению ко всем документам, которые, как вам кажется, могут содержать макровирусы.

Симптомы неисправностей

После того как вы установили антивирусное программное обеспечение, и оно начало работу, его работа на серверах и клиентских компьютерах должна проходить без всяких сбоев. Впрочем, иногда они возникают. В этой части главы речь пойдет о том, что делать с наиболее распространенными типами неисправностей.

Симптом 19.1. Невозможно одновременно запустить несколько антивирусных программ

Эта проблема встречается довольно часто, причем обычно она возникает тогда, когда средства защиты от вирусов, расположенные в памяти, начинают конфликтовать с файл-ориентированными антивирусными средствами. При попытке запустить несколько антивирусных программ всегда присутствует риск странных результатов и ложных аварийных сигналов. Например, некоторые антивирусные программы хранят свои строки образов вирусов в памяти в незащищенном виде. При этом запуск несовместимых или конфликтующих антивирусных средств может привести к интерпретации других строк образов или активности в памяти как вирусов. Одновременно следует запускать лишь одну антивирусную программу.

Симптом 19.2. Ваше антивирусное средство не работает или приводит к некорректной работе других драйверов

Некоторые резидентные программы (Terminate-and-Stay-Resident software, TSR) могут конфликтовать с антивирусными программами, особенно если последние тоже являются резидентными. В случае возникновения подобных сбоев вы можете попытаться загрузить систему с чистого загрузочного диска таким образом, чтобы в ней не осталось никаких драйверов и резидентных программ, кроме антивирусной.

Симптом 19.3. Вы замечаете, что антивирусная программа значительно замедляет операции обращения к диску или при работе в Windows блокируется

Обычно многие антивирусные средства (в особенности резидентные) действительно в некоторой степени замедляют операции доступа к диску. Если же производительность диска снижается очень сильно, или во время работы антивирусная программа приостанавливается, вполне возможно, что с ней конфликтует кэш диска. Попробуйте увеличить количество буферов с помощью файла CONFIG.SYS. Если неисправность сохранится, попытайтесь запустить антивирусное средство и во время его работы отключить программное обеспечение обмена с диском через кэш. В других случаях устранить неисправность, вероятно, поможет получение заплаты или обновления от производителя антивирусной программы.

Симптом 19.4. Антивирусная программа выдает ложные аварийные сигналы

Ложные аварийные сигналы генерируются антивирусными программами довольно часто. Как правило, это происходит из-за конфликтов с другим работающим в сис-

теме резидентным ПО. Попробуйте запустить программу с чистого загрузочного диска. Характер методик обнаружения вирусов также играет свою роль при появлении ложных сообщений об ошибках. Например, типичной методикой обнаружения вирусов является сравнение файлов, но файлы могут видоизменяться по многим причинам, а не только вследствие появления вирусов. Таким образом, вероятность ложных аварийных сигналов довольно велика. Погрешности, которые могут приводить к ложным аварийным сигналам, характерны и для других методик. Попытайтесь получить от производителя вашего антивирусного пакета обновленную базу данных образов вирусов.

Симптом 19.5. Вам не удается удалить резидентную антивирусную программу

Возможно, в системе работает другая резидентная программа или фоновое приложение, конфликтующее с антивирусным средством. Вероятно, для того чтобы очистить антивирусную программу, вам придется перезагрузить систему. В будущем старайтесь загружать антивирусное программное обеспечение в последнюю очередь, после загрузки всех прочих драйверов, резидентных программ или фоновых приложений.

Симптом 19.6. Механизм поиска вирусов выполняет операции поиска очень медленно

Как правило, такие неисправности возникают с некоторыми устаревшими антивирусными программами. В идеале, у вас должна быть возможность устранить эту неисправность путем обновления механизма поиска вирусов до новейшей заплаты или версии. Если латание или обновление программы невозможно, попробуйте проводить поиск только по программным файлам (Program Files), но не по всем (All Files) и не по сжатым (Compressed Files) файлам.

Симптом 19.7. Во время проведения операций поиска механизм поиска вирусов конфликтует с загрузочным сектором

Если механизм поиска вирусов конфликтует с вашим загрузочным сектором (либо во время, либо после инсталляции), попробуйте выбрать функцию специальной установки ("Custom Setup") и отключить первоначальный анализ системы, проходящий во время инсталляции. Затем скорректируйте настройки механизма поиска таким образом, чтобы он пропускал операцию поиска при загрузке. Например, если вы пользуетесь антивирусной программой McAfee VirusScan, отредактируйте файл DEFAULT.VSC, заменив значение `bSkipBootScan=0` в секции `[Scan Options]` на `bSkipBootScan=1`. В результате при запуске VirusScan операция поиска в загрузочном секторе будет пропускаться. Следовательно, проверка загрузочного сектора на наличие в нем вирусов проводиться не будет.

Симптом 19.8. При установке антивирусной программы на сервер NetWare 4.x вы сталкиваетесь с ошибками NDS

Например, если вы устанавливаете продукт типа Norton AntiVirus Corporate Edition на сервер NetWare 4.x с устаревшей версией файла clib.nlm, на экране появляются следующие сообщения об ошибках:

```
Error importing NWDSCreateContextHandle
Error (0xa0000014)(-1610612716) initializing DS in DS Preliminaries Error
```

```
Error: 0xa0000014(-1610612716) in line 255: [DSPROFILE] Error
Error: Not authenticated with Novell Directory Services in line 278:
[DSOBJECTS]
```

Установите последнюю версию файла clib.nlm от Novell. Этот файл присутствует в последней заплате обновления NetWare (имеется в виду LIBUPF или более новая версия), которую можно загрузить с Web-сайта поддержки продуктов Novell по адресу **support.novell.com**. Чтобы устранить данную неисправность, установите эту заплату на сервере NetWare 4.x, а затем проведите повторную инсталляцию антивирусного программного обеспечения.

Симптом 19.9. Вы сталкиваетесь с ошибкой "свертывание постороннего процесса"

В антивирусных продуктах типа Norton AntiVirus Corporate Edition эта ошибка обозначается как 0x20000046E. Как правило, она появляется в том случае, если вы проводите установку антивирусного программного обеспечения с использованием метода, не предусмотренного для данного продукта. Обычно это происходит при попытке запуска ручной или регулярной операции поиска. Возможно, вам придется предоставить антивирусной программе возможность взаимодействия с рабочим столом (для этого зайдите в Norton AntiVirus Service и проверьте, установлен ли флажок, разрешающий взаимодействие с рабочим столом). Вы также можете полностью удалить антивирусное программное обеспечение, а затем провести его повторную установку в соответствии с инструкциями производителя.

Симптом 19.10. Вы сталкиваетесь с ошибкой невозможности загрузить <имя_файла>

Например, после установки Norton AntiVirus может появиться ошибка, в соответствии с которой "загрузить listview.ocx невозможно". Это означает, что в ходе процесса инсталляции один или несколько файлов не были зарегистрированы. Что касается этой ошибки, встречающейся в Norton AntiVirus, среди незарегистрированных файлов могут числиться clntcon.ocx, srvcon.ocx или ldvpocx.ocx. Такая ситуация могла сложиться, если при выходе из программы установки (Setup) процесс инсталляции был еще не завершен, или если в каталоге, из которого выполнялась установка антивирусной программы, отсутствует какой-нибудь важный файл DLL (например, transman.dll). Обычно наилучшее решение заключается в удалении антивирусного программного обеспечения с его последующей повторной установкой.

Симптом 19.11. После установки антивирусной программы вы сталкиваетесь с трудностями при запуске системы

Например, в клиентских системах Windows на пиктограмме антивирусной программы в меню системы присутствует желтый восклицательный знак. Этот знак появляется после перезагрузки в условиях, когда защита в реальном времени не включена. На компьютерах с Windows может появляться сообщение об ошибке типа следующего:

```
RTVSCN95 caused a General Protection Fault in module krnl386.exe
```

Подобные неисправности, как правило, обусловлены конфликтом синхронизации между антивирусным программным обеспечением (например, Norton AntiVirus Cor-

porate Edition) и другим приложением или службой, загрузка которой происходит при запуске системы. Чтобы устранить эту неисправность на компьютерах Windows NT/2000, измените последовательность загрузки службы Norton AntiVirus Corporate Edition Client путем создания зависимости от другой службы.

Примечание

За инструкциями по созданию зависимости обращайтесь к статье Q193888 базы знаний Microsoft (Microsoft Knowledge Base).

Симптом 19.12. После установки антивирусной программы вы сталкиваетесь с трудностями при отключении системы

Например, при попытке отключить систему или перезагрузить компьютер, на котором установлено антивирусное программное обеспечение, он может перестать отвечать или вывести следующее сообщение об ошибке:

```
The application cannot respond to the End Task request.
```

Некоторые антивирусные средства (в том числе Norton AntiVirus Corporate Edition) проводят поиск по диску A: во время перезапуска или закрытия системы, тем самым предохраняя компьютер от инфицирования от загрузочного вируса. На некоторых компьютерах флоппи-дисковод выступает источником появления сбоев, связанных с синхронизацией при отключении системы. Чтобы устранить эти трудности, вам придется внести изменения в реестр. Начните с создания его резервной копии.

Примечание

Перед внесением любых изменений в системный реестр его необходимо резервировать. Неверное редактирование реестра может привести к невосстановимым потерям данных или к повреждению файлов. Вносите изменения только в указанные ключи.

1. Выберите **Start** (Пуск).
2. Выберите **Run** (Выполнить). В результате появится диалоговое окно **Run**.
3. Введите `Regedit` и нажмите кнопку **OK**. В результате откроется программа Registry Editor (Редактор реестра).
4. Зайдите в меню **Registry** (Реестр) и выберите пункт **Export Registry File** (Экспортировать файл реестра).
5. Убедитесь в наличии в диалоговом окне **Export Registry File** следующих настроек:
   - **Save in** (Сохранить в): Desktop (Рабочий стол);
   - **File name** (Имя файла): Backup;
   - **Save as type** (Тип файла): Registration Files (Файл реестра);
   - **Export range** (Диапазон экспорта): All (Весь реестр)
6. Нажмите кнопку **Save** (Сохранить).
7. Выйдите из Registry Editor (Редактор реестра) и проверьте, есть ли на рабочем столе файл реестра Backup.reg.

Теперь приступайте к редактированию реестра; целью этих действий должно быть приостановление операции поиска на гибком диске:

1. Выберите **Start** (Пуск).
2. Выберите **Run** (Выполнить). В результате появится диалоговое окно **Run**.
3. Введите `Regedit` и нажмите кнопку **OK**. В результате откроется Registry Editor (Редактор реестра).
4. Перейдите к следующему подключу:

   `HKEY_LOCAL_MACHINE\Software\Intel\LanDesk\VirusProtect6\CurrentVersion`

5. Щелкните правой кнопкой мыши на правой панели и выберите **New** (Новый), **DWORD Value** (Двойное слово).
6. Назовите значение `Skipshutdownfloppycheck`.
7. Щелкните правой кнопкой мыши на новом значении `Skipshutdownfloppycheck` и выберите **Modify** (Изменить).
8. В текстовом окне **Value Data** (Значение) введите `1`.
9. Чтобы создать новое значение под названием `Skipshutdownscan`, равное `1`, повторите шаги 4—7.
10. Чтобы вновь разрешить поиск на гибком диске при отключении системы, приравняйте значения `Skipchutdownfloppycheck` и `Skipshutdownscan` к нулю.
11. Чтобы сохранить изменения, выберите пункт **Exit** (Выход) меню **Registry** (Реестр).

Симптом 19.13. После обновления 16-битовый клиент дважды упоминается в управляющем программном обеспечении

После обновления 16-битового клиента антивирусного ПО первоначально в антивирусной управляющей программе (например, Symantec System Center) вы видите две копии одного и того же клиентского компьютера. Дело в том, что в перечне клиентов сервера антивирусной программы старый клиент все еще присутствует. После того как сервер обновляет свой перечень клиентов, он удаляет старую копию 16-битового клиента антивирусной программы. Впоследствии в управляющем программном обеспечении выводится только обновленный 16-битовый клиент.

Симптом 19.14. Вы сталкиваетесь с трудностями при загрузке антивирусного программного обеспечения для NetWare

Например, в ходе загрузки Norton AntiVirus Corporate Edition для NetWare вы можете столкнуться со следующим сообщением об ошибке:

```
RTVSCAN could not load NDS function.
```

Ошибка этого типа обычно возникает вследствие программной несовместимости. В случае с Norton AntiVirus вполне возможно, что вы пользуетесь устаревшим файлом dsapi.nlm. Этот файл следует обновить. Загрузите его новейшую версию с сайта Novell по адресу **www.novell.com** и проведите повторную инсталляцию антивирусного ПО (например, Norton AntiVirus Corporate Edition).

Возможно, для выявления устаревших загружаемых модулей NetWare вы захотите воспользоваться утилитой Config Reader. Она берет входные данные из файла CONFIG.TXT и представляет их таким образом, что у вас появляется больше возможностей для анализа, чем если бы вы просматривали его с помощью текстового редактора. Config Reader можно скачать с Web-сайта Novell.

Дополнительные ресурсы

Command Worldwide: **www.commandcom.com**.

EICAR: **www.eicar.org**.

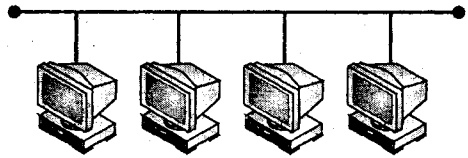
IBM: **www.research.ibm.com/antivirus/**.

McAfee: **www.mcafee.com** или **www.networkassociates.com**.

NCSA (TrueSecure): **www.truesecure.com**.

Dr. Solomon: **www.drsolomon.com**.

Symantec: **www.symantec.com/avcenter/**.



ГЛАВА 20

Резервирование и восстановление данных в сети

Нередко сбои в работе сети и потеря данных происходят неожиданно. Технический специалист может без особых проблем заменить неисправные компоненты и поврежденный кабель, но восстановить потерянные данные практически невозможно. Их нужно создавать заново. Ни одна компания лишилась прибыли (и даже вышла из бизнеса), потеряв важные данные. К уничтожению данных могут привести разнообразные естественные и искусственные факторы, среди которых можно выделить следующие:

- неисправность компонентов (например, сетевого адаптера);
- компьютерные вирусы (появившиеся в ходе передачи файлов или применения инфицированных приложений);
- удаление и повреждение данных (например, вредительство со стороны сотрудника);
- пожары, происходящие в результате поджогов или аварий в системе электроснабжения;
- стихийные бедствия (в том числе грозовые разряды, наводнения, смерчи и землетрясения);
- сбои в подаче электропитания и скачки напряжения;
- воровство и вандализм.

Методики создания, подтверждения и восстановления резервных копий являются неотъемлемыми составляющими процесса обслуживания сети. Простейшим и наименее дорогим способом избежать потери данных является организация расписания периодических операций по резервированию (которые предпочтительнее проводить с помощью внесетевых устройств хранения). Резервирование на магнитной ленте (рис. 20.1) представляет собой простой и экономичный способ обеспечения сохранности и возможности применения сетевых данных. Надежная стратегия резервирования минимизирует риск потери данных и предусматривает выполнение операций по текущему резервированию (т. е. создание копий существующих файлов). Таким образом, в случае потери или повреждения исходных данных операционные системы, приложения и файлы данных можно восстановить. В этой главе будут рассмотрены принципы и практические методы хранения резервных данных на магнитных лентах, а также ряд общих вопросов, связанных с поиском неисправностей.

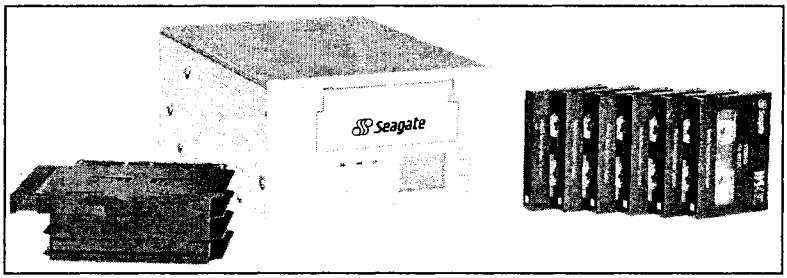


Рис. 20.1. Накопитель на магнитной ленте Seagate 240 DAT (публикуется с разрешения Seagate)

Основы записи на магнитной ленте

Когда нужно проводить резервирование? Однозначного ответа на этот вопрос не существует, потому что ситуация в каждой сети уникальна. При построении графика резервирования рекомендуется следовать простому правилу: если вы не можете без чего-то обойтись, зарезервируйте это. Критические данные можно резервировать каждый день, каждую неделю или каждый месяц. Это зависит от того, насколько важны данные и как часто они обновляются. Лучше всего планировать операции резервирования в периоды низкого уровня использования систем (например, поздним вечером или в выходные). Во время выполнения резервирования об этом следует оповещать пользователей, чтобы в этот период они не обращались к серверу.

Будете ли вы резервировать целые диски, отдельные каталоги или файлы, зависит от того, насколько быстро вы сможете восстановить работу после потери важных данных. Полное резервирование делает задачу восстановления конфигурации диска намного проще, поскольку все данные восстанавливаются единовременно, но при этом может потребоваться несколько кассет (в особенности если речь идет о больших объемах данных). Резервирование отдельных файлов и каталогов обычно проходит быстрее и требует меньшего количества кассет, но зато в таком случае вам, вероятно, придется проводить восстановление конфигурации дисков вручную. В идеале, емкости накопителя на магнитной ленте должно быть достаточно для резервирования крупнейшего из всех серверов сети. Он также должен поддерживать обнаружение ошибок и их устранение во время операций резервирования и восстановления.

Методы резервирования

Единого способа резервирования данных сервера не существует. Вы можете выбрать одну из нескольких распространенных методик резервирования, причем большинство администраторов предпочитают использовать их сочетания.

- *Полное резервирование.* Полное резервирование применяется для сохранения и маркировки определенных файлов вне зависимости от того, были ли они изменены со времени последней подобной операции. В результате обеспечивается наиболее полная и удобная защита данных, но реализация этой методики занимает больше времени.

- *Копирование.* При копировании все выбранные файлы резервируются, но не маркируются как зарезервированные.
- *Добавочное резервирование.* В ходе выполнения этого процесса выбранные файлы сохраняются и маркируются лишь в том случае, если они были изменены с момента предыдущего их резервирования.
- *Ежедневное копирование.* Это вариант копирования, при котором сохраняются лишь те файлы, которые были изменены в течение текущего дня; при этом они не маркируются как зарезервированные.
- *Разностное резервирование.* В ходе этого процесса выбранные файлы сохраняются лишь в том случае, если они были изменены с момента последнего резервирования; при этом они не маркируются как зарезервированные.

Например, вы можете выбрать следующую схему: начать цикл резервирования в понедельник с выполнения полного резервирования, потом каждый день вплоть до конца недели производить добавочное резервирование (для сохранения измененных за это время файлов), а затем, в следующий понедельник, запустить этот цикл с самого начала. Естественно, реальная частота проведения операций резервирования будет зависеть от потребностей вашей сети. Большинство стратегий резервирования предусматривают использование большого количества кассет при условии их регулярной ротации.

Резервные копии абсолютно бесполезны, если с их помощью нельзя провести восстановление. Любой опытный технический специалист посоветует вам тестировать (подтверждать) резервные копии. Администраторы сетей периодически проводят испытания аварийного восстановления, создавая резервные копии, удаляя файлы, восстанавливая данные и затем, пытаясь ими воспользоваться. Во многих случаях эти испытания проводятся менее опытными техниками (под наблюдением администратора), которые тем самым укрепляют свои навыки восстановления. Такие испытания проводятся для того, чтобы подтвердить факт резервирования необходимых данных, а также наличие отработанной процедуры восстановления.

Вне зависимости от того, какой план резервирования вы примете на вооружение, не экономьте на качестве кассет. Срок повторного использования кассет ничем не ограничен, так что выбор качественной кассеты, рекомендованной для применения на вашем накопителе, поможет вам достичь наилучших результатов сохранения данных на наиболее длительный период времени.

Добавочное и разностное резервирование

На полное резервирование и последующее восстановление уходит наибольшее количество времени, но эта процедура способна привести вашу систему в то состояние, в котором она пребывала в момент выполнения резервирования (вам не придется тратить время на повторную настройку аппаратной части и установку отдельных приложений). При добавочном и разностном резервировании сохраняются только те файлы, которые были изменены со времени предыдущего резервирования. Впрочем, при добавочном резервировании измененные файлы маркируются, а при разностном нет. Это означает, что со временем разностные резервные копии увеличиваются в объеме, т. к. в них постоянно включаются все файлы, измененные с момента последней процедуры полного резервирования. При проведении добавочного и разностного резервирования задействуется меньшее количество файлов, создание соответ-

ствующих резервных копий и последующее восстановление обычно занимает меньше времени, но зато эти операции не распространяются на всю систему.

На практике все, как правило, начинается с проведения полного резервирования системы; после этого, в ходе изменений, происходящих с системой и ее данными, периодически проводятся операции добавочного резервирования. При использовании такой схемы сначала восстанавливается полная резервная копия, а затем в нее интегрируются все добавочные резервные копии до тех пор, пока система не восстановит свое последнее состояние. Впрочем, восстановление большого количества добавочных резервных копий может занять много времени. Если вы предпочитаете проводить разностное резервирование, то сначала вам придется восстановить полную резервную копию, а затем последнюю разностную копию, т. к. она будет включать все файлы, измененные с момента проведения последнего полного резервирования. Поэтому если дело касается сравнительно небольшого количества файлов, разностное резервирование, вероятно, оказывается эффективнее добавочного.

Рассмотрим пример. Предположим, что вы выполняете полное резервирование системы, а после этого всю неделю работаете с файлом *A*. При проведении добавочного резервирования будет сохранен только файл *A*. Если далее вы будете работать с файлом *B*, то при выполнении следующего добавочного резервирования будет сохранен только файл *B*. Если возникнет необходимость в восстановлении системы, то сначала вы восстановите из полной резервной копии, затем — добавочной резервной копии с файлом *A*, добавочной резервной копии с файлом *B* и т. д. Если же, работая с файлом *A*, вы выполните разностное резервирование, сохранен будет только он, но когда вы завершите работу с файлом *B* и проведете еще одну операцию разностного резервирования, сохранены будут оба файла: как *A*, так и *B*. При восстановлении системы вы воспользуетесь полной резервной копией и последней разностной резервной копией, потому что в ней будут сохранены все файлы, измененные с момента последнего полного резервирования. Операции разностного резервирования экономят ваше время в процессе восстановления.

Журналы резервирования

Процедуры резервирования также следует регистрировать (либо в виде отдельной записи, либо как часть журнала сопровождения сервера). Полная запись резервирования может оказаться важной при последующем проведении восстановления данных; в ней должна фиксироваться следующая информация:

- дата резервирования;
- номер набора кассет (или другой идентификатор);
- тип выполненной операции резервирования (полная, добавочная и т. д.);
- компьютер/сервер, по отношению к которому была проведена операция резервирования;
- диски/файлы, по отношению к которым была проведена операция резервирования;
- имя человека, выполнившего резервирование;
- физическое местоположение зарезервированных лент (если они хранятся вне рабочего места).

Методы чередования кассет

Естественно, кассеты являются наиболее распространенными носителями из тех, что применяются в системах сетевого резервирования. Количество операций резервирования, которые вы будете производить за неделю или за месяц, зависит от степени активности в вашей системе или сети, но при этом целостность резервных копий ограничена возможностями кассетами. Если при реализации режима резервирования вы будете пользоваться несколькими кассетами, вам не придется писать новые данные поверх текущей резервной копии (что в случае прерывания процесса может привести к аварийной ситуации). *Чередование кассет* — это распространенная методика, помогающая обеспечить защищенность и целостность данных в любое время.

Примечание

Существует множество рациональных способов чередования кассет. В этом разделе будут рассматриваться лишь некоторые распространенные методы.

Две кассеты

Как правило, это вариант считается базовым. Он идеально подходит для отдельных пользователей, а также для тех, кто не так часто работает на компьютере. Обычно используется две разновидности этой методики. Чаще всего реализуется вариант создания полных резервных копий (с их постоянным чередованием). Например, переформатирование кассеты *A* и резервирование на ней выполняется 1 марта, а аналогичные операции с кассетой *B* проводятся 1 апреля; после этого кассета *A* переформатируется и применяется для создания полной резервной копии 1 мая и т. д. Этот метод гарантирует отсутствие необходимости в перезаписи данных поверх текущей резервной копии. Альтернативная методика предполагает создание полной резервной копии на кассете *A*, а затем, в случае необходимости, резервирование изменений на кассете *B*.

Три кассеты

Трехкассетный цикл часто применяется в небольших офисах или в домашних условиях, т. е. в тех случаях, когда каждый день изменения вносятся в небольшое количество файлов. Понять смысл этой методики проще, если рассмотреть период длительностью в одну неделю. В понедельник делается полная резервная копия на кассете *A*. Со вторника по пятницу выполняется резервирование изменений (т. е. создаются добавочные резервные копии) на кассете *B*. На следующей неделе создается полная резервная копия на кассете *C*, а кассета *A* в это время помещается на безопасное хранение вне рабочего места. Тогда же происходит стирание или переформатирование кассеты *B*, и на протяжении всей недели она применяется для резервирования изменений. В понедельник следующей недели кассета *C* помещается на хранение в безопасное место вне рабочего пространства, а кассета *A* извлекается из него с целью ее последующего стирания или переформатирования для проведения очередной операции полного резервирования. Таким образом, кассеты *A* и *C*, применяемые для создания полных резервных копий, чередуются каждую неделю, а кассета *B* хранится на рабочем месте для выполнения ежедневного резервирования изменений.

Если уровень использования вашей системы не оправдывает ежедневное сохранение данных, попробуйте проводить резервирование раз в неделю. Первого числа данного месяца записывайте полную резервную копию на кассету *A*, а затем, каждую неделю в течение всего последующего месяца (или в любое другое время при необходимости защиты новых файлов), пользуйтесь кассетой *B* для выполнения резервирования изменений. Первого числа следующего месяца запишите полную резервную копию на кассету *C* и поместите кассету *A* на безопасное хранение вне рабочего места. Сотрите содержимое кассеты *B* и проводите с ее помощью операции добавочного резервирования на протяжении всего последующего месяца. Первого числа третьего месяца переместите кассету *C* на хранение вне рабочего места, сотрите содержимое кассеты *A*, выполните операцию полного резервирования, а затем сотрите кассету *B* и применяйте ее для резервирования изменений. Таким образом, чередование кассет *A* и *C* производится первого числа каждого месяца, а не в первый день каждой недели.

Шесть кассет

Схема чередования шести кассет предназначена для предприятий и офисов с оживленной деятельностью, в которых редактирование и обновление важных файлов производится каждый день. Начните неделю со стирания или переформатирования кассет *A* и *F*; после этого создайте полные резервные копии на обеих кассетах. Поместите кассету *F* на безопасное хранение вне рабочего места. С помощью кассет *B*, *C*, *D* и *E* выполняйте резервирование изменений (добавочное резервирование) со вторника по пятницу. В понедельник следующей недели кассеты *A* и *F* следует стереть и создать на них полные резервные копии еще раз. На протяжении всей недели кассета, предназначенная для применения в определенный день, будет стираться и заполняться добавочной резервной копией.

Десять кассет

При необходимости еженедельного и ежемесячного сопровождения внесистемных архивов вы можете реализовать десятикассетный цикл чередования (который, на самом деле, представляет собой модификацию шестикассетного цикла). Путем прибавления к шестикассетному циклу еще четырех кассет у вас появляется возможность создания полных резервных копий в первый день каждой недели с их последующим безопасным хранением вне рабочего пространства. Например, предположим, что в первый понедельник месяца создаются полные резервные копии на кассетах *A* и *F* (как и в шестикассетной схеме), причем кассета *F* помещается на хранение вне рабочего места. Со вторника по четверг для формирования добавочных резервных копий за каждый день применяются кассеты *B*, *C*, *D* и *E*. Кассета *F* становится архивом недели 1. На следующей неделе полные резервные копии создаются на кассетах *A* и *G*, в то время как кассеты *B*, *C*, *D* и *E* используются для резервирования изменений. Кассета *G* становится архивом за неделю 2. На третьей неделе полные резервные копии сохраняются на кассетах *A* и *H*; архивом этой недели становится кассета *H*. На кассеты *A* и *I* помещаются полные резервные копии за четвертую неделю, причем функцию ее архива выполняет кассета *I*. Наконец, кассета *J* применяется для создания полной резервной копии в последний день месяца. Для многих предприятий этот процесс представляется избыточным, но в отношении организаций, в которых ставится требование долговременного архивирования (такими организациями, например, могут быть государственные подрядчики), он может оказаться очень полезным.

Установка накопителей на магнитной ленте

Установка накопителя на магнитной ленте, как правило, не представляет трудностей; обычно она сводится к простому монтажу самого устройства, проводке кабеля к свободному адаптеру SCSI (иногда — IDE) и подключению питания. После установки при включении питания дисковод выполняет операцию самотестирования; затем вы должны установить подходящие драйверы и необходимые программы резервирования. В этой части главы рассматриваются принципы установки аппаратного и программного обеспечения.

Монтаж аппаратуры

Обычно процесс установки аппаратуры подразумевает надежный монтаж и проводку кабеля. Ниже представлены этапы монтажа встроенного накопителя на магнитной ленте.

Примечание

Эти этапы представляют собой лишь общее руководство. При настройке и установке накопителя на магнитной ленте вы в любом случае должны следовать инструкциям его производителя.

1. Распакуйте накопитель на магнитной ленте и подготовьте его для применения на вашем сервере. Для этого нужно провести конфигурирование его идентификатора SCSI, выполнить настройки четности SCSI (четность или нечетность), а также контроль по четности (включен или отключен). Убедитесь в том, что идентификатор SCSI не конфликтует с другими устройствами SCSI в рамках данной системы. Если вы устанавливаете накопитель на магнитной ленте ATAPI IDE, нужно настроить его либо как ведущее (master), либо как ведомое (slave) устройство IDE.
2. Отключите питание сервера, на котором предполагаете монтировать накопитель на магнитной ленте, и отсоедините его от сети электропитания (своевременно предупредите о своих намерениях всех пользователей, чтобы у них была возможность завершить работу с этим сервером). Отключите сервер от остальной сети.
3. Откройте сервер и снимите крышку отсека дисковода, в который собираетесь устанавливать новое устройство. Плавно поместите устройство в отсек и зафиксируйте его четырьмя крепежными винтами. Установка меньшего количества винтов приведет к чрезмерной вибрации устройства.
4. Подключите к накопителю на магнитной ленте сигнальный кабель SCSI (или IDE). Если это устройство SCSI является последним в цепочке SCSI, его кабель SCSI необходимо надежно терминировать.
5. Теперь подключите свободный силовой кабель устройства и убедитесь в том, что он полностью зафиксирован.
6. Выполните тщательную проводку кабелей и убедитесь в том, что они расположены на достаточном расстоянии от вентиляторов или других устройств. Не устанавливайте корпус сервера и не подключайте его к сети, пока не убедитесь в надежности монтажа.

Тестирование при включенном питании

После монтажа накопителя на магнитной ленте вы можете проверить его работу, подключив сервер к источнику питания. Убедитесь в том, что горит светодиод питания, и проконтролируйте появление индикаторных сообщений процедуры POST устройства. В табл. 20.1 приводятся сигналы индикаторов, характерные для типичного накопителя на магнитной ленте.

Таблица 20.1. *Обзор значений светодиодов накопителя на магнитной ленте DLLT2000*

Индикатор	Цвет	Состояние	Рабочее состояние
Write Protected (защита от записи)	Оранжевый	Светится	Кассета защищена от записи
		Не светится	Запись на кассете разрешена
Tape in Use (кассета используется)	Желтый	Мигает	Кассета в работе
		Светится	Кассета загружена и готова к работе
Use Cleaning Tape (воспользуйтесь чистящей кассетой)	Желтый	Светится	Головка накопителя на магнитной ленте нуждается в чистке, или присутствует дефект кассеты. Чистящая кассета предприняла попытку чистки головки устройства, но кассета кончилась, а задача выполнена не была. Неисправная кассета с данными; попробуйте воспользоваться другой кассетой
		Не светится	Операция чистки завершена, или ее проведение не является необходимым
Operate Handle	Зеленый	Светится	Можно вставить/извлечь кассету
		Не светится	Нельзя вставлять/извлекать кассету
Все правосторонние индикаторы	Мигают	—	Произошла ошибка устройства
2.6	Желтый	Светится	Указывает на то, что кассета записана в формате 2.6.
		Мигает	Указывает на то, что кассета записана в другом формате
6.0	Желтый	Светится	Указывает на то, что кассета записана в формате 6.0
		Мигает	Указывает на то, что кассета записана в другом формате.
10.0	Желтый	Сигнализирует (по умолчанию)	Указывает на то, что кассета записана в формате 10.0
		Не светится	Указывает на то, что кассета записана в другом формате

Таблица 20.1 (окончание)

Индикатор	Цвет	Состояние	Рабочее состояние
Compress (сжатие)	Желтый	Светится	Режим сжатия включен
		Не светится	Режим сжатия отключен
Density Override (подмена плотности)	Желтый	Светится	Вы определили плотность с передней панели
		Не светится (по умолчанию)	Плотность будет определена хостом (автоматически)
		Мигает	Вы находитесь в режиме выбора плотности

Например, DLT2000 следует определенной последовательности событий, начиная с правосторонних индикаторов.

1. Индикаторы, расположенные на правой стороне передней панели, начинают работать последовательно (сверху вниз).
2. Все индикаторы сигнализируют в течение примерно 3 секунд.
3. Индикатор Tape in Use (использования ленты) начинает мигать, а затем отключается.

Есть несколько возможных ситуаций.

- Если кассета не вставлена, сигнализирует индикатор Operate Handle совместно со звуковым сигналом.
- Если кассета вставлена, индикатор Tape in Use начинает мигать и останавливается при готовности устройства.
- Если крышка отсека открыта, начинает мигать индикатор Operate Handle, сообщая о необходимости закрытия отсека. Затем мигает индикатор Tape in Use; после этого начинает мигать индикатор Operate Handle, и срабатывает звуковой сигнал.

Если индикаторы накопителя на магнитной ленте реагируют ожидаемым образом, можно предположить, что это устройство установлено и работает корректно. Можно переходить к установке драйверов и тестированию дисковода. Если нормальной подачи питания на устройство не произошло, вы должны проверить надежность монтажа и при необходимости заменить подозрительное устройство.

Установка программного обеспечения

Убедившись в надежности установки и нормальном режиме работы накопителя на магнитной ленте, следует установить программное обеспечение, необходимое для его функционирования. В первую очередь необходимо установить драйверы устройства для того, чтобы Windows NT/2000 (или другая ОС) получила возможность обращаться к этому устройству. Затем вы должны будете установить подходящую утилиту резервирования для организации файлов, расписаний, областей охвата носителей (для нескольких лент) и другие функции. Начнем с установки драйверов.

Загрузка драйверов устройства

Как и в случае с большинством других компьютерных устройств, драйверы необходимы для того, чтобы операционная система могла обращаться к различным компонентам аппаратного обеспечения. Драйверы на сопроводительном компакт-диске накопителя на магнитной ленте нужны в том случае, если вы будете пользоваться собственными программами резервирования для вашей операционной системы. Однако многие коммерческие программы резервирования в полной мере обеспечивают необходимую поддержку драйверов. Ниже приводятся этапы установки типичных драйверов в операционной системе Windows NT.

1. Вставьте компакт-диск накопителя на магнитной ленте в дисковод `x` (где `x` — это имя дисковода CD-ROM).
2. Последовательно выберите **Start** (Пуск), **Settings** (Настройка), **Control Panel** (Панель управления).
3. Двойным щелчком выберите пиктограмму **Tape Devices** (Устройства записи). Если других драйверов накопителей на магнитной ленте в системе не установлено, то после выбора **Tape Devices** в **Control Panel** появится меню **Install Driver** (Установка драйвера). Если же драйвер накопителя на магнитной ленте уже установлен, вы увидите меню **Tape Devices** (Устройства записи). В этом меню нужно перейти на вкладку **Drivers** (Драйверы), а затем, чтобы попасть в меню **Install Driver** (Установка драйвера), нажать кнопку **Add** (Добавить).
4. В меню **Install Driver** (Установка драйвера) выберите **Have Disk** (Есть диск); в результате должно появиться окно **Install from Disk** (Установка с диска).
5. В окне **Copy Manufactures' Files From** (Копировать файлы изготовителя с) выберите имя дисковода CD-ROM.
6. Нажмите кнопку **Browse** (Просмотр); после этого появится окно **Locate File** (Разместите файл).
7. Выберите каталог nt_driver и проверьте, выводится ли объект OEMSETUP.
8. Нажмите кнопку **Open** (Открыть).
9. Теперь должно вновь появиться окно **Install from Disk** (Установка с диска). Скопируйте файлы производителя из каталога `x:\nt_driver` (где `x` — это имя дисковода CD-ROM).
10. Нажмите кнопку **OK**.
11. Появится окно **Install Driver** (Установка драйвера). Нажмите кнопку **OK**.
12. Когда на экран будет выведено окно **New SCSI Tape Device** (Новое SCSI-устройство записи), нажмите кнопку **OK**.
13. Теперь появится окно **Windows NT Setup**.
14. Введите `x:\nt_driver` (где `x` — это имя дисковода CD-ROM).
15. Нажмите кнопку **Continue** (Продолжить); в результате произойдет загрузка драйвера.
16. На экране появится окно **Tape Devices** (Устройства записи). Нажмите кнопку **OK**.
17. Извлеките компакт-диск из привода CD-ROM и перезагрузите систему.

18. После перезагрузки системы последовательно выберите **Start** (Пуск), **Settings** (Настройка), **Control Panel** (Панель управления).
19. Чтобы проверить, произошла ли загрузка драйвера, двойным щелчком выберите пиктограмму **Tape Devices** (Устройства записи).
20. Если драйвер не загрузился, проверьте надежность подключения накопителя на магнитной ленте к системе и при необходимости повторите весь процесс, начиная с шага 1.

Ниже приводятся типичные этапы инсталляции в операционной системе Windows 2000.

1. Включите компьютер и запустите Windows.
2. Щелкните правой кнопкой мыши на пиктограмме **My Computer** (Мой компьютер) и выберите пункт **Manage** (Управление). В результате произойдет запуск программы **Computer Management** (Управление компьютером).
3. В окне программы **Computer Management** (рис. 20.2) выделите **Device Manager** (Диспетчер устройств). В правой части окна будет выведен список соответствующих аппаратных подсистем.

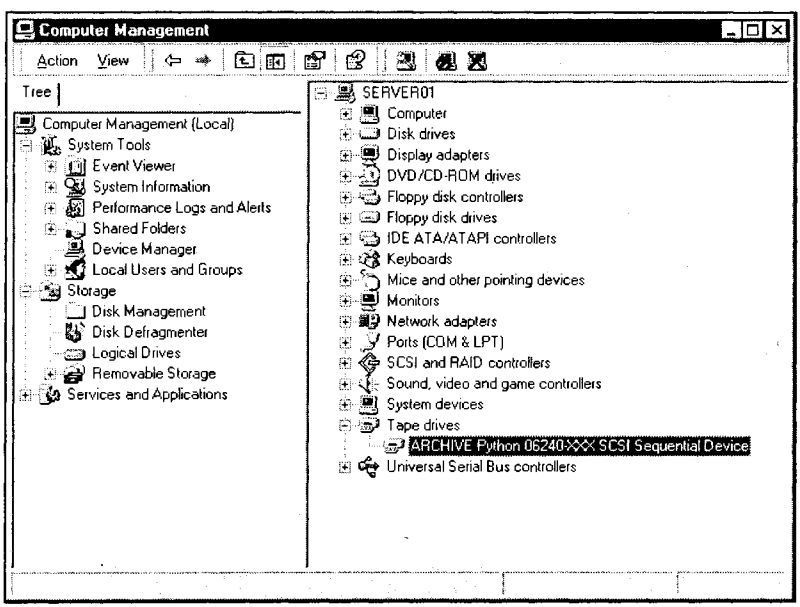


Рис. 20.2. Для идентификации накопителя на магнитной ленте, установленного на вашем персональном компьютере или сервере, воспользуйтесь **Device Manager** (Диспетчер устройств) операционной системы Windows 2000

4. Нужный вам накопитель на магнитной ленте может находиться в разделе **Tape Drives** (Приводы ленточных накопителей) или **Other Devices** (Другие устройства). Откройте тот раздел, в котором он обозначен. Щелкните на накопителе на магнитной ленте правой кнопкой мыши и выберите пункт **Properties** (Свойства).

5. Если Windows 2000 не обнаруживает накопитель на магнитной ленте в разделе **Tape Drivers** (Приводы ленточных накопителей) или **Other Devices** (Другие устройства), вы должны приступить к поиску неисправностей этого устройства. Не продолжайте процесс инсталляции, пока не справитесь с этой проблемой.
6. В окне **Properties** (Свойства) проверьте соответствие указанного в нем идентификатора SCSI идентификатору устанавливаемого накопителя на магнитной ленте.
7. Откройте вкладку **Driver** (Драйвер) и нажмите кнопку **Update Driver** (Обновить драйвер). В результате произойдет запуск мастера Upgrade Device Driver.
8. В диалоговом окне устройства нажмите кнопку **Next** (Следующий).
9. Установите переключатель в положение **Display a list of the known drivers for this device so that I can choose a specific driver** (Показать список известных драйверов для этого устройства, чтобы я мог выбрать нужный драйвер).
10. Нажмите кнопку **Next** (Следующий).
11. Если накопитель на магнитной ленте неизвестен системе, следующим этапом станет **Hardware Type** (Тип оборудования). В противном случае появится этап **Select a Device Driver** (Установка драйвера устройства).
12. В окне **Hardware Type** (Тип оборудования) следует выбрать либо **Other Devices** (Другие устройства), либо **Tape Drives** (Приводы ленточных накопителей). Затем, чтобы перейти к следующему этапу, выберите **Have Disk** (Есть диск).
13. В окне **Select a Device Driver** следует выбрать **Have Disk** (Есть диск).
14. Вставьте в привод CD-ROM нужный компакт-диск и укажите путь `X:\2000_driver` (где `X` — это имя дисковода CD-ROM).
15. Нажмите кнопку **OK**.
16. Выделите драйвер, соответствующий вашему накопителю на магнитной ленте, и нажмите кнопку **Next** (Следующий).
17. Возможно, вы увидите диалоговое окно с сообщением о несовместимости драйвера с аппаратным обеспечением. Чтобы продолжить установку драйвера, нажмите кнопку **Yes**.
18. Появится окно **Start Device Driver Installation** (Начать установку драйвера устройства).
19. Чтобы установить драйвер, нажмите кнопку **Next** (Следующий).
20. Если мастер сообщит, что данный драйвер уже существует в системе, и пригласит вас сделать выбор, выберите **New** (Новый).
21. На экране появится окно **Windows 2000 Setup**. Проверьте правильность пути к драйверу и нажмите кнопку **Continue** (Продолжить).
22. Следующим будет выведено окно **Completing the Upgrade Driver Wizard** (Завершить работу мастера обновления драйвера). Нажмите кнопку **Finish** (Готово). Возможно, вам будет предложено перезагрузить систему.
23. Установка драйвера накопителя на магнитной ленте завершена.

Установка программы резервирования

После завершения установки драйверов настало время переходить к инсталляции программ резервирования. В этой части главы будет рассматриваться процесс инсталляции, а также применение программного обеспечения BackupExec. Чтобы установить BackupExec непосредственно с компакт-диска, вставьте его в привод CD-ROM. После этого произойдет запуск стандартной программы Auto-run, так что для завершения установки BackupExec вам останется лишь следовать экранным инструкциям. Большинство типов устройств резервирования автоматически обнаруживаются и настраиваются при первом запуске BackupExec. Ваше устройство резервирования будет приведено в окне **Where to Back Up**. При инсталляции программ типа BackupExec сама программа и ее каталог интегрируются в меню **Start** (Пуск) операционной системы Windows (если в процессе установки пиктограмма BackupExec появилась на вашем рабочем столе, то двойным щелчком на ней вы сможете открыть эту программу). Чтобы запустить программу вручную, сделайте следующее.

1. Нажмите кнопку **Start** (Пуск) на панели задач Windows.
2. Выберите **Programs** (Программы), **BackupExec** и установите курсор мыши на каталог BackupExec.
3. Щелкните на пиктограмме **BackupExec**.
4. Программа BackupExec откроется (и появится на панели задач).
5. На экран будет выведено окно **BackupExec Startup**.

Автоматическая защита данных

Автоматическая защита данных (Automatic Data Protection, ADP) обеспечивает проведение регулярного резервирования информации. При первом запуске программы резервирования вы сталкиваетесь с предложением активировать ADP. Любые задания по резервированию, выполненные посредством ADP, впоследствии можно откорректировать с помощью BackupExec. Если настройки расширенного управления питанием (APM) вашей системы предполагают отключение жестких дисков по прошествии определенного периода времени, BackupExec не сможет перезагрузить компьютер и приступить к выполнению запланированного задания по резервированию. Чтобы активировать ADP, выполните следующие действия.

1. Укажите день недели, в который предполагается выполнять задание по резервированию, или выберите **Day** (Дата) или **Weekday** (Рабочие дни).
2. Если вы выбрали определенный день недели, появится опция **New and Changed Files** (Новые и измененные файлы). В случае выбора **Day** или **Weekday**, опция **New and Changed Files** выведена не будет, зато автоматически будут выполняться операции резервирования всех выбранных файлов (**All Selected Files**).
3. Нажмите кнопку **OK**.

Резервирование одной кнопкой

Функция резервирования одной кнопкой предполагает запуск операций резервирования всех локальных жестких дисков, включая данные о состоянии системы. Чтобы активировать функцию резервирования одной кнопкой, сделайте следующее.

1. Дважды щелкните на пиктограмме **One-Button Backup** на рабочем столе или выберите **Start** (Пуск), **Programs** (Программы), **BackupExec**, **One-Button Backup**.

2. В результате появится диалоговое окно **One Button Backup** (рис. 20.3).
3. Выберите нужное устройство (т. е. ваш накопитель на магнитной ленте) в выпадающем списке.
4. Нажмите кнопку **Start** (Пуск).

Примечание

Если при выполнении задания по резервированию на текущей кассете закончится свободное пространство, BackupExec пригласит вас поместить в устройство очередную пустую кассету.

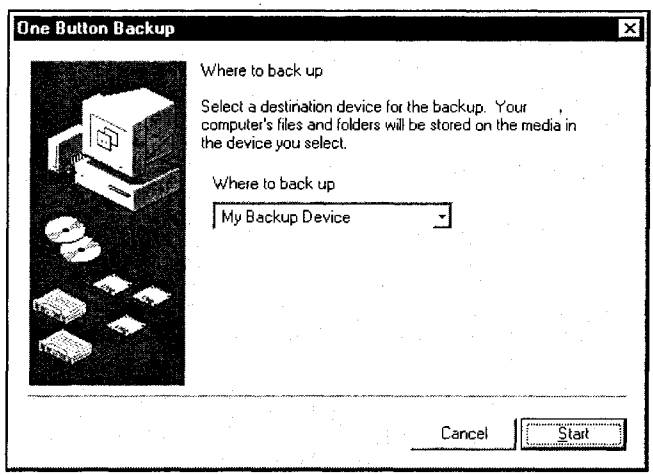


Рис. 20.3. Для занятых администраторов резервирование одной кнопкой упрощает процесс создания резервных копий

5. В зависимости от нижеследующих критериев, будут производиться операции полного или разностного резервирования (с настройками по умолчанию).
6. Резервирование всех выбранных файлов (**All Selected Files**) будет проводиться в том случае, если с момента последнего выполнения такой операции было создано десять разностных копий (вне зависимости от конкретных дат) или если со времени последнего резервирования прошло более семи дней.
7. Разностное резервирование производится в том случае, если со времени создания последней резервной копии всех выбранных файлов (**All Selected Files**) прошло не более семи дней.

Восстановление одной кнопкой

Кнопка **One-Button Restore** производит запуск ряда диалоговых окон, обеспечивающих проведение восстановления системы в несколько этапов. Чтобы активировать функцию восстановления одной кнопкой, выполните следующие действия.

1. Последовательно выберите команды **Start** (Пуск), **Programs** (Программы), **BackupExec**, **One-Button Restore**.
2. В результате появится диалоговое окно **One-Button Restore**.

3. Выберите нужное устройство в выпадающем списке.
4. Чтобы продолжить, нажмите кнопку **Next** (Следующий).
5. Проверьте перечень дисков, каталогов и файлов, которые предполагается восстановить.
6. Чтобы запустить процесс восстановления файлов, нажмите кнопку **Start** (Пуск).

Примечание

Если при выполнении задания по резервированию на текущей кассете закончится свободное пространство, BackupExec пригласит вас поместить в устройство очередную пустую кассету.

Выполнение резервирования

Программа BackupExec использует задания по резервированию в целях сохранения и повторного применения вариантов выбора файлов и опций. Вы можете сформировать задание по резервированию, указав нужные диски и файлы, выбрав настройки и опции программ и сохранив эти варианты выбора в рамках задания с новым именем. Задание по резервированию содержит все варианты выбора, сделанные на момент его сохранения:

- диски, каталоги и файлы, подлежащие резервированию;
- тип резервирования;
- устройство резервирования;
- выбранные опции и варианты выбора, принимаемые по умолчанию.

С помощью меню **Job** (Работа) можно открывать, сохранять и удалять задания по резервированию. В окне **Backup** (Резервирование) вы можете открыть задание по резервированию, указав его в списке **Backup Job**. Чтобы внести в задание по резервированию изменения, просто выполните новые действия по выбору файлов или опций. Впоследствии, при запуске операции резервирования, все эти изменения будут автоматически сохранены. Чтобы сохранить изменения под другим именем, выберите в меню **Job** пункт **Save As** (Сохранить как) и укажите новое имя (или введите новое имя в поле **Job Name**). Если вы попытаетесь сохранить новое задание с помощью существующего имени, программа спросит вас, нужно ли перезаписать существующие задания. Если вы выберите **Overwrite**, ранее существовавшее задание будет заменено новым.

Мастер резервирования

Для создания новых заданий по резервированию, а также для внесения изменений и переименования существующих файлов заданий, вы можете воспользоваться мастером Backup Wizard. В случае сохранения заданий по резервированию впоследствии их можно будет запустить повторно, причем выполнять еще раз действия по указанию вариантов выбора не придется. В окне **Backup Job** приводятся все сохраненные задания по резервированию. Чтобы сохранить задание под новым именем, введите имя в этом окне. Рассмотрим типичную операцию резервирования при ее проведении с помощью Backup Wizard.

1. В окне **Startup** (Запуск) выберите **Backup Wizard**, а затем нажмите кнопку **OK**. Вы также можете щелкнуть кнопкой мыши на пиктограмме **Backup Wizard** на панели

инструментов. В результате появится окно **What to back up** (Что резервировать) — компонент мастера Backup Wizard (рис. 20.4).

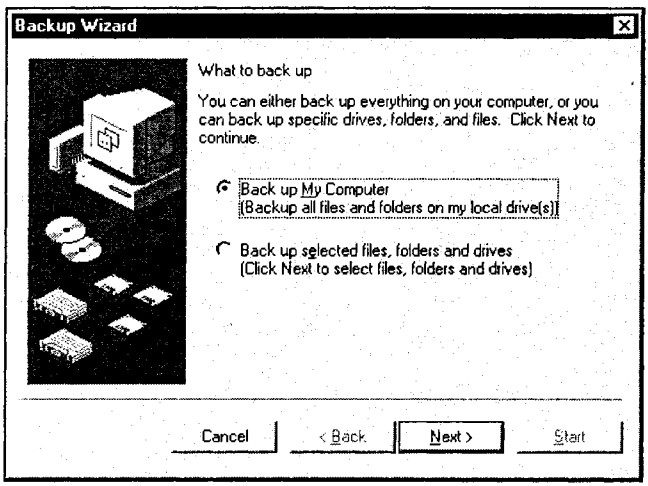


Рис. 20.4. Запуск мастера резервирования и выбор между полным или частичным резервированием

2. Укажите диски и файлы, которые хотите зарезервировать. Чтобы провести резервирование всех файлов, каталогов и дисков вашей системы, выберите **Back up My Computer**. Чтобы продолжить, нажмите кнопку **Next**. После этого появится окно **Backup Type Wizard**. Если вы планируете создать резервные копии лишь части файлов, каталогов или дисков, выберите **Back up selected files, folders and drives**. В результате на экране появится диалоговое окно **Backup Wizard Selection**.
3. Укажите те диски, каталоги и файлы, которые вы планируете зарезервировать. Чтобы продолжить, нажмите кнопку **Next**. Выберите тип резервирования.
4. Чтобы создать резервные копии всех выбранных файлов, выберите **All Selected Files**, а затем нажмите кнопку **Next**. Чтобы выполнить операцию резервирования только новых файлов, а также тех файлов, которые были изменены с момента последнего резервирования всех выбранных файлов (**All Selected Files**), укажите **New and Changed Files Only**, а затем нажмите кнопку **Next**.
5. В списке **Where To Back Up** определите размещение новой резервной копии.
6. Чтобы продолжить, нажмите кнопку **Next**. В результате появится окно **How to back up** (рис. 20.5).
7. Задайте настройки резервирования в этом окне. Чтобы продолжить, нажмите кнопку **Next**. Затем появится окно **When to Back Up Wizard** (Когда резервировать).
8. Чтобы запустить операцию резервирования немедленно, выберите **Now**; если же вы хотите запланировать резервирование на более позднее время, выберите **Later**. Если вы выбрали вариант резервирования, в дальнейшем укажите частоту выполнения операций, задайте время, дату и/или дни недели, в которые будут выполняться задания по резервированию.

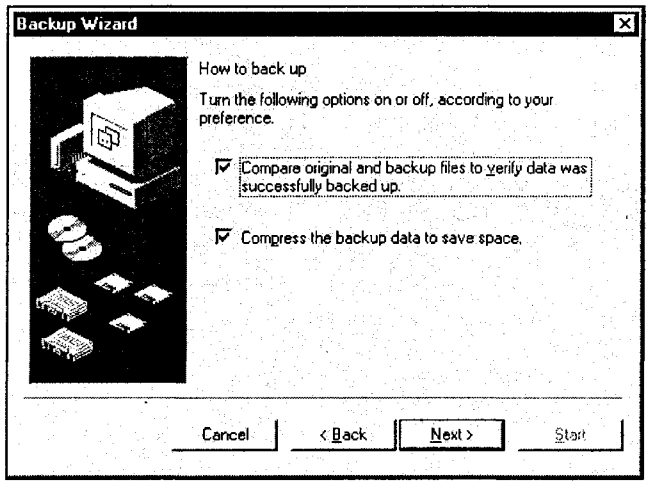


Рис. 20.5. Настройка сравнения и сжатия в мастере резервирования

9. Чтобы продолжить, нажмите кнопку **Next**. В результате появится окно **Name the backup job** (рис. 20.6).

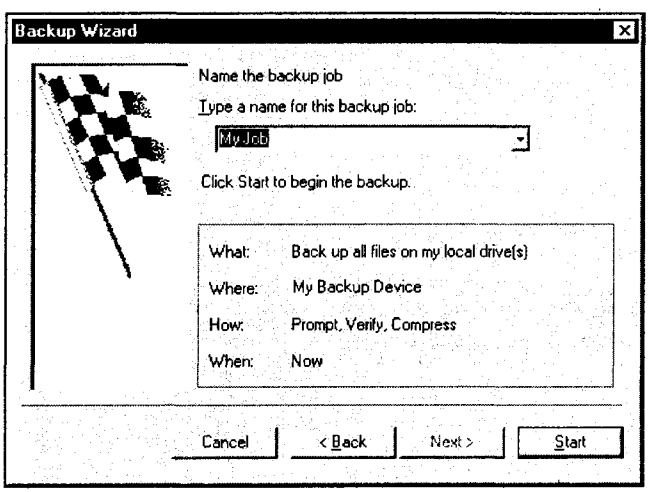


Рис. 20.6. Назначение заданий и запуск операций резервирования с помощью мастера резервирования

10. Введите имя данного задания по резервированию. Ознакомьтесь со сводкой настроек этого задания. Для изменения опций пользуйтесь кнопками **Back** и **Next**. Чтобы активировать задание по резервированию, нажмите кнопку **Start**. После этого на экране появится окно **Backup Progress**. Если вы планируете произвести операцию резервирования в соответствии с заранее составленным графиком, нажмите кнопку **OK**.

Примечание

Если при выполнении задания по резервированию на текущей кассете закончится свободное пространство, BackupExec пригласит вас поместить в устройство очередную пустую кассету.

Проведение сравнения

Сравнение — это самостоятельная функция программы резервирования, призванная обеспечить максимальную целостность данных. После создания резерва окно **BackupExec Compare** позволяет проверить идентичность информации, хранящейся на резервной магнитной ленте и на жестком диске (с помощью этой функции вы можете убедиться в том, что данные читаемы и могут быть задействованы для последующего восстановления). Операции сравнения следует проводить после создания первых нескольких резервных копий, а также после изменения конфигурации системы. Так вы сможете убедиться в корректности работы BackupExec на вашем компьютере. Когда бы вы ни приступили к сравнению, эта операция позволяет узнать, насколько файлы в наборе резервирования отличаются от тех файлов, которые в данный момент находятся на жестком диске. Переход на вкладку **Compare** (рис. 20.7) предоставляет возможность быстрого обращения к опциям сравнения. Эта вкладка состоит из трех основных секций.

- **Compare from**. Раскрывающийся список **Compare from** содержит ссылки на все доступные устройства резервирования, которые можно использовать при сравнении.

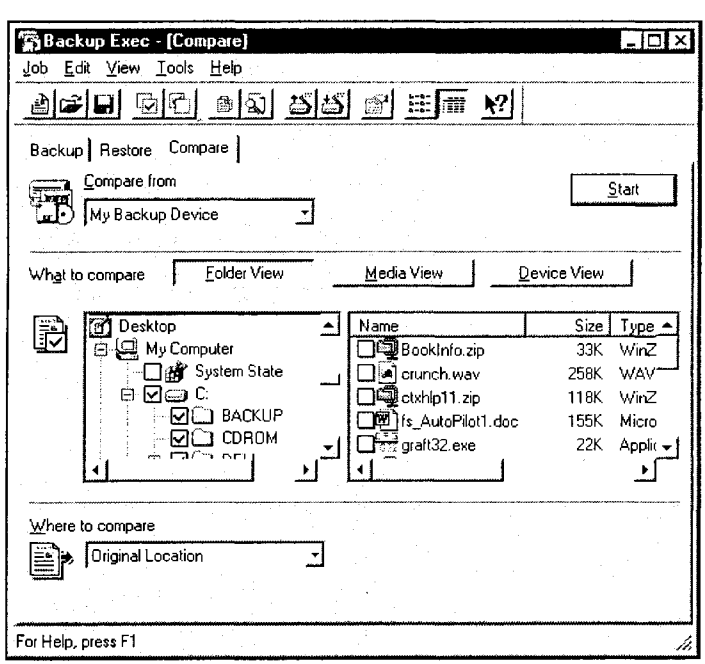


Рис. 20.7. Проведение операции сравнения позволяет проверить текущую резервную копию и повысить надежность последующих операций восстановления

Чтобы изменить диск, с которым будет проводиться сравнение, выберите другой элемент этого раскрывающегося списка.

- **What to compare**. В этой области вы можете выбрать отдельные файлы для сравнения на основе каталогов, носителей или устройства.
- **Where to compare**. Как правило, сравнение файлов проводится в отношении того же диска или каталога, из которого было выполнено их резервирование. Впрочем, если их размещение изменилось, раскрывающийся список **Where to compare** позволяет указать новое местоположение исходных файлов.

После выполнения всех настроек, нажмите кнопку **Start**, чтобы запустить процесс сравнения файлов. Когда процесс сравнения завершится, появятся кнопки **OK** и **Report**. Чтобы просмотреть краткий отчет о выполненной операции сравнения, нажмите кнопку **Report**; чтобы продолжить, нажмите кнопку **OK**.

Проведение восстановления

Функция BackupExec Restore выполняет считывание выбранных наборов резервирования, а затем восстанавливает входящие в них файлы, помещая их в указанное место (обычно применяется их исходное размещение). Вы можете восстановить один файл, несколько выбранных файлов или все файлы набора резервирования. У вас есть возможность выбрать отдельные версии файла, указать размещение восстанавливаемых файлов, а также изменить настройки. Ниже мы рассмотрим операцию аварийного восстановления и работу мастера Restore Wizard.

Аварийное восстановление

Эта первая процедура предоставляет вам возможность быстрого и беспрепятственного восстановления всех файлов в случае отказа жесткого диска (она также может оказаться полезной при перемещении всех ваших файлов на новый компьютер). Прежде чем восстанавливать файлы после возникновения неисправности жесткого диска, необходимо подготовить новый жесткий диск (т. е. провести операции `Fdisk` и `Format`), переустановить операционную систему Windows, а затем (если вы работаете в Windows 2000), выполнить следующие действия.

1. Когда в компьютере будет установлен работающий диск, а операционная система Windows 2000 будет переустановлена, проведите инсталляцию и настройку BackupExec (или другой программы резервирования, которой вы пользуетесь).
2. Соберите все кассеты, на которых содержатся наиболее свежие резервные копии, выполненные по схемам **All Selected Files** (при полном резервировании) и **New and Changed Files** (при добавочном резервировании). Конкретные наборы резервирования, которые вам понадобятся, зависят от того, какой стратегией резервирования вы пользуетесь.
   - *Только полное резервирование* (**All Selected Files only**). Восстанавливайте только самый последний набор резервирования.
   - *Полное резервирование* (**All Selected Files**) *и разностное резервирование* (**New and Changed Files**). Сначала проведите полное восстановление, а затем восстановите самый свежий набор разностного резервирования.
   - *Полное резервирование* (**All Selected Files**) *и добавочное резервирование* (**New and Changed Files**). Сначала проведите полное восстановление, а затем по порядку

(начиная с самого старшего) восстановите каждый из наборов добавочного резервирования.

3. Восстановите набор резервирования **All Selected Files**. В окне **Restore** выполните следующие настройки:
   - **What to restore**. Выберите окно **Device**, а затем укажите каждый локальный диск.
   - **Where to restore**. Выберите **Original Locations**.
   - **How to restore**. Выберите **Always Replace**.

Примечание

Если с момента последнего резервирования состояния системы в аппаратную конфигурацию были привнесены изменения, то восстановление состояния системы может привести к серьезным проблемам.

4. Если с момента последнего резервирования состояния системы аппаратная конфигурация вашего компьютера и его системные настройки не изменились, установите флажок, находящийся рядом с пиктограммой **System State** на панели выбора **Restore Window**. В результате все файлы, содержащие данные о состоянии системы, будут восстановлены вместе со всеми выбранными локальными дисками. Впрочем, если аппаратная конфигурация вашей системы подвергалась изменениям (например, вы установили новый дисковод или изменили настройки прерываний какой-нибудь платы), обязательно сделайте так, чтобы флажок **Restore System State** был снят. В этом случае произойдет восстановление только файлов, выбранных с локальных дисков.
5. Нажмите кнопку **Start**.
6. По завершении операции восстановления вам будет предложено перезагрузить компьютер. Нажмите кнопку **Yes**.
7. Теперь проведите восстановление всех наборов резервирования, составленных по схеме **New and Changed Files**.

Восстановление файлов Bindery

У вас есть возможность провести восстановление файлов Bindery. Если ранее вы создавали резервные копии файлов, расположенных в томе SYS или на Novell Server, установив при этом флажок **Back up NetWare Bindery**, вы можете восстановить файлы Bindery, выполнив действия, аналогичные следующим.

1. Перейдите на вкладку **Restore**. В результате откроется окно **Restore**.
2. Укажите любые файлы, находящиеся в томе SYS.
3. На вопрос о том, следует ли восстановить Bindery, ответьте нажатием кнопки **Yes**.

Мастер восстановления

Простейший способ восстановления потерянных или поврежденных файлов предполагает использование мастера восстановления (Restore Wizard) программы BackupExec.

Этот мастер поможет вам пройти все этапы и провести все настройки, необходимые для формирования задания по восстановлению. Чтобы создать задание по восстановлению с помощью Restore Wizard, сделайте следующее.

1. В окне **Startup** выберите **Restore Wizard** и нажмите кнопку **OK**. Вы также можете нажать кнопку **Restore Wizard** на панели инструментов или выбрать пункт **Restore Wizard** в меню **Tools**. В результате появится окно **Restore from** (рис. 20.8).

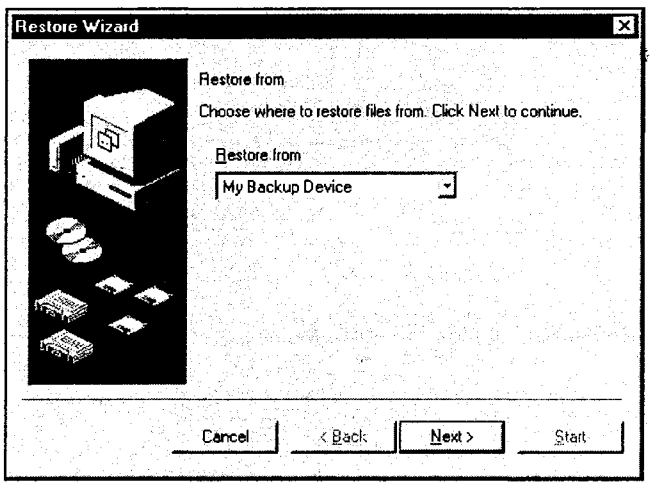


Рис. 20.8. Мастер восстановления позволяет вам выбрать, с какого источника следует проводить операцию восстановления

2. Выберите устройство резервирования, с которого будет выполняться восстановление, и нажмите кнопку **Next**. В результате появится окно **View files to restore**.
3. Вы можете выбрать нужные файлы как из каталога, хранящегося на вашем жестком диске, так и с носителя, установленного в накопитель на магнитной ленте. Чтобы продолжить, нажмите кнопку **Next**. После этого появится окно **Restore Wizard** (рис. 20.9).
4. Установите флажки напротив тех элементов, которые вы планируете восстановить. Чтобы продолжить, нажмите кнопку **Next**. В результате появится **Where to Restore**.
5. Выберите размещение восстанавливаемых файлов. Если вы решите провести их восстановление с размещением в другом месте, введите в окне нужный путь или нажмите кнопку **Browse**. Файлы будут восстановлены с применением исходной структуры каталогов, если только вы не установите флажок **Restore all files to a single folder**. Чтобы продолжить, нажмите кнопку **Next**. В результате появится окно **How to restore** (рис. 20.10) — компонент мастера Restore Wizard.
6. Выберите одну из опций и нажмите кнопку **Start**.
7. На экране появится окно **Media Required**. Следуйте инструкциям на экране, а затем нажмите кнопку **OK**. После этого появится окно **Restore Progress**.

Примечание

Если для выполнения задания по резервированию потребовалось несколько кассет, поместите в накопитель на магнитной ленте первую кассету из набора резервирования. Программа BackupExec оповестит вас о необходимости установки каждой последующей кассеты.

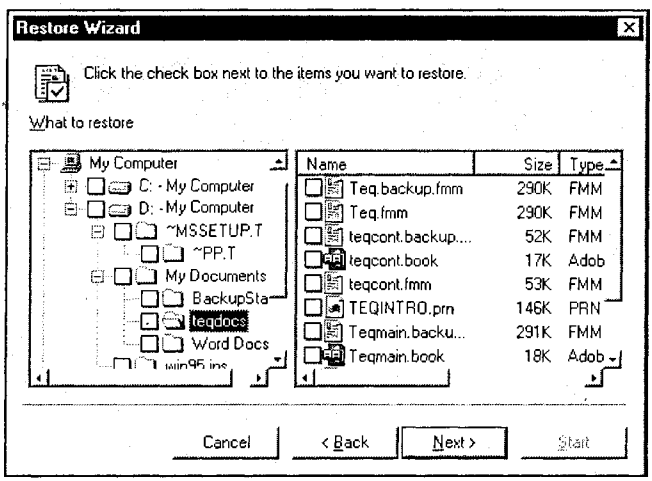


Рис. 20.9. Установите флажки, расположенные напротив тех элементов, которые вы хотите восстановить

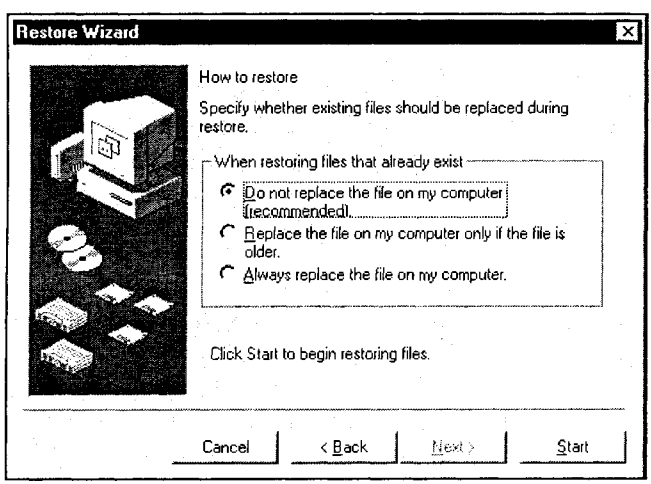


Рис. 20.10. Выберите способ восстановления файлов с помощью мастера восстановления

Проверка установки

После установки нового накопителя на магнитной ленте и программного обеспечения типа Seagate BackupExec вы должны проверить, опознает ли эта программа, а

также ваша система новый дисковод, причем сделать это нужно еще до попытки резервирования данных. Запустите Seagate BackupExec. Просмотрите список целевых устройств, расположенный в окне меню **Where to back up**. Если ваш накопитель на магнитной ленте входит в этот раскрывающийся список, значит, программа Seagate BackupExec опознала его. Это означает, что ваш накопитель на магнитной ленте и программа резервирования готовы к выполнению операций, связанных с резервированием данных. Если ваш накопитель на магнитной ленте отсутствует в этом раскрывающемся списке, значит, программное обеспечение не может его обнаружить.

Поиск неисправностей накопителей на магнитной ленте

Кассеты и накопители на магнитной ленте разрабатываются прочными и обеспечивают длительную, надежную работу при тщательном уходе. Впрочем, хорошо известно, что накопители на магнитной ленте излишне специализированы. Приводные механизмы, драйверы устройства, программы резервирования и кассеты должны отвечать требованиям совместимости. Следовательно, важна корректная установка устройства, его регулярное текущее обслуживание, а также своевременная локализация неисправностей накопителей на магнитной ленте. В этой части главы речь пойдет о распространенных неисправностях кассет и накопителей на магнитной ленте; здесь же будут предложены их решения.

Распространенные сбои при резервировании

Несмотря на то, что резервирование обычно считается экономически эффективной формой архивации данных и надежным средством их защиты, операции по резервированию едва ли можно признать безупречными. Существует большое количество проблем, которые могут неблагоприятно сказаться на ваших (или вашего клиента) усилиях, связанных с резервированием. Ниже приводится несколько "подводных камней", которых следует остерегаться при планировании или выполнении резервирования.

- *Нерегулярное или непоследовательное резервирование.* Вероятно, это самая опасная проблема из всех, что могут возникнуть при реализации стратегии резервирования. Чтобы резервные копии были эффективными, их необходимо создавать регулярно. Слишком часто пользователи выполняют несколько начальных операций резервирования, предусмотренных графиком, а после этого перестают следовать графику, не создавая последующие резервные копии. Вскоре те резервные копии, которые были созданы, оказываются настолько устаревшими, что становятся совершенно бесполезными. Когда происходит аварийная ситуация, оказывается, что инвестиции в оборудование и носители не окупились. Администраторы должны взять себе за правило проводить операции резервирования регулярно и соблюдать последовательность.
- *Плохо организована маркировка и хранение резервных копий.* Эта проблема типична для сложных схем чередования кассет. Зачастую кассеты и другие носители резервных копий разбрасываются по комнате или по отделу, причем их содержимое помечено плохо или не помечено вообще. Эффективные стратегии резервирования предполагают маркирование каждой кассеты и четкое обозначение ее

содержимого. В этом случае никто не сможет случайно выбросить или записать кассету. Комплекты кассет всегда следует хранить вместе в закрытом ящике или на стеллаже, т. е. так же, как вы храните книги. Довольно трудно проводить регулярные операции резервирования, если для этого постоянно приходится искать нужные кассеты и угадывать, какую из них нужно записать в этот раз. Возьмите себе за правило хранить кассеты (и вообще все магнитные носители) вдали от телефонов, мониторов, источников питания, при надлежащих режимах температуры и влажности.

- *Недостаточная готовность к аварийным ситуациям.* Это еще одно препятствие к успешному проведению операций резервирования. Слишком часто предприятия вкладывают значительные средства в оборудование для резервирования, а потом оставляют кассеты с резервными копиями лежащими прямо на компьютерах. Если в случае аварийной ситуации вы рассчитываете воспользоваться резервными копиями, кассеты нужно хранить в месте, достаточно защищенном от всяких неприятностей (т. е. от огня, наводнений, краж или диверсий). Во многих случаях с этой функцией довольно неплохо справляется огнеупорный сейф или картотечный шкаф. Те же принципы актуальны и в том случае, если вы планируете хранить резервные копии вне рабочего места.
- *Недостаточное тестирование и текущее обслуживание.* Некоторые предприятия настолько увлекаются проведением резервирования, что не проверяют надежность резервных копий. При возникновении аварийных ситуаций они ужасаются, обнаруживая, что в резервных копиях недостает важнейших файлов, они не читаются или некорректно восстанавливаются. Таким образом, резервная копия становится практически бесполезной. После создания резервной копии ее следует протестировать, используя функции сравнения или подтверждения программы резервирования, чтобы проверить соответствие содержимого кассеты набору файлов на диске. Это занимает немного больше времени, но выполнять эти операции в каждом случае создания резервной копии не нужно. Появление сообщения об ошибке обычно означает, что накопитель на магнитной ленте неисправен. Возможно, необходимые при его эксплуатации регулярные операции по чистке не проводились. Попробуйте очистить устройство резервирования, следуя рекомендациям производителя, а затем проведите операцию резервирования повторно. Время от времени стоит проверять возможности создания резервных копий с помощью процедуры испытаний резервирования.
- *Недостаточное внимание к носителям.* Как и дискеты, кассеты являются магнитными носителями. К сожалению, срок службы магнитных носителей не бесконечен. Одна из наиболее серьезных проблем, связанных с частым проведением резервирования, заключается в том, что пользователи приписывают ошибки создания резервных копий или сравнения неисправностям накопителей или программам резервирования, в то время как на самом деле проблема связана с изношенностью кассеты. Как правило, следует планировать замену кассет, по меньшей мере, раз в год. Если вы часто проводите операции резервирования, то и замена кассет должна производиться чаще. Срок годности кассеты зависит и от ее качества. Высококачественные кассеты служат дольше, чем кассеты низкого качества. Часто оказывается, что разумнее потратить немного больше на надежную, высококачественную кассету, чем незначительно сэкономить, купив кассету по низкой цене, а потом обнаружить, что она изнашивается намного быстрее или теряет данные, когда они так нужны!

Текущее обслуживание накопителей на магнитной ленте и кассет

Накопители на магнитной ленте требуют регулярного обслуживания. Только в этом случае они могут нормально работать. Как правило, вы должны проводить две операции, относящиеся к текущему обслуживанию: чистку накопителя на магнитной ленте и техническое обслуживание кассет. Эти рутинные процедуры способны сильно повлиять на общую эффективность работы накопителя на магнитной ленте и повысить надежность резервных копий.

Примечание

Здесь приводятся лишь общие инструкции. Чтобы ознакомиться с рекомендациями по чистке для вашего устройства, а также с предупреждениями производителя, обращайтесь к руководству по эксплуатации устройства. В каждом устройстве применяются разные процедуры чистки и профилактического обслуживания. Для некоторых накопителей на магнитной ленте необходимо периодическое смазывание.

Чистка накопителя на магнитной ленте

Как и флоппи-дисководы, накопители на магнитной ленте обеспечивают непосредственный контакт магнитного носителя с магнитными головками считывания/записи. С течением времени магнитные окиси с ленты оседают на поверхности головки. Окиси (в сочетании с частицами пыли и дымовым загрязнением) накапливаются и начинают действовать как клинья, которые не позволяют ленте напрямую соприкасаться с поверхностью головки. Даже если у вас никогда не возникнет повода демонтировать накопитель на магнитной ленте, вы должны принять за правило регулярное выполнение его чистки. Систематическая чистка увеличивает срок службы носителей информации и способна значительно снизить частоту появления ошибок данных, в особенности во время операций по восстановлению данных, когда проблемы могут привести к прекращению операций.

Цель операции чистки накопителя на магнитной ленте очень проста: вы должны удалить все инородные вещества, которые могут накопиться на головке считывания/записи. Наиболее распространенный метод чистки предусматривает использование готовой чистящей кассеты. Такая кассета содержит отрезок абразивного чистящего материала небольшой концентрации. Когда в устройстве проигрывается чистящая кассета, с головки удаляются все инородные частицы. Чистящая кассета часто применяется несколько раз, а затем выбрасывается. Некоторые чистящие кассеты можно использовать сухими, а другие нужно смачивать чистящим спиртовым раствором. Преимуществом чистящей кассеты является простота использования. Процедура ее применения проходит быстро, причем для этого вам не приходится демонтировать накопитель на магнитной ленте. Так как кассета типа QIC и Travan движется по головке считывания/записи значительно медленнее, чем гибкий диск, вам не нужно беспокоиться о возможных повреждениях головки считывания/записи из-за трения. DAT (Digital Audio Tape — цифровая аудиолента) и 8-миллиметровые (спиральные) головки движутся по ленте быстро, так что вам нужно точно определить продолжительность чистки. Вы добьетесь наилучшего длительного эффекта, пользуясь сухими чистящими кассетами с пропиткой, снижающей трение.

Примечание

Чистящие кассеты обычно не перематываются; после полного оборота в устройстве они просто выбрасываются. Впрочем, многие накопители на магнитной ленте не обнаруживают окончание чистящей ленты. Вы должны регулярно проверять чистящие кассеты и выбрасывать их, как только их ресурс исчерпан.

Чистка с помощью автоматической загрузки

Автоматическая загрузка — это функция, обеспечивающая загрузку и выгрузку кассет DAT со спиральной разверткой (примерно таким же образом в видеомагнитофонах применяется автоматическая загрузка кассет). В некоторых накопителях на магнитной ленте DAT механизм загрузки извлекает кассеты из отсека, помещает их в устройство DAT, а затем, после выгрузки кассет внутренним устройством, помещает их обратно в отсек. Механизмы автоматической загрузки и направляющие также нуждаются в регулярной чистке (а может быть, и в смазывании). Это нужно делать раз в месяц или при сигнализировании об ошибке автоматической загрузки на передней панели.

Текущее обслуживание кассет

Накопители на магнитной ленте — это одно из наиболее прочных устройств в мире персональных компьютеров. Кассета состоит из жесткой пластиковой оболочки, а головка считывания/записи обычно защищена металлическим или пластиковым корпусом. Но и кассеты подвержены физическим повреждениям. Чтобы сохранить целостность содержащихся на них данных, с ними нужно обращаться с осторожностью. Наши советы помогут вам обеспечить длительную работу кассет.

- *Не оставляйте на ленте отпечатки пальцев.* Не открывайте шторку доступа к ленте на кассетах и не прикасайтесь к самой ленте. Отпечатки пальцев на ленте могут помешать накопителю считать с нее информацию и привести к появлению ошибок.
- *Установите переключатель защиты от записи.* Выполнив резервирование, обязательно установите переключатель защиты от записи. Так вы уменьшите вероятность непреднамеренной перезаписи важных данных в случае, если данная кассета останется немаркированной.
- *Остерегайтесь магнитных полей.* Ленты чувствительны к магнитным полям, излучаемым мониторами, звонками электромеханических телефонов, вентиляторами и тому подобными устройствами. Держите ленты вдали от источников магнитных полей.
- *Остерегайтесь тонера.* Тонер, применяемый в лазерных принтерах и фотокопировальных устройствах, представляет собой мельчайшую пыль, которая может источаться устройствами в небольших количествах. Чтобы избежать случайного загрязнения пылью красящего порошка, храните кассеты на достаточном удалении от принтеров и копиров.
- *Следите за условиями хранения кассет.* Берегите кассеты от прямого солнечного света, храните их сухими и избегайте резких перепадов температуры (внезапных переходов от жары к холоду). Прежде чем использовать кассету, дайте ей время постепенно достичь комнатной температуры.

- *Регулярно перематывайте кассеты.* Прежде чем использовать кассету, которая лежала без употребления в течение месяца или дольше, воспользуйтесь программой резервирования, чтобы перемотать эту кассету. Так вы сможете избавиться от "тесных" участков, которые возникают на кассетах довольно часто.

Вероятно, вы замечали, что при частом воспроизведении видеокассеты качество изображения и звука, записанных на ней, начинает понемногу ухудшаться. Это естественное действие стирания, которое происходит, когда носитель постоянно соприкасается с головками считывания/записи. Кассеты служат не вечно, и после некоторого периода употребления их следует уничтожать, причем делать это нужно до того, как их надежность снизится до такой степени, что ваши данные окажутся в опасности. Срок службы кассеты обычно измеряется в прогонах. Но отследить количество прогонов трудно, т. к. при проведении одной операции резервирования и восстановления происходит множество прогонов. Срок службы кассеты зависит от того, как она используется. Например, ежедневные операции резервирования на 8-миллиметровую ленту могут привести к тому, что первая половина пленки износится, а вторая останется почти неиспользованной. Как правило, разумно следовать правилу "20 случаев применения": если кассета используется каждый день, ее нужно менять каждый месяц. Если лента используется каждую неделю, меняйте ее каждые полгода. Если лента используется раз в месяц, ее следует менять каждые 18—24 месяца.

Примечание

Независимо от того, как вы планируете замену кассет, имейте в виду, что каждая кассета подлежит немедленной замене в случае ее намокания, замораживания или перегрева, а также в ситуации постоянно повторяющихся ошибок носителя, о которых сообщает ваша программа резервирования.

Ошибки, возникающие из-за игнорирования операций чистки

Накопитель на магнитной ленте — это один из механизмов, наиболее подверженных накоплению загрязнений. Если не содержать накопитель на магнитной ленте в чистоте, будет происходить большое количество выпадений сигналов, при которых устройство не сможет производить считывание или запись данных на кассету (при несоблюдении рекомендованного графика чистки головки устройства вы можете потерять до 20% емкости резервирования и производительности). Профессиональные накопители на магнитной ленте обычно предусматривают проведение текущего контроля общего количества выпадений сигналов. Когда их число достигает предварительно установленного порога (определяемого в микропрограммном обеспечении устройства), светодиод устройства начинает медленно мигать, указывая на то, что устройство нуждается в чистке. Ниже упоминаются лишь некоторые ошибки, которые могут быть вызваны несоблюдением регулярности текущего обслуживания и чистки накопителя на магнитной ленте.

- *Выпадение сигнала.* Выпадения вызваны слабостью сигнала, поступающего от загрязненных головок считывания/записи, что может привести к снижению емкости кассеты и эффективности операций резервирования.
- *Ошибки носителя.* Ленты в кассетах резервирования могут мяться, рваться и часто повреждаться из-за загрязнения головки считывания/записи. В результате может потребоваться замена неисправной кассеты.

- *Ошибки считывания или записи.* В процессе резервирования из-за загрязнения головки считывания/записи данные могут не записаться на кассету. Даже если данные на кассете резервирования уже есть, их извлечение может стать невозможным, если загрязненной головке не удастся их считать.
- *Ошибки форматирования.* В процессе резервирования данные фиксируются на кассете в определенном формате, применение которого помогает их извлекать. Загрязненность головки записи может приводить к ошибкам форматирования, а это означает, что впоследствии данные будут потеряны, или их не удастся считать.
- *Дефектные участки.* Лента может не воспринимать данные вследствие повреждения кассеты. Помимо этого, головка считывания/записи может не справиться с чтением данных с дефектных участков, появление которых обуславливается неисправностью кассеты.

Неисправности кассет и приводов DAT

Накопители на магнитной ленте DAT особенно чувствительны к загрязняющим веществам и дефектам кассет. Если кассета DAT близка к неисправности или неисправна, накопитель на магнитной ленте генерирует ошибку, которая либо выводится через индикатор(ы) устройства, либо передается программе резервирования. Фиксируется несколько свойств кассет DAT, которые могут привести к выводу ошибок устройствами DAT.

- *Засорение головки.* Это наиболее распространенная проблема, вызванная наличием на головках считывания/записи случайных частиц. Этот осадок не позволяет устройству производить считывание или запись на ленту. Сообщения о засорении головок могут поступать различными путями (в зависимости от версии микропрограммного обеспечения). При засорении головки необходимо выполнить ее четырехкратную чистку. Проблемы с лентой также могут приводить к засорению головки. Следите за сбоями ленты при первых трех случаях ее применения. Если кассета дает сбой два раза из трех, она должна быть признана неисправной и заменена.
- *Слишком плотно скрепленные кассеты.* Такая ситуация может быть ошибочно допущена на этапе производства (когда лента трется о верхнюю и/или нижнюю внутреннюю часть оболочки кассеты). В результате появляется сопротивление, достаточное для того, чтобы накопитель на магнитной ленте DAT потерял возможность равномерного продвижения ленты. Например, функция автоматической загрузки выводит сообщение "BAD TPE #", где # указывает на номер места кассеты. Чрезмерно плотно скрепленные кассеты необходимо заменять.
- *Неисправности призмы-отражателя начала/конца ленты.* Неисправности такого рода обуславливаются дефектами кассет. Они встречаются не часто, но когда случаются, периодически мешают лентопротяжному механизму определять начало или конец кассеты. В результате механизмы, которые отвечают за движение ленты, внезапно прекращают работать, о чем вас извещает сообщение о соответствующей ошибке. Подобные кассеты необходимо заменять.
- *Физические повреждения ленты.* Они могут наноситься лентопротяжным механизмом, но могут появляться и на этапе производства. Подобная проблема всегда возникает в точно определенном месте ленты. Подтвердить ее наличие мож-

но только путем тестирования с помощью специального инструмента отладки, который способен выбрасывать ленту без ее перемотки и, таким образом, демонстрировать повреждение; в этом случае требуется фиксация ленты. Как правило, кассеты с подобными дефектами рекомендуется заменять.

- *Смещение центра ленты.* Проблемы подобного рода обычно вызывают шум во время высокоскоростных движений ленты, например, при обратной перемотке. В таких случаях кассету рекомендуется менять.

Рекомендуемые способы чистки накопителей на магнитной ленте DAT

Чтобы оптимизировать производительность и надежность накопителей на магнитной ленте DAT, следуйте приведенным ниже рекомендациям по их чистке.

- При использовании новых кассет в целях резервирования, накопители на магнитной ленте DAT необходимо чистить через каждые 8 часов считывания/записи вплоть до того момента, когда вся кассета с данными не будет использована пять раз.
- Для кассет, которые уже использовались пять или более раз, чистить накопители на магнитной ленте DAT нужно каждые 25 часов считывания/записи.
- Чистите накопители на магнитной ленте DAT, прежде чем приступить к полному резервированию сервера (или крупной системы).
- Регулярные операции следует проводить однократно. Так вы сможете минимизировать износ головки. В некоторых случаях один цикл не обеспечивает полной очистки головок считывания/записи накопителя. Если программа резервирования выводит сообщения об ошибке, проведите повторную чистку устройства. Так вы сможете устранить одну из возможных причин возникновения ошибок.
- Незагрязненность головок после сбоя можно обеспечить только путем четырехкратной чистки. Вполне возможно, что один цикл чистки не приведет к полному устранению засорения головки.
- При активации автоматической загрузки держите чистящую кассету в последнем посадочном месте. За инструкциями по планированию и осуществлению операций автоматической чистки с помощью программы резервирования обращайтесь к руководству по эксплуатации этой программы.
- Чистящие кассеты DAT обычно выдерживают 30 циклов (прогонов) чистки. Не забывайте менять чистящую кассету после истощения ее ресурсов.

Симптомы неисправностей

Наши рекомендации могут помочь вам устранить многие простые проблемы и упущения, но бывают случаи, когда нужна более детальная информация. Приведенные ниже ситуации очерчивают часто встречающиеся аппаратные и программные проблемы и содержат инструкции по их устранению.

Симптом 20.1. Накопитель на магнитной ленте не работает

Начните ремонт с проверки очевидных ошибок, которые могли быть допущены при монтаже и настройке. Для начала проверьте, подается ли к накопителю на магнитной ленте питание (обычно, если это так, на устройстве загорается индикатор питания). Внутренний накопитель на магнитной ленте обычно питается от компьютера,

в котором он установлен, так что вам нужно проверить надежность подключения внутреннего четырехвыводного разъема питания. Внешние накопители на магнитной ленте почти всегда питаются от отдельного адаптера переменного тока или источника питания, но некоторые специализированные устройства могут питаться через свои соединительные кабели. Проверьте выходную мощность каждого внешнего адаптера переменного тока или источника питания. Если выходная мощность адаптера переменного тока низка или отсутствует вообще, его необходимо заменить.

Проверьте надежность подключения соединительного кабеля между накопителем на магнитной ленте и платой контроллера. Убедитесь в том, что ваша программа резервирования работает и имеет все настройки, необходимые для взаимодействия с данной моделью накопителя на магнитной ленте. Если вы пытаетесь найти неисправность в рамках нового, непроверенного монтажа, проверьте адрес, прерывание и настройки DMA платы контроллера, т. к. конфликты настроек способны заблокировать программный пакет или привести устройство в нерабочее состояние. Проверьте саму кассету. Необходимо, чтобы она была установлена в устройстве надежно и полностью.

Проверьте сигналы индикаторов устройства, которые могут указывать на его неисправность. Если ошибка указывает на неисправность устройства, накопитель на магнитной ленте необходимо заменить. Если устройство просто не взаимодействует с системой, проверьте надежность его монтажа, контроллер, драйвер и программу резервирования.

Симптом 20.2. Операции считывания и записи на кассету не производятся, но лента и головка движутся

Вероятно, программа резервирования указывает на наличие ошибок считывания/записи. Начните ремонт с проверки самой кассеты. Кассета должна быть помещена в устройство полностью и надежно, плотно фиксироваться на катушке. Если кассета правильно вставлена в устройство, попробуйте вставить другую кассету. Старые кассеты могут портиться до такой степени, когда надежное считывание данных и их запись становятся невозможны. Если новая кассета работает исправно, выбросьте и замените старую кассету. Если же неисправность сохраняется, попробуйте почистить головки считывания/записи накопителя на магнитной ленте. Избыточное скопление пыли или остаточных окисей вполне может препятствовать нормальному проведению операций записи/считывания с ленты. Если вы все еще сталкиваетесь с проблемами при чтении/записи, вполне возможно, что головки считывания/записи или связанные с ними схемы повреждены. Попробуйте заменить накопитель на магнитной ленте.

Симптом 20.3. Накопитель на магнитной ленте осуществляет запись на кассету с защитой от записи

Когда кассета защищена от записи, накопитель на магнитной ленте не может проводить по отношению к ней операции записи. Прежде всего, вам нужно снять и проверить состояние кассеты. Проверьте, действительно ли переключатель защиты от записи установлен в положение "защищено". Если переключатель стоит в другом положении, то на кассету можно производить запись. Если переключатель защиты от записи установлен в защитное положение, вам следует заменить накопитель на магнитной ленте.

Симптом 20.4. Программа резервирования указывает на "слишком большое количество дефектных секторов" на кассете

Вы можете столкнуться с ошибкой типа "неудачи при исправлении ошибок". Ошибки такого типа обычно означают, что нечитаемыми является более 5% секторов ленты. Во многих случаях эта неисправность обуславливается загрязнением головок считывания/записи. Попытайтесь прочистить блок головок считывания/записи. Если сбои будут продолжаться, попробуйте воспользоваться новой кассетой. Если и это не поможет, проверьте надежность монтажа источника питания и сигнальных кабелей накопителя на магнитной ленте.

Симптом 20.5. Программа резервирования на магнитных лентах генерирует ошибку XX накопителя на магнитной ленте

Тип ошибки ("xx") зависит от конкретного накопителя на магнитной ленте и программы резервирования, которыми вы пользуетесь, так что за точными расшифровками кодов вам следует обращаться к руководству по эксплуатации. Приведенные ниже примеры кода относятся к программе резервирования на магнитных лентах Colorado.

- 0Ah (обрыв или загрязнение ленты). Тщательно прочистите головки считывания/записи и замените кассету (в случае обрыва ленты).
- 0Bh (ошибка доступа). Прежде чем пытаться провести операцию резервирования, переформатируйте кассету.
- 1Ah (произошел сброс по включению питания). Проверьте силовые и сигнальные соединения накопителя на магнитной ленте и повторите попытку.
- 1Bh (произошел программный сброс). Закройте все приложения, которые могут конфликтовать с программой резервирования на магнитных лентах.
- 04h (заклинивание привода накопителя на магнитной ленте). Извлеките кассету и убедитесь в том, что ничто (включая кассету) не блокирует привод(ы). Вставьте новую кассету и повторите попытку.

Симптом 20.6. Накопитель на магнитной ленте работает в DOS, но отказывается работать в Windows 9x и более поздних версиях

В первую очередь проверьте, обнаруживает ли программа резервирования, которой вы пользуетесь в Windows 9x, накопитель на магнитной ленте. Если программа резервирования работает исправно, вполне возможно, что с накопителем на магнитной ленте конфликтует один или несколько драйверов Windows 9x. Если обращение к накопителю на магнитной ленте теперь возможно, вам нужно будет проверить, не случаются ли конфликты драйверов или программ. Часто подобная ситуация происходит тогда, когда при резервировании на магнитной ленте через параллельный порт драйверы Windows 9x блокируют обращение к параллельному порту, пользуясь сторонними драйверами принтеров, загруженными SYSTEM.INI. Вам следует проверить секцию `[386Enh]` файла SYSTEM.INI и с помощью точек с запятыми "перераз-метить" все строки `device=`, нарушающие нормальную работу.

Симптом 20.7. Программа резервирования генерирует ошибку оверлея типа "не удалось открыть файл: QBACKUP.OVL"

Невозможность открытия файлов OVL часто обуславливается недостаточностью буферов. Например, в файле CONFIG.SYS обычно должно быть установлено значение

BUFFERS=30 или выше. В противном случае утилита резервирования может работать некорректно. После внесения изменений в файл CONFIG.SYS не забудьте сохранить их, прежде чем перезагружать компьютер.

Примечание

Возьмите за правило создавать резервные копии файлов CONFIG.SYS и AUTOEXEC.BAT, прежде чем вносить в них какие-либо изменения. Так вы сможете с легкостью восстановить исходные загрузочные файлы, не прибегая к их повторному редактированию.

Симптом 20.8. Вы сталкиваетесь с ошибками носителей, ошибками дефектных участков, системными ошибками или блокировками

Известно, что подобного рода проблемы случаются с кассетами типа Travan, причем в таком случае нужно рассмотреть несколько вариантов. Для начала попробуйте извлечь из устройства кассету с данными Travan, а затем вставить ее заново. Во многих случаях такое действие предоставляет лентопротяжному механизму возможность сброса любых ошибок. Если неисправности сохранятся, попытайтесь провести повторную инициализацию кассеты с данными (обычно это делается с помощью программы резервирования типа Tools и Initialize). Учтите, что повторная инициализация кассеты приведет к тому, что все находящиеся на ней данные станут непригодными для применения. Попробуйте также отключить сжатие данных.

Примечание

Все кассеты с данными TR-4 существуют в заданном формате, причем повторно отформатировать их вам удастся лишь в том случае, если ваш накопитель на магнитной ленте поддерживает форматирование лент TR-4. Следовательно, не стоит полностью стирать кассеты TR-4 с помощью электромагнита или аналогичного устройства.

Симптом 20.9. Во время инициализации в среде DOS или Windows драйвер накопителя на магнитной ленте SCSI (например, BPASPI.SYS) сообщает об ошибке, в соответствии с которой "устройство ASPI не найдено"

Во многих случаях выясняется, что причиной возникновения подобной неисправности является тест драйвера на наличие расширенных параллельных портов; следовательно, вы должны попытаться отключить тест EPP, добавив в драйвер накопителя на магнитной ленте ASPI ключ командной строки, например, так:

```
device=\bpaspi\bpaspi.sys NOEPP
```

Имейте в виду, что ваш накопитель на магнитной ленте и его драйвер могут поддерживать применение других ключей командной строки. После внесения изменений в файл CONFIG.SYS, сохраните их, а затем, прежде чем перезагружать систему, отключите накопитель на магнитной ленте и компьютер.

Симптом 20.10. При использовании накопителя на магнитной ленте Colorado Trakker вам не удается заставить его надежно сохранять или восстанавливать файлы

Возможно, вы встретитесь с сообщениями об ошибках типа: "Невозможно выполнить корректную передачу данных. Повторите операцию", "Заголовок ленты содер-

жит неожиданные или недействительные значения", "Программа Microsoft Backup столкнулась с ошибкой при считывании данной кассеты. Эта ошибка может быть вызвана тем, что кассета не отформатирована или отформатирована неверно. Проведите повторное форматирование кассеты, а затем повторите попытку". Практически во всех случаях оказывается, что накопитель на магнитной ленте (или программа резервирования) не работают через параллельные порты EPP или ECP. Вы должны открыть CMOS Setup и заменить режим параллельных портов на режим совместимости (Compatibility mode).

Примечание

Если при резервировании файлов вы и не столкнетесь с ошибками, то впоследствии вам, возможно, не удастся сравнить или восстановить эти файлы. Если вы все же сможете восстановить файлы, то данные, восстановленные на жестком диске, могут оказаться поврежденными.

Симптом 20.11. На проведение операции резервирования уходит намного больше времени, чем вы ожидали

Подобная низкая производительность операции резервирования может сопровождаться столь же низкой производительностью жесткого диска при выполнении других задач в Windows. К такому эффекту могут приводить различные факторы. Во-первых, вполне вероятен недостаток свободных ресурсов оперативной памяти. Возможно, в одно и то же время открыто слишком много программ или объем установленной в системе физической памяти слишком мал. Попробуйте перед запуском процесса резервирования закрыть все программы. Если от этого производительность не повысится, удалите все программы из каталога Startup и из строк `load=` и `run=` файла WIN.INI, а затем перезагрузите Windows. Если и это не приведет к желаемому результату, вполне вероятно, что для повышения производительности объем системной оперативной памяти нужно увеличить.

Возможно, один или несколько жестких дисков в системе работают в режиме совместимости. Если на вкладке **Performance** свойств системы (**System properties**) указано, что один или несколько жестких дисков работают в режиме эмуляции MS-DOS, смена этого режима и должна являться решением, позволяющим повысить производительность резервирования. Возможно, вам понадобится новый драйвер защищенного режима для жесткого диска. Даже если ваши жесткие диски не находятся в режиме эмуляции MS-DOS, скорость резервирования может обуславливаться их общей производительностью. Например, если вы пользуетесь жестким диском IDE, его производительность может зависеть от другого устройства, подключенного к тому же каналу IDE-контроллера (например, от приводов CD-ROM). Попробуйте установить медленно работающее устройство на отдельный IDE-контроллер или на второй канал IDE двухпортового контроллера.

Если вы пользуетесь сжатием диска, работая на компьютере со старым процессором, то производительность жесткого диска может быть заметно снижена. При использовании стороннего программного обеспечения сжатия диска, применяющего для обращения к сжатым дискам драйвер реального режима, повышение производительности можно осуществить путем замены этого драйвера на драйвер защищенного режима (для этого нужно связаться с производителем программы сжатия, которой вы пользуетесь).

Проверьте фрагментацию файлов на вашем жестком диске. Плохо фрагментированные жесткие диски могут оказывать негативное влияние на производительность программ резервирования и других задач в Windows. Чтобы выполнить дефрагментацию жестких дисков, запустите утилиту DEFRAG. Наконец, довольно часто программа резервирования имеет возможность обнаруживать и обходить непригодные секторы на ленте, но процесс, который для этого применяется, может занимать много времени. Если вы подозреваете, что производительность повышается вследствие наличия на ленте непригодных секторов, попробуйте использовать новую кассету или кассету, на которой непригодные секторы гарантированно отсутствуют.

Симптом 20.12. Во время выполнения операций резервирования фиксируются избыточные движения ленты

При нормальной работе накопителей на магнитной ленте они пишут данные сначала на одну дорожку от одного конца ленты до другого, затем на другую дорожку данных до начала ленты и т. д., вплоть до полного заполнения ленты. При этом возможно частое передвижение ленты из начала в конец и обратно. Если окно резервирования открыто, сверните его. Когда это окно находится в открытом состоянии, системе приходится постоянно обновлять экран, а это отбирает ресурсы у программы, отсылающей данные накопителю на магнитной ленте. Если ваша система поддерживает работу в ускоренном режиме, попробуйте отключить этот режим (особенно при подключении накопителя на магнитной ленте к параллельному порту).

Дополнительные ресурсы

Периферийные устройства компьютера: **www.cpuinc.com**.

Exabyte: **www.exabyte.com**.

Seagate: **www.seagate.com**.

Tandberg Data: **www.tandberg.com**.

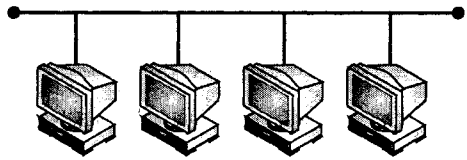
Overland Data: **www.ovrland.com**.

Hewlett-Packard: **www.hp.com/tape/colorado/index.html**.

AIT Technology: **www.aittape.com**.

Стандарты DLT: **www.dlttape.com**.

Стандарты LTO: **www.lto-technology.com**.



ГЛАВА 21

Внедрение простейшей сети

Сети не возникают из ничего. Они создаются на основе детального плана, который разрабатывается исходя из тщательного анализа характеристик задействованных аппаратных и программных элементов. Развертывание удачной сети требует обширного планирования и подбора. При работе с существующей сетью необходимо иметь доступ ко всем имеющимся документам, картам, схемам и прочей административной информации. Располагая такой информацией, вы можете подбирать новое аппаратное и программное обеспечение, а также кабели, совместимые с существующей схемой сети. Развертывание новой сети с нуля — это более сложное предприятие. Вы должны будете оценить потребности вашей организации и ее сотрудников, выбрать аппаратное и программное обеспечение, отвечающие этим потребностям (и бюджету), спланировать и провести монтаж, а затем сформировать систему защиты посредством учетных записей и коллективных ресурсов. Основной принцип заключается в том, что тщательное планирование и методический подход совершенно необходимы в деле модернизации существующей сети или создания новой. В этой главе вы ознакомитесь с некоторыми элементами сетевого планирования и его примерами, и сможете получить представление об основных принципах настройки и устранения неисправностей.

Проектирование простейшей сети

При модернизации существующей сети или проектировании новой первым этапом должно быть планирование. Это утверждение может показаться совершенно очевидным, но вы бы изумились, если бы знали, сколько сил затрачено на исправление недосмотров и проблем, связанных с совместимостью. Тщательное планирование и его критический анализ могут устранить множество потенциальных проблем (и ненужных затрат) на этапе непосредственной реализации. Процесс планирования обычно можно разделить на пять основных этапов: постановка задач, оценка имеющихся ресурсов, составление рабочего плана, проведение его критического анализа и, наконец, осуществление рабочего плана. В идеале, реализованный план должен совпадать с целями, поставленными в начале работы над проектом (или даже превышать их).

Постановка задач

Как ни удивительно, постановка четких задач часто оказывается самой трудной и нервирующей частью всего процесса. На этом этапе необходимо обозначить предполагаемые действия и задачи, которые нужно решить. Если вам нужно всего лишь поставить очередную рабочую станцию или обновить сетевой адаптер, это не очень важно, но при необходимости формирования или расширения сети это совершенно необходимо, т. к. определение целей заложит основы выполнения всего проекта. Например, в ходе типичного процесса планирования вам, вероятно, понадобится ответить на следующие вопросы.

- ❒ Сколько пользователей нужно объединить в сеть?
- ❒ Сколько существующих компьютеров нужно подсоединить?
- ❒ Сколько существующих устройств (например, принтеров) нужно подсоединить?
- ❒ Сколько новых компьютеров нужно добавить в сеть (и нужно ли это делать)?
- ❒ Сколько новых устройств (например, принтеров) нужно добавить в сеть?
- ❒ Существует ли необходимость в обеспечении возможности последующего расширения? Если существует, то на сколько пользователей или устройств следует рассчитывать?
- ❒ Требуются ли какие-то необычные ресурсы (например, возможность подключения к сети Интернет отдельного пользователя или группы)?
- ❒ Кто отвечает за сопровождение сети и ее администрирование?

Естественно, вариантов ответов на эти вопросы бесчисленное множество, и в каждой ситуации может потребоваться информация в большем или меньшем объеме. В конечном итоге цель заключается в том, чтобы четко определить задачи, которые предстоит решить, и в полной мере понять ожидания вашего клиента от готовой сети. Именно ясное очерчивание целей поможет вам обеспечить соответствие потребностям клиента. Проблема, связанная с постановкой задачи, заключается в том, что сам клиент (в качестве клиента может выступать как сторонняя компания, так и начальник отдела той компании, в которой вы работаете) нередко плохо представляет себе, чего же он хочет. Возможно, вам просто заявят: "Хочу, чтобы все сотрудники компании (или отдела) находились в сети". Не забывайте о том, что ваш клиент обычно знает об организации сетей меньше, чем вы, так что вам, наверное, придется узнать некоторые подробности, и лишь после этого вы сможете представить конкретный план.

Оценка ресурсов

После того как вы узнали о требованиях, предъявляемых к будущей сети, необходимо провести оценку имеющихся аппаратных и программных ресурсов, с которыми вам предстоит работать. Помните, что многие пользователи из числа сотрудников компании или отдела уже имеют в своем распоряжении компьютеры. Иногда на них уже установлены сетевые адаптеры или сетевое программное обеспечение; возможно, они даже являются частью некоторой существующей сетевой инфраструктуры. Прежде чем излагать свои рекомендации по приобретению нового оборудования, важно выяснить, какая аппаратура уже используется. Например, предположим, что

у вас есть ряд отдельных персональных компьютеров на базе Windows 9x. Вполне вероятно, что вам придется заменить или модернизировать некоторые самые старые компьютеры, установить сетевые адаптеры на оставшихся и установить на компьютер, который предполагается сделать сервером, операционную систему Windows NT/2000 или NetWare. Вы должны учесть аппаратные, программные и сетевые ресурсы, а также возможности соединения.

Проверка аппаратного обеспечения

Если вы когда-нибудь сталкивались с минимальными системными требованиями, предъявляемыми новыми играми или пакетами программ для повышения производительности компьютера, вам известно, что программные средства предъявляют к аппаратному обеспечению системы некоторые требования. Компьютер должен соответствовать или превышать этот минимальный уровень, чтобы обеспечивать нормальную работу программного обеспечения. В условиях сети значимость этого фактора возрастает. Путем оценки имеющегося аппаратного обеспечения вы можете принимать обоснованные решения о том, какие компьютеры нужно заменить, какие модернизировать, какие добавить. Изначальное знание технических характеристик каждой системы может предотвратить появление серьезных проблем, связанных с производительностью или совместимостью в дальнейшем. Определение отдельных ключевых устройств облегчает задачу своевременного обновления драйверов. В отношении каждого компьютера вы должны будете собрать некоторые данные, например, такие:

- производитель и модель компьютера (например, Gateway Performa 1100);
- производитель и быстродействие процессора (например, Intel Pentium III 1,1 ГГц);
- объем установленной оперативной памяти (например, 256 Мбайт);
- производитель и объем каждого жесткого диска (например, C: Maxtor 30 Гбайт);
- подробная информация обо всех прочих установленных дисководах (например, CD-ROM, привод гибких дисков, дисководы Iomega);
- характеристики монитора (например, Gateway Vivitron21, 21 дюйм);
- характеристики видеокарты (например, Voodoo3 3Dfx 16 Мбайт);
- характеристики сетевого адаптера (если он установлен);
- перечислить все установленные периферийные устройства (например, принтеры или сканеры) и проверить наличие оригинальных установочных дискет или компакт-дисков для каждого из них;
- обозначить тип системной шины (например, EISA, ISA или PCI) и проверить, сколько разъемов на ней остаются незанятыми. Эта информация потребуется, если вы решите установить сетевой адаптер или модернизировать контроллер дисков.

Проверка программного обеспечения

Помимо регистрации данных об аппаратуре системы, отведите некоторое время на анализ применяемого в ней программного обеспечения. Эта информация может оказаться важной, т. к. она определяет аппаратную совместимость. Например, если в

ходе развертывания сети вы обновите все компьютеры, установив на них операционную систему Windows 2000, впоследствии может обнаружиться, что некоторые установленные на них программы (которые, вполне возможно, используются ежедневно) перестали работать. Это особенно опасно, если в компании или в отделе применяются заказные специально спроектированные или специализированные программы типа бухгалтерских баз данных. В условиях сети нормально работают очень немногие специализированные программы. В других случаях сетевой режим может быть не разрешен лицензионными соглашениями. Вероятно, вам придется связаться с производителем специализированных программ и узнать, как они поведут себя в условиях сети. Соберите следующие данные об операционной системе и каждом программном приложении:

- название программы;
- номер версии программы;
- наличие/отсутствие оригинальных установочных дискет или компакт-дисков для каждой программы;
- данные о лицензировании каждой программы (возможно, для того, чтобы пользоваться программой в сети, требуется ее обновление).

Проблемы, связанные с программной совместимостью, удивительным образом выйдут на поверхность, когда вы начнете вплотную знакомиться с теми программами, которые применяются различными пользователями. Например, в бухгалтерии используется WordPerfect, а в отделе сбыта — Microsoft Office. Вам придется обновить некоторые приложения, чтобы в масштабах всей сети ввести стандарт на какой-то один комплект программ. В свою очередь, эти действия могут создать необходимость дополнительного обучения пользователей, не умеющих работать с выбранным программным обеспечением.

Проверка возможности соединения

На сегодняшний день большинство сетей предусматривают какой-либо вариант подключения к сети связи, таким образом, обеспечивая возможность установления доступа к сети Интернет или к серверу удаленного доступа (RAS, Remote Access Server). *Сервер удаленного доступа* — это хост в локальной сети, в состав которого входят модемы и который обеспечивает подключение пользователей к сети через телефонные линии. Обратите внимание на телефонные линии, проведенные во всех задействованных офисах и вообще в местах размещения рабочих мест пользователей. Например, если компания или отдел располагает электронной телефонной сетью, то телефонные розетки должны быть в каждом офисе, но при этом вполне возможно, что они не способны обеспечить модемное соединение. Для передачи голоса и данных может потребоваться отдельная телефонная розетка. Аналогичным образом, цифровая телефонная связь (телефонная система для частного пользования) может вообще не поддерживать стандартные модемы. Короче говоря, вы должны проверить характеристики телефонных соединений.

Проверка ресурсов сети

В последнюю очередь следует оценить существующие сетевые ресурсы. Узнайте, есть ли распределительные панели, стенные розетки RJ-45 или BNC, ранее прове-

денные участки кабеля и все прочие элементы существующей инфраструктуры, которые вам могут пригодиться. Если компания или отдел уже располагает кабельной системой неэкранированной витой пары категории 5, причем она присутствует во всех помещениях (возможно, ее проводка была выполнена при постройке здания), это в значительной степени упростит физическое развертывание сетевой проводки (и снизит издержки на ее организацию). Чем выполнять проводку с нуля, проще добавить или изменить ее так, чтобы она смогла удовлетворить потребности ваших пользователей. Во многих случаях полезно получить комплект проектных планов, чтобы отследить существующую схему проводки и при необходимости сформировать новую.

На этом этапе стоит продумать физическую базу развертывания сети. В зависимости от размера помещения, количества пользователей и условий (офис или производство) вы можете выбрать, какую проводку нужно выполнить, и какой носитель (коаксиальный кабель или витая пара) лучше других подойдет в вашей ситуации.

Составление рабочего плана

Следующим этапом будет непосредственное планирование работ, совершенно необходимое для развертывания сети. Естественно, план будет начинаться с перечисления имеющихся ресурсов и подробного описания действий, выполнение которых требуется для достижения целей организации сети. Такой план может подразумевать модернизацию или замену существующих и установку новых компьютеров, оборудование этих компьютеров с расчетом на работу в сети, монтаж проводки, инсталляцию программного обеспечения и надлежащую настройку сети. В процессе планирования обычно рассматриваются вопросы временных рамок и финансирования. В большинстве случаев до начала работ этот план нужно представить клиенту на утверждение.

Работа в рамках бюджета

Самый масштабный технический проект абсолютно бесполезен, если для его реализации требуется слишком много денег. Если расходы, необходимые для выполнения проекта, не учтены в бюджете, никакие творческие усилия не смогут заставить проект работать. Прежде чем приступать к проекту, узнайте его бюджет. Ознакомьтесь с финансовыми границами проекта и не выходите за их рамки. Если вы считаете, что бюджет проекта нереалистичен, выскажите свое мнение сразу. Вы сможете изменить бюджет (или проект), сделав его более осуществимым.

Возможно, вы обнаружите, что практически аналогичную функциональность проекта можно обеспечить, заменив дорогостоящие компоненты более дешевыми. Впрочем, не стоит пользоваться нестандартными продуктами. В конечном итоге на ремонт и сопровождение вы потратите больше, чем сэкономите. Если вам приходится снизить параметры проекта до такого уровня, который не сможет обеспечить запланированную функциональность, но и в таких условиях проект выходит за рамки бюджета, придется известить руководство о необходимости пожертвовать низкоприоритетными функциями. Лучше предусмотреть устойчивый комплект базовых функций и отказаться от менее важных возможностей, чем экономить на всех компонентах проекта.

Типы сетей

При проектировании или модернизации сети вы должны решить, будет ли она одноранговой или основанной на сервере. Это решение очень важно, т. к. оно определяет количество пользователей в сети, ее расширяемость, безопасность, бюджет, трафик и состав административного персонала. Обычно приходится изначально работать с сетями серверного типа. Тем не менее вы должны иметь представление о факторах, определяющих выбор того или иного типа сети.

Одноранговая сеть

Малые предприятия и группы, состоящие из нескольких пользователей, могут извлечь значительную выгоду из организации *одноранговой сети*. Эта схема предполагает равноправие всех пользователей сети и единые для всех права доступа ко всем компьютерам в рамках сети, при условии, что другие пользователи располагают коллективными ресурсами в сети. В одноранговой сети не предусматривается централизованное администрирование или сопровождение. Ответственность за работу сети распространяется на всех ее участников, и именно отдельные пользователи определяют, какие данные или ресурсы, расположенные на их компьютерах, могут использоваться коллективно. Для некоторых предприятий, которые не могут позволить себе нанять штатного сетевого администратора, это может оказаться большим плюсом.

Тем не менее у одноранговой сети есть свои недостатки. Все компьютеры и ресурсы должны постоянно работать. Например, если пользователь с лазерным принтером выключит свой компьютер, все остальные участники сети не смогут пользоваться этим лазерным принтером. Помимо этого, если, скажем, на одном компьютере произойдет перезагрузка, а в это время к его ресурсам будет пытаться обратиться другой участник сети, соединение между ними будет разорвано. Производительность также ограничена. Если какой-то пользователь обращается к ресурсам, расположенным на вашем компьютере, он потребляет мощности вашего процессора. Таким образом, при обращении к вашему компьютеру любого другого пользователя его производительность снижается. Одноранговые сети, как правило, не подходят для групп численностью более десяти человек.

Сети на основе сервера

В *сети на основе сервера* ресурсы обычно сосредоточены на нескольких основных компьютерах, и к ним могут обращаться многие клиенты. Например, один сервер управляет всеми принтерами, другой сервер управляет всеми файлами и т. д. Так как серверы редко выключаются (в идеале они вообще не должны выключаться), доступность ресурсов в сети всегда сохраняется. Поскольку клиенты могут обращаться к серверам, но не к системам других пользователей, производительность серверов обуславливается только сетевым трафиком (производительность рабочих станций остается неизменной). Серверные сети характеризуются масштабируемостью. По мере увеличения сетевого трафика серверы могут подвергаться модернизации (или увеличиваться в количестве).

Централизованный характер серверных сетей делает их более защищенными, чем одноранговые сети. В одноранговой среде все ресурсы совместно используются всеми участниками сети. Например, если бухгалтерия делает коллективным каталог, в котором хранятся файлы с данными об окладах, к ним могут обращаться все уча-

стники сети. Это, безусловно, небезопасно. С другой стороны, в серверных сетях применяются учетные записи и права доступа, так что отдельные пользователи (и группы пользователей) могут обращаться к определенным файлам и каталогам, не делая эти данные доступными всем участникам сети.

Гибриды

Одноранговый и серверный принципы, естественно, можно сочетать. Многие небольшие компании, планирующие в будущем расширяться, организуют одноранговую сеть для обслуживания нескольких пользователей, и одновременно устанавливают специальный компьютер, выполняющий функции файлового/печатного сервера. Таким образом, для обращения к файловому/печатному серверу потребуется учетная запись и права доступа, в то время как обращение к другим компьютерам-участникам сети будет осуществляться без ограничений. По мере развития сети и роста ее трафика пользователей можно перевести с одноранговой сети на одну из более традиционных серверных архитектур (шинную, звездообразную или кольцевую), учитывая их наряду с новыми пользователями.

Топология и архитектура

Разобравшись с типом сети, вы можете определиться с выбором подходящей сетевой топологии: шинной, кольцевой или звездообразной (все эти топологии подробно *рассматриваются в гл. 2*). *Шинную топологию* часто называют "линейным каналом", т. к. она предполагает подключение компьютеров от одного к другому. Она состоит из одного кабеля — *магистрали* (ее также называют транком или сегментом), которая соединяет все компьютеры в сети через единую шину. Это простейший и самый распространенный метод организации в сеть относительно небольшого количества компьютеров Ethernet. Так как данные отсылаются в цельную сеть в форме электронного сигнала, они проходят из одного конца кабеля в другой. Если разрешить сигналу непрерывно продолжаться, он начинает отражаться по кабелю во все стороны, не позволяя отсылать сигналы другим компьютерам. Таким образом, после достижения сигналом целевого адреса назначения его необходимо остановить. Для предотвращения отражения сигналов на обоих концах кабеля устанавливается компонент под названием оконечной нагрузки. Он поглощает свободные сигналы. В результате поглощения сигналов кабель освобождается, и все остальные компьютеры получают возможность отсылать данные.

В *звездообразной топологии* сегменты кабеля, отходящие от каждого компьютера, подключаются к центральному компоненту — *концентратору* (при подключении групп компьютеров также может применяться коммутатор). Концентраторы (или коммутаторы) могут группироваться и обеспечивать работу в сети большого количества систем. На рис. 21.1 показана простая сеть, в которой две рабочие станции и сервер подключены к концентратору в рамках звездообразной топологии. С передающего компьютера сигналы через коммутатор поступают на все компьютеры в сети. Эта топология появилась на заре вычислительной техники, когда компьютеры подключались к центральной универсальной вычислительной машине. Звездообразная топология обладает преимуществом, которое заключается в централизации ресурсов и управления, и часто применяется в сетях Ethernet 10/100/1000 (принципы Ethernet *рассматриваются в гл. 2*). Но поскольку каждый компьютер подключается к центральной точке, для организации этой топологии применительно к крупной сети требуется большое количество кабелей. В случае неисправности центральной точки

(например, концентратора) из строя выходит вся сеть (более подробно о концентраторах, коммутаторах и других соединяющих устройствах вы можете узнать из *гл. 13 и 14*).

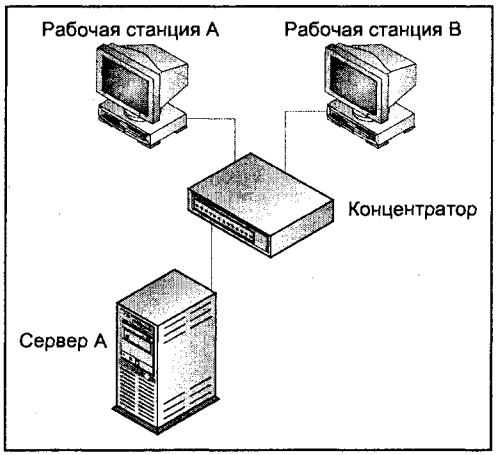


Рис. 21.1. Простая сеть с двумя компьютерами и сервером

Кольцевая топология (почти всегда применяемая для организации сетей типа маркерного кольца) подразумевает подключение компьютеров к одному круговому кабелю. В отличие от шинной топологии, здесь отсутствуют терминированные концы. Сигналы проходят по контуру в одном направлении транзитом через все компьютеры, которые могут выполнять функции повторителя, усиливая сигнал и переправляя его к следующему компьютеру. Неисправность одного компьютера может оказать влияние на работоспособность целой сети. На практике кольцевая топология напоминает звезду, в которой все компьютеры подключаются к центральной точке — она называется модулем многоточечного доступа (MAU, Multipoint Access Unit). Такой "контур" формируется схемой внутри MAU, причем несколько устройств MAU можно сгруппировать, в результате чего они обеспечивают работу большего количества компьютеров. Сети на базе кольцевой топологии обладают превосходными возможностями, связанными с самодиагностикой (архитектура маркерного кольца *рассматривается в гл. 2*).

Варианты беспроводной связи

Подавляющее большинство сетей работают на основе одной из форм физического кабеля, по которому осуществляется передача данных, но бывают случаи, когда кабель не является приемлемым решением. Зачастую конструкция здания оказывается плохо приспособленной для прокладки новых кабелей. В других ситуациях пользователю может потребоваться такая степень мобильности, достичь которую посредством кабеля не представляется возможным. Методики беспроводного доступа помогают упростить сложные вопросы проводки кабелей и обеспечить мобильность пользователей (принципы беспроводной связи *представлены в гл. 6*).

Беспроводные сети реализуются посредством беспроводной *точки доступа* (WAP, Wireless Access Point — не путать с беспроводным прикладным протоколом WAP, применяемым в беспроводных устройствах), которая выполняет функцию приемо-

передатчика, обеспечивающего соединение с кабельной сетью. Одна или несколько рабочих станций с беспроводными сетевыми адаптерами могут обмениваться данными с WAP, тем самым, получая доступ к остальной части сети (как показано на рис. 21.2). При необходимости расширенного диапазона (например, для повышения степени мобильности) есть возможность установки нескольких беспроводных точек доступа в разных местах в пределах сети. При этом пользователи могут перемещаться между смежными точками доступа.

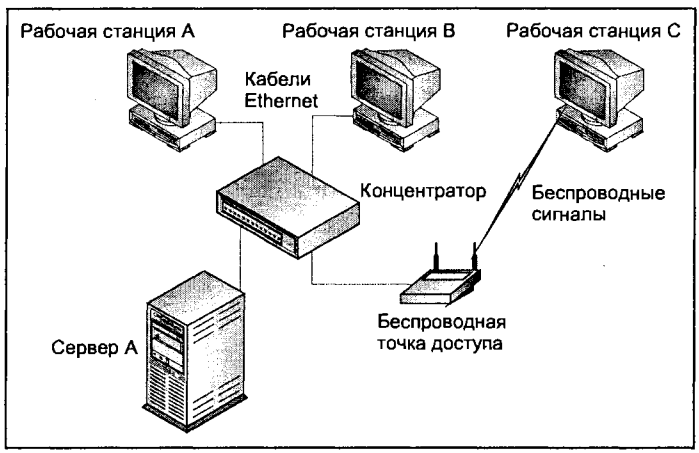


Рис. 21.2. Простейшая сеть с поддержкой беспроводной связи

Общие рекомендации

Вы должны понять, что не существует какого-то единственно "правильного" способа развертывания сети. Вариантов сетевых конструкций столько, сколько есть проектировщиков. Тем не менее некоторые инструкции общего характера помогут вам направить вашу новоиспеченную сеть по верному пути развития. Нижеследующая анкета упростит принятие решения о том, какой тип сети — одноранговый или серверный — вам лучше всего подойдет, сформирует общее представление о том, какую роль в вашей сети будут выполнять серверы, и определит подходящую топологию. Просто пометьте подходящий ответ на каждый вопрос, а затем подсчитайте результаты — наиболее часто встречающийся ответ, как правило, оказывается оптимальным решением.

- ❒ Сколько (приблизительно) пользователей должна обслуживать ваша сеть (и сколько их будет в ближайшем будущем)?
  - *0–10.* Воспользуйтесь одноранговой схемой.
  - *11+.* Воспользуйтесь серверной схемой.
- ❒ Существует ли необходимость в ограничении или регулировании доступа к данным и ресурсам вашей сети на основании распространенной схемы обеспечения защиты?
  - *Нет.* Воспользуйтесь одноранговой схемой.
  - *Да.* Воспользуйтесь серверной схемой.

- ❒ Какие функции будут выполнять компьютеры, размещенные в сети?
  - *Клиент/сервер.* Воспользуйтесь одноранговой схемой.
  - *Клиент.* Воспользуйтесь серверной схемой.
  - *Сервер.* Воспользуйтесь серверной схемой.
- ❒ Будет ли пользователям сети предоставлена возможность собственными силами решать задачи, связанные с администрированием и управлением?
  - *Нет.* Воспользуйтесь серверной схемой.
  - *Да.* Воспользуйтесь одноранговой схемой.
- ❒ Будет ли пользователям сети предоставлена возможность делать свои ресурсы коллективными и устанавливать другие сетевые политики для собственных компьютеров?
  - *Нет.* Воспользуйтесь серверной схемой.
  - *Да.* Воспользуйтесь одноранговой схемой.
- ❒ Будет ли в вашей сети работать администратор, ответственный за установление сетевых политик и полномочий?
  - *Нет.* Воспользуйтесь одноранговой схемой.
  - *Да.* Воспользуйтесь серверной схемой.
- ❒ Будут ли в вашей сети присутствовать центральные серверы?
  - *Нет.* Воспользуйтесь одноранговой схемой.
  - *Да.* Воспользуйтесь серверной схемой.

Если вы предпочли организовать серверную сеть, нижеследующие вопросы помогут вам спрогнозировать и решить вопросы, связанные с нагрузкой и расположением, которые довольно часто возникают при организации серверной среды.

- ❒ Отметьте задачи, которые должны решать ваши серверы:
  - обмен информацией;
  - базы данных;
  - печать;
  - дублирование/резервирование;
  - электронная почта;
  - пользовательские каталоги;
  - приложения;
  - факсимильные сообщения;
  - обычное хранение данных.
- ❒ Будут ли в сети присутствовать серверы со специализацией на выполнении определенных задач (например, Web- или FTP-сервер)?
  - Да.
  - Нет.

- ❒ Сколько (приблизительно) серверов присутствует в вашей сети в настоящее время (и сколько, как вы предполагаете, их будет в общей сложности)?
  - 0–5.
  - 6–10.
  - 11–50.
  - 51–100.
  - 100+.
- ❒ Будут ли сетевые серверы расположены в одном месте или рассредоточены по разным местам?
  - Будут централизованы.
  - Будут рассредоточены (почему?).
- ❒ Будут ли некоторые сетевые серверы расположены в защищенном месте?
  - Да.
  - Нет (почему?).

Теперь самое время определиться с топологией сети. Если вам не удается отдать предпочтение одному типу топологии и отказаться от другого, нижеследующие вопросы вам помогут.

- ❒ Сколько (приблизительно) пользователей должна обслуживать ваша сеть (и сколько их будет в ближайшем будущем)?
  - *0–10.* Воспользуйтесь шинной топологией (хотя подойдет и любая другая).
  - *11+.* Воспользуйтесь звездообразной или кольцевой топологией.
- ❒ Является ли производительность сети в реальном времени фактором, влияющим на выбор сетевой топологии?
  - *Нет.* Подойдет любая топология.
  - *Да.* Временные характеристики кольцевых станций предсказуемы, так что следует выбрать кольцевую топологию.
- ❒ Является ли автоматический поиск неисправностей значимым фактором?
  - *Нет.* Подойдет любая топология.
  - *Да.* Кольцевая топология обнаруживает установленные/демонтированные станции, так что следует выбрать кольцевую топологию (если этот вариант сочетается с другими решениями, принятыми на основе представленных здесь вопросов).
- ❒ Является ли простота обнаружения неисправностей значимым фактором?
  - *Нет.* Подойдет любая топология.
  - *Да.* Звездообразная топология предусматривает простоту соединений и перекрестных межсоединений станций.
- ❒ Можете ли вы заключить, что существующий план физического размещения компьютера и рабочая площадь помещения естественным образом приспособлены к определенной топологии?
  - *Нет.*
  - *Да* (к какой топологии?)

- Является ли простота перестройки структуры значимым фактором?
  - *Нет.* Подойдет любая топология.
  - *Да.* Звездообразная топология предусматривает простоту соединений и перекрестных межсоединений станций.
- Можете ли вы заключить, что существующую проводку в ваших помещениях можно приспособить к организации новой сети?
  - Нет.
  - Да (к какой топологии?)

Примечание

Естественно, представленные здесь вопросы — это лишь обобщенные инструкции, и в процессе принятия решений вы можете руководствоваться любыми другими значимыми факторами.

Выбор носителя

Теперь, когда вы определились с физической и логической схемами сети, самое время выбрать тип проводки (носителя). Это решение имеет большое значение, т. к. на проведение кабеля в здании затрачиваются большие усилия. Издержки возрастают еще больше, если возникает необходимость замены неподходящей или несоответствующей проводки. Носитель должен подходить не только к типу вашей сети, но и к определенным требованиям ее расположения. Например, если несколько рабочих станций расположены в производственной среде, где генерируются существенные электрические помехи, может потребоваться оптоволоконный кабель, не подверженный влиянию электрических сигналов. Для сравнения, простая витая пара (или экранированная витая пара), как правило, подходит только для офисной среды (прокладка кабеля *рассматривается в гл. 8*).

Другой аспект сетевых носителей имеет отношение к возможности последующего расширения сети. Применение минимального кабеля в условиях сегодняшнего трафика, вероятно, поможет сэкономить средства, но если количество пользователей и объем трафика возрастут, проводка может оказаться абсолютно несоответствующей новым требованиям, и из-за этого вы будете вынуждены провести трудоемкую и дорогостоящую процедуру повторного монтажа кабеля. Например, предположим, что вы решили проложить в небольшой сети неэкранированную витую пару категории 3. Естественно, этот кабель сможет обеспечить работу нескольких рабочих станций, но ограничение скорости передачи данных в сети будет составлять 10 Мбит/с. Через несколько лет количество рабочих станций в сети может резко увеличиться, и сеть с такой скоростью передачи будет работать очень медленно. Если же вы подготовитесь к такому развитию событий и сразу проведете неэкранированную витую пару категории 5 (или кабель с еще более прогрессивными характеристиками), вы сможете довести скорость передачи данных в сети до 100 Мбит/с и выше. Причем сделать это можно будет в любой момент и переделывать для этого всю проводку в здании не понадобится. Чтобы такая возможность появилась, достаточно лишь немного увеличить расходы на кабель. Сегодня появляется все большее количество решений, предполагающих применение беспроводных сетевых адаптеров и точек

доступа, предназначенных для ситуаций, когда провести постоянный кабель между компьютером и концентратором (или коммутатором) физически сложно.

Исследования показали, что более чем в 80% всех сетей применяется неэкранированная витая пара в условиях звездообразной топологии Ethernet. Так как большая часть издержек на проводку кабеля связана с работой, довольно часто разница в цене между неэкранированной витой парой категории 3 и аналогичным кабелем категории 5 (или даже более высоких классов типа категорий 6 и 7) оказывается незначительной. В большинстве новых сетевых схем применяются кабели категории 5 или выше, поскольку они поддерживают скорость передачи до 100/1000 Мбит/с. Например, категория 6 позволяет немедленно реализовать скорость в 100 Мбит/с и обновить это решение до 1000 Мбит/с впоследствии. Впрочем, неэкранированная витая пара подходит не для всех сетевых решений. Если вы не можете определиться с выбором того или иного сетевого носителя, нижеследующая серия вопросов поможет определить тот носитель, который окажется оптимальным именно для вашей ситуации.

- ❒ Являются ли легкость поиска неисправностей и дешевизна обслуживания/обновления кабеля значимыми факторами?
  - *Нет.* Подойдет любой кабель.
  - *Да.* Неэкранированную (а также экранированную) витую пару можно приобрести всегда и недорого.
- ❒ Не превышает ли максимальное расстояние от сетевых компьютеров до кабельной или распределительной панели 100 м (328 футов)?
  - *Нет.* Неэкранированная витая пара лучше подходит для небольших расстояний.
  - *Да.* Для значительных расстояний лучше подходит коаксиальный или оптоволоконный кабель.
- ❒ Является ли легкость перекомпоновки значимым фактором?
  - *Нет.* Подойдет любой проведенный кабель.
  - *Да.* Неэкранированная витая пара предполагает применение коннекторов RJ-45, которые при необходимости можно переместить.
- ❒ Присутствует ли в вашей сети проводка экранированной витой парой?
  - *Нет.* Подойдет любой проведенный кабель.
  - *Да.* Экранированной витой парой следует пользоваться, если она уже проведена в сети, или если проблемы, связанные с электрическими шумами, делают ее применение необходимостью.
- ❒ Можете ли вы заключить, что топология или сетевой адаптер, задействованные в вашей сети, требуют применения экранированной витой пары?
  - *Нет.* Решение о выборе экранированной витой пары (в противоположность неэкранированной) следует обосновывать другими факторами.
  - *Да.* Если сетевой адаптер станции требует применения экранированной витой пары, нужно проводить именно ее.

- ❒ Есть ли необходимость в применении кабеля, который по степени устойчивости к электромагнитным помехам или радиопомехам превышает показатели неэкранированной витой пары?
  - *Нет.* Подойдет неэкранированная витая пара (следует рассмотреть другие факторы).
  - *Да.* При наличии электромагнитных помех или радиопомех следует воспользоваться экранированной витой парой, коаксиальным или оптоволоконным кабелем.
- ❒ Нужен ли вам кабель, абсолютно устойчивый в отношении электромагнитных помех или радиопомех?
  - *Нет.* Подойдет любой проведенный кабель.
  - *Да.* Полную невосприимчивость к электромагнитным помехам и радиопомехам обеспечивает только оптоволоконный кабель.
- ❒ Присутствует ли в вашей сети проводка коаксиального кабеля?
  - *Нет.* Подойдет любой проведенный кабель.
  - *Да.* Если в сети уже проведен коаксиальный кабель, пользоваться следует именно им.
- ❒ Если у вас оборудование, которое в настоящее время требует применения сетевых адаптеров маркерного кольца (например, универсальная вычислительная машина IBM) или каким-либо другим образом применяет маркерное кольцо?
  - *Нет.* Подойдет любой проведенный кабель.
  - *Да.* Для обеспечения работы существующей инфраструктуры следует выбрать кольцевую архитектуру.
- ❒ Ваша сеть очень мала (в ней 10 или меньше компьютеров)?
  - *Нет.* Подойдет любой проведенный кабель.
  - *Да.* В вашей ситуации подойдет коаксиальный кабель (при шинной топологии) или неэкранированная витая пара (при звездообразной топологии).
- ❒ Нужен ли вам сетевой кабель, в сравнительной степени защищенный от прослушивания или разведывательного оборудования для сбора данных?
  - *Нет.* Подойдет любой проведенный кабель.
  - *Да.* Высокая степень защиты характерна для оптоволоконного кабеля.
- ❒ Нужны ли вам скорости передачи данных, превышающие возможности медных носителей?
  - *Нет.* Подойдет любой проведенный кабель.
  - *Да.* Оптоволоконный кабель предусматривает очень высокие скорости передачи данных.
- ❒ Испытывают ли пользователи вашей сети потребность в физическом перемещении своих компьютеров в течение рабочего дня?
  - *Нет.* Подойдет любой проведенный кабель.
  - *Да.* Возможность свободного перемещения в рамках заданного диапазона обеспечивается беспроводными сетевыми компонентами.

- Есть ли какие-то физические ограничения, которые делают кабельное подключение компьютеров к сети очень сложной (или невозможной) задачей?
  - *Нет.* Подойдет любой проведенный кабель.
  - *Да.* Беспроводные сетевые компоненты компенсируют недостатки кабеля.

Составление логических и физических карт

На этом этапе вы можете приступать к составлению схемы сети на бумаге. Как правило, этот процесс предполагает создание физической и логической схем сети, которые должны учитывать всех ее пользователей и все периферийные устройства. Физическая схема обычно представляет собой карту, на которой приводится схема здания, расположение каждого аппаратного компонента, а также общий план проводки кабеля между сервером, каждым из компьютеров и периферийными устройствами. Пример схемы простейшей сети показан на рис. 21.3. Если некоторая сетевая инфраструктура уже имеется, ее также необходимо указать в схеме. Вам следует также создать логическую схему сетевой топологии (например, шинной или звездообразной) и включить в нее сервер(ы), каждый компьютер и все периферийные устройства. Такая документация не только оказывается полезной при развертывании

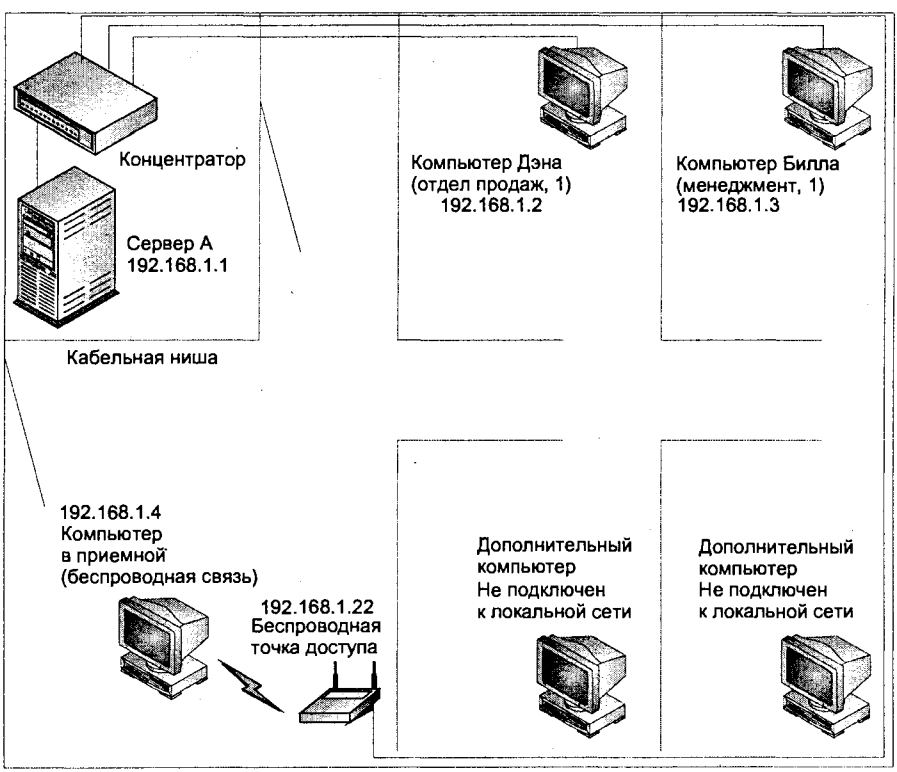


Рис. 21.3. Физическая карта помогает определить расположение и адреса всех сетевых устройств

сети. Она приобретет огромную ценность при необходимости поиска неисправностей или расширения сети. Эта документация также поможет другим техническим специалистам получить представление о сети.

Определение возможных узких мест

Если существующая сеть тщательно проектируется в расчете на выполнение текущих задач, старайтесь прогнозировать новые требования, предъявляемые к сети вашим проектом. Например, если маршрутизатор или другое устройство уже работает почти на максимальном уровне использования, то в вашем проекте придется предусмотреть модернизацию этих устройств. Что касается серверных приложений, то здесь может потребоваться планирование обновления оперативной памяти или установки второго (третьего) процессора.

Не совершайте ошибок, недооценивая влияние вашего проекта на сеть в целом. Если перед вами стоит задача выполнения всестороннего анализа, направленного на определение текущих рабочих условий производственной сети, выполните его, и только потом приступайте к проектированию. Но еще до проведения анализа должны быть выявлены те области в рамках сети, на которые ваш проект окажет наибольшее воздействие. Например, если вы планируете установить на существующий сервер новое серверное приложение, вам должно быть известно, что это приложение предъявляет некоторые требования к процессору, памяти и каналу, на котором установлены диски. Сетевой трафик, связанный с использованием приложений, также вырастет. В ходе проведения первоначального анализа сосредоточиться нужно именно на таких областях. Так вы определите, какую нагрузку испытывают все задействованные устройства.

Один из способов прогнозирования воздействия вашего проекта на сеть предусматривает тщательный анализ функционирования этого проекта после его реализации в качестве экспериментального. Чтобы получить четкое представление о требованиях, предъявляемых вашим проектом к уровню производительности, пользуйтесь инструментальными средствами типа Performance Monitor и сетевыми анализаторами пакетов.

Примечание

Даже если ваш бюджет не позволяет модернизировать компоненты, которые должны работать на уровне, превышающем их возможности, обозначьте в вашем проекте такие перегруженные области (некоторые части вашей сети, возможно, находятся вне рамок ответственности вашего отдела).

Критический анализ рабочего плана

После завершения написания плана самое время представить его клиенту. Встречи, направленные на его обсуждение, часто принимают неформальный характер, но они всегда сохраняют свою значимость. Просматривая план, ваш клиент имеет возможность задать вопросы и убедиться в том, что предполагаемая сеть отвечает его потребностям. В процессе такого ознакомления обычно всплывают недостатки и недосмотры, а все возникшие в последний момент идеи и требования можно обсудить до того, как деньги будут потрачены. Вероятно, вам придется вернуться к планированию и откорректировать некоторые решения, что позволит решить все трудности

и уложиться в ограниченные рамки бюджета, а после этого провести просмотр плана еще раз. Довольно часто перед тем, как утверждается окончательный план сети, он проходит через несколько стадий критического анализа (этих стадий тем больше, чем крупнее и сложнее планируемая сеть). После утверждения вашего плана клиентом (когда спорных вопросов не остается) вам нужно только реализовать его.

Осуществление рабочего плана

Следующим этапом является развертывание сети в соответствии с подготовленным планом. Если проведена достаточно серьезная работа, связанная с планированием, вы должны знать, какое аппаратное и программное обеспечение следует заказать, и понимать, какую проводку нужно выполнить для обеспечения работы каждого устройства. Типичная реализация, как правило, предполагает прокладку кабелей, размещение каждого из устройств, их соединение, установку программного обеспечения и настройку сети.

Проводка кабеля

На этом этапе вы (или профессиональная команда) должны выполнить физическую проводку. Приступать к проводке лучше всего тогда, когда заказ на все остальное оборудование находится на выполнении. Практически во всех случаях существует необходимость проводки через стены, потолки и полы. Для примера мы рассмотрим монтаж кабельной системы Ethernet категории 5. Простейший способ развертывания сети в условиях небольшого офиса предполагает применение физической звездообразной топологии. Центром любой звездообразной топологии является наборная панель. Она представляет собой ряд гнездовых коннекторов RJ-45 с терминалами для подключения проводов.

На среднестатистической панели присутствует 12 или более коннекторов RJ-45, причем каждый коннектор содержит восемь точек соединения — по одному выводу на каждый из восьми проводов витых пар. В большинстве случаев в соединениях применяется цветовое кодирование, упрощающее процесс монтажа. Смысл заключается в том, чтобы установить наборную панель (панели) в одном месте. Часто она монтируется в специальной кабельной нише или рядом с концентратором (как правило, недалеко от сервера) так, чтобы установление соединений с сетью не представляло проблем. Чтобы подключить сетевой адаптер компьютера к кабелю, вы должны установить розетку категории 5 рядом с концентратором и на концах всех кабелей. Путем подобной конфигурации вы получаете возможность без труда отключать и повторно подключать рабочие станции (через близлежащую стенную розетку), а также выполнять быструю перенастройку компьютеров на наборной панели.

Например, предположим, что компьютер перестал работать. Вы можете с легкостью отключить компьютер от одной стенной розетки и подключить его к другой, свободной розетке. Если в этом случае компьютер заработает, вы будете знать, что проблема относится к проводке, наборной панели или концентратору/коммутатору. В качестве другого примера предположим, что из строя вышел порт концентратора/коммутатора. С помощью наборной панели вы без труда сможете на время подключить компьютер к другому, работающему порту концентратора/коммутатора. Все это можно сделать, не нарушая постоянную структуру кабелей, проведенных через стены, потолки и полы.

Примечание

Не забывайте, что все кабели, пролегающие над потолком или под полом, должны соответствовать местным строительным нормам и правилам обеспечения противопожарной безопасности. Там, где это необходимо, следует проводить пленумный кабель.

Монтаж устройств

После завершения проводки и определения местоположения каждого устройства нужно приступать к подключению устройств. Соединения должны быть прямыми. Они выполняются путем подключения сравнительно короткого фрагментного кабеля между портом сетевого адаптера и стенной (или напольной) розеткой RJ-45. В случае применения концентратора вам понадобится короткий соединительный кабель. С его помощью вы сможете подключить наборную панель к соответствующей розетке на концентраторе. Другими словами, чтобы подключить компьютер к сети, вы должны подсоединить порт концентратора к стенной розетке RJ-45. Посредством кабеля эта розетка подключена к другой розетке RJ-45, расположенной рядом с соответствующим компьютером. Другой соединительный кабель подсоединяет эту стенную розетку RJ-45 к сетевому адаптеру компьютера. На этом путь от компьютера к концентратору завершается. Затем с помощью отдельного соединения концентратор подключается к серверу (желательно, чтобы он был расположен неподалеку).

Вопросы программного обеспечения

После монтажа аппаратной части вы должны сосредоточиться на программном обеспечении. Как правило, на этом этапе происходит установка приложений, работающих на сервере и клиентских компьютерах, драйверов, редиректоров и т. п. Затем необходимо настроить сеть, определив в ней права доступа и коллективные ресурсы (т. е. сформировать систему защиты), чтобы пользователи могли обращаться к серверу, обмениваться сообщениями и т. д.

Практические примеры

Теперь, когда вы познакомились с некоторыми основными принципами сетевого планирования и связанными с ним проблемами, самое время рассмотреть некоторые практические примеры. Вы уже могли убедиться в том, что не существует никакого "правильного" способа проектирования или реализации сети, но в представленных ниже примерах на практике воплощаются сформулированные к настоящему моменту основные идеи и сводятся воедино многие проблемы, рассмотренные в предыдущих главах.

Пример: подключение нового компьютера

Проектируя сеть для некой производственной компании, вы учли возможность возникновения необходимости в подключении к ней дополнительных компьютеров. Коммерческий директор, получив дополнительный компьютер, неожиданно принес его вам. Он надеется, что вы подключите его к сети как можно быстрее, чтобы новый сотрудник смог приступить к исполнению своих обязанностей через два дня.

В этом компьютере нет сетевого адаптера. Вам нужно будет установить адаптер, а затем подключить новый компьютер к существующей сети (подробное изложение процессов монтажа и поиска неисправностей сетевых адаптеров содержится в *гл. 10*).

В первую очередь настройте новый компьютер и убедитесь в том, что он находится в нормальном, рабочем состоянии. Если операционная система допускает такие действия, проведите проверку на предмет свободных прерываний. Вполне вероятно, что эта информация потребуется при настройке сетевого адаптера. Отметьте объем установленной оперативной памяти и емкость диска (возможно, эти параметры окажутся недостаточными для работы в сети или для ресурсоемких приложений). После этого закройте все работающие программы и выключите компьютер. Отсоедините все кабели и откройте системный блок. Посмотрите, есть ли на материнской плате свободные разъемы шин. При наличии незанятого слота PCI именно на нем следует остановить выбор. Иначе выберите разъем ISA.

Достаньте сетевой адаптер, совместимый с незанятым разъемом шины, сетевой архитектурой (например, Ethernet или маркерное кольцо) и типом кабельных коннекторов (например, BNC или UTP), принятых в сети вашей компании. Не забывайте, что, если в существующей сети применяется неэкранированная витая пара с частотой 100 МГц и выше, сетевой адаптер должен уметь работать на такой скорости. Обычно в комплекте с сетевым адаптером поставляются и драйверы для вашей операционной системы (как правило, они записаны на дискетах или на компакт-дисках). Если на новом компьютере нет привода CD-ROM, придется скопировать драйверы на гибкие диски. Для этого вам понадобится компьютер с установленным приводом CD-ROM.

Установите сетевой адаптер в подходящий разъем шины и заново подключите все кабели системы. Включите компьютер и, после того как он обнаружит сетевой адаптер, установите последние версии драйверов. Прежде чем система получит возможность взаимодействия с сетью, в ней нужно установить подходящие протоколы обмена данными (IPX/SPX или TCP/IP). Обычно это программное обеспечение устанавливается через операционную систему. После монтажа и обнаружения сетевого адаптера, установки всех необходимых протоколов обмена данными и их привязки к адаптеру вы можете приступать к подключению сетевого кабеля к гнезду сетевого адаптера. Наконец, протестируйте выполненную сборку, запросив сетевые ресурсы методом вашей сети. Например, подтвердить наличие нового компьютера можно, поискав его имя в папке **My Network Places** (Мое сетевое окружение).

Пример: одноранговое решение

Здесь мы сталкиваемся с более сложной проблемой, требующей творческого подхода. Небольшая компания в Вермонте разрабатывает и производит наборы инструментов для постройки срубных домов. Владелец этой компании хочет спроектировать в ее помещениях сеть, способную обеспечивать работу 10 компьютеров и пользователей. В компании работают два специалиста по продажам, руководитель отдела, составитель проектов, художник-оформитель, производственный мастер, а также несколько сотрудников, не пользующихся компьютерами.

Компьютер, за которым работает владелец компании, оснащен операционной системой Windows 98, стандартным комплектом офисных приложений и популярной прикладной программой управления проектами. Руководитель отдела, на компьюте-

ре которого установлен тот же комплект офисных приложений, что и у владельца, печатает на лазерном принтере, подключенном непосредственно к компьютеру. Помимо прочих сотрудников, на фирме работает оператор системы автоматизированного проектирования, делающий чертежи изделий для работающих на производстве. На его компьютере установлена ОС Windows NT, а важнейшим для него является векторная программа автоматизированного проектирования, вывод из которой производится на рулонный плоттер, подключенный непосредственно к принтерному порту компьютера.

Оба специалиста по продажам имеют портативные компьютеры с операционными системами Windows 98, а работают они, главным образом, с приложениями, входящими в тот же самый офисный комплект приложений. Художник-оформитель, специализирующийся на компьютерной графике, создающий иллюстрации для каталогов и материалы для презентаций, пользуется компьютером Apple G3 с профессиональным компьютерным программным обеспечением и с тем же самым комплектом офисных приложений, которые установлены на компьютерах владельца и руководителя отдела. Ее компьютер выводит печатные материалы на цветной принтер PostScript с высоким разрешением, подключенный к стандартному порту. В конечном счете владелец хочет, чтобы все участники сети могли обмениваться файлами и пользоваться обоими принтерами. Он дал понять, что сеть, требующая высоких административных издержек, ему не нужна.

Вариант решения

В данном случае приемлемо множество решений, и ниже приводится лишь один набор рекомендаций. В первую очередь, т. к. владелец не желает рассматривать проектирование сети, которая потребует высоких административных издержек, наиболее оптимальным представляется решение организации одноранговой сети. Этот вариант является подходящим, т. к. участников сети не так уж много. Технически можно было бы применить серверный подход, но он предполагает администрирование сети, от которого владелец отказывается. Путем объединения в одноранговую сеть существующих компьютеров компании (а следовательно, организации совместного использования файлов и принтеров) и соединения компьютеров посредством неэкранированной витой пары Ethernet на скорости передачи данных 100 Мбит/с с применением стека TCP/IP достигается достаточная степень взаимодействия.

Совместное использование файлов и принтеров предоставляет пользователям возможность коллективного доступа к лазерному и цветному PostScript-принтерам, подключенным к существующим системам. Впрочем, вы можете предложить подключить эти принтеры к серверу печати Ethernet (такие устройства *рассматриваются в гл. 16*), который обеспечит возможность централизованного и автономного расположения принтеров. Таким образом, руководителю отдела и художнику-оформителю не придется постоянно держать свои компьютеры в работающем состоянии. Сервер печати подключается к порту концентратора или коммутатора Ethernet.

Обеспечение взаимодействия с системой Apple связано с некоторыми трудностями, но путем активации служб Apple на компьютере с Windows NT можно создать путь между художником-оформителем (применяющим операционную систему от Apple) и всеми остальными сотрудниками (пользующимися одной из двух сетевых операционных систем Windows).

Пример: соединение двух зданий

Здесь мы приведем третий пример, в котором рассмотрим вопросы дальнего соединения между зданиями. Небольшая маркетинговая компания арендует две группы помещений в зданиях *B* и *H* пригородного офисного комплекса. Коммерческие функции в компании выполняют 12 человек (в эту группу включается персонал и сотрудники бухгалтерии); все они работают в здании *B*. Творческие сотрудники (копирайтеры, оформители, а также люди, работающие в производственном отделе) в количестве 22-х человек сидят в здании *H*. Расстояние между зданиями *B* и *H* составляет 600 м (около 1970 футов).

Коммерческие сотрудники, размещающиеся в здании *B*, располагают коаксиальным каналом, проведенным пять лет назад, который объединяет их компьютеры в одноранговую рабочую группу. Творческие сотрудники в здании *H* работают на разнородных компьютерах (в числе которых есть и Apple Macintosh), не объединенных в сеть. Владельцы компании хотели бы организовать сеть, в которой должны участвовать компьютеры творческих сотрудников, а затем подключить эту сеть к сети, в которой работают коммерческие сотрудники. Они также хотят стандартизировать типы сетей, применяемые в обеих сетях, чтобы свести вопросы поиска неисправностей к минимуму. Какой тип сети следует реализовать? Какую архитектуру следует внедрить в обоих зданиях? Какая архитектура подходит для подключения сетей, находящихся в двух этих зданиях?

Примечание

Имейте в виду, что единственно "верного" решения этой проблемы не существует. Можно рассмотреть множество вариантов. Вполне вероятно, что вы найдете другое решение, которое окажется удачнее, чем то, что предлагаем мы.

Выбор типа сети

В данном случае предлагается серверная сеть. Дело в том, что общее количество рабочих станций (34) превышает рекомендуемый лимит в 10 компьютеров в рамках одноранговой сети. Так как в этой компании применяются разнородные компьютеры (PC и Macintosh), внедрить серверную сеть будет проще. Стандартизация и объединение всех компьютеров в сеть позволит компании прийти к более централизованной схеме администрирования. Организация серверной сети в данный момент поставит ее на путь централизации систем и предоставит возможность расширения в будущем. Одноранговая сеть, несомненно, ограничит возможности расширения. Поскольку компании нужна серверная операционная система, способная обслуживать как Macintosh, так и PC, вы можете остановить свой выбор на Microsoft Windows NT/2000 Server; впрочем, есть несколько других серверных операционных систем (например, NetWare), которые могут выполнять те же функции.

Архитектура в зданиях

В пределах обоих офисов мы рекомендуем Ethernet 100BaseT, т. к. это решение поддерживается всеми платформами, а его преимущества включают легкость поиска неисправностей и монтажа. Варианты маркерного кольца и ArcNet также допустимы; в то же время LocalTalk не отвечает предъявленным требованиями в силу своей медленной работы и трудностей, связанных с поиском плат LocalTalk.

Архитектура между зданиями

Для проведения кабеля между двумя зданиями рекомендуется оптоволоконный кабель Ethernet (называемый 100BaseF). На то есть две причины. Во-первых, оптоволоконный кабель обладает дистанционными возможностями, достаточными для покрытия расстояния в 600 м (около 1970 футов). Во-вторых, для соединения оптоволоконного кабеля, пролегающего из одного здания, с кабелем 100BaseT, смонтированного в другом здании, можно установить повторитель.

Организация доступа к сети Интернет

Современные сети редко существуют обособленно. Локальные сети зачастую объединяются в глобальные или подключаются к самой крупной глобальной сети — Интернету. Благодаря доступу к Интернету в рамках локальной сети пользователи сетей могут каждый день обмениваться электронной почтой и обращаться к ресурсам Интернета. В этой части главы вы ознакомитесь с вариантами предоставления доступа к Интернету из локальной сети и рассмотрите некоторые примеры такого доступа из простейшей сети.

Доступ к глобальной сети

У локальных сетей есть физические и дистанционные ограничения. Так как локальные сети не обеспечивают всех возможностей, необходимых для делового взаимодействия, требуется их подключение к другим типам сред. Только таким образом можно обеспечить наличие всех служб обмена информацией. С помощью устройств типа маршрутизаторов, а также провайдеров служб обмена информацией, можно расширять локальные сети от обслуживания ограниченной области до осуществления взаимодействия в глобальной сети, способной обеспечивать передачу данных в масштабах штата, страны и даже всего мира. Для пользователя глобальная сеть производит впечатление локальной сети. При грамотной реализации первая неотличима от второй. Для организации глобальной сети локальные сети соединяются с такими средами, как:

- сети с коммутацией пакетов;
- оптоволоконный кабель;
- ультракоротковолновые передатчики;
- спутниковые каналы;
- коаксиальные системы кабельного телевидения.

Эти каналы глобальной сети обычно арендуются у поставщиков услуг. Обмен информацией между локальными сетями обеспечивается посредством следующих технологий передачи:

- аналоговых;
- цифровых;
- коммутации пакетов.

Аналоговые соединения

Те самые коммутируемые телефонные линии (PSTN, Public Switched Telephone Network), которые применяются в телефонии, доступны и для компьютеров. Технология PSTN предусматривает голосовые коммутируемые линии, которые можно представить как один большой канал глобальной сети. Так как технология PSTN разрабатывалась главным образом для передачи речевой информации, скорость передачи данных может оказаться очень низкой, а качество — неустойчивым. Качество любого отдельно взятого сеанса связи обуславливается качеством коммутированных для него каналов. Впрочем, для обеспечения постоянных высокоскоростных соединений через телефонную систему существует технология DSL.

Цифровые соединения

В некоторых случаях аналоговые линии оказываются вполне достаточными. Тем не менее, когда организация вырабатывает такие объемы трафика, что время, затрачиваемое на его передачу, делает аналоговые соединения неэффективными и дорогостоящими, приходит время поиска альтернатив. Например, организации, для которых необходима более скоростная передача данных, могут остановить свой выбор на линиях цифровой передачи информации (DDS, Digital Data Service). Технология DDS предусматривает двухточечную синхронную передачу данных на скорости 2,4, 4,8, 9,6 или 56 Кбит/с. *Двухточечные цифровые каналы* — это специализированные каналы, выделяемые несколькими владельцами сетей связи. Владелец сети связи гарантирует дуплексную пропускную способность, устанавливая постоянный канал из каждой конечной точки в локальную сеть. Основным преимуществом цифровых каналов является то, что они обеспечивают передачу данных почти на 99%. Цифровые каналы существуют в нескольких разновидностях, включая DDS, T1 (1,544 Мбит/с), фракционный (Fractional) T1 (64-кбитовые приращения пропускной способности T1), T3 (45 Мбит/с), T4 и коммутируемые 56. Так как в DDS применяется цифровая передача данных, для функционирования этой службы модемы не нужны. Напротив, DDS осуществляет отсылку данных с моста на маршрутизатор посредством устройства, которое называется *модулем обслуживания канала и данных* (CSU/DSU, Channel Service Unit/Data Service Unit).

Это полная аналогия высокоскоростной кабельной службы. Сетевой адаптер компьютера (посредством протоколов TCP/IP) обменивается данными с кабельным модулем CSU/DSU (называемым *кабельным модемом*, хотя с технической точки зрения это название некорректно), подключенным к кабельной сети. Соединение является постоянным; оно предусматривает более высокую пропускную способность, чем простые коммутационные службы. Например, посредством кабельного модуля CSU/DSU (подобного изображенному на рис. 21.4) пользователь может без труда установить связь с Интернетом со своей локальной кабельной службы. Для обмена информацией с кабельным модемом, который затем связывается с кабельной сетью, компьютер пользуется сетевым адаптером Ethernet.

Мультиплексирование

В каналах T1 применяется *мультиплексирование*, поддерживающее совместное использование одной и той же физической сигнальной линии (линий) несколькими сигналами. Несколько сигналов, поступающих из различных источников, собираются

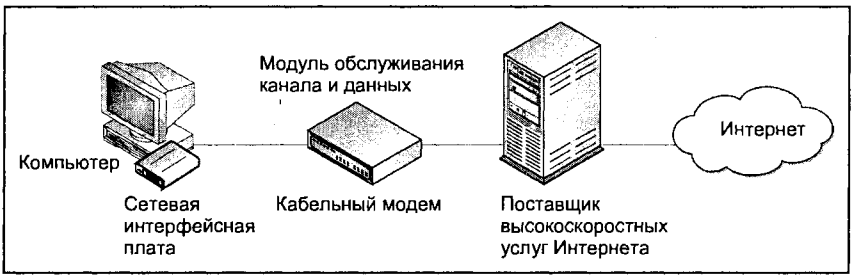


Рис. 21.4. Организация высокоскоростного доступа к сети Интернет с отдельного компьютера

вместе в устройстве под названием *мультиплексора*, а затем вводятся в один кабель для дальнейшей передачи. На принимающем конце данные демультиплексируются в свою исходную форму. Этот подход появился, когда телефонные кабели (каждый из которых мог передавать лишь один разговор) стали переполняться. Решение этой проблемы, названное *T-Carrier*, обеспечивает передачу многочисленных вызовов по одному кабелю телефонной системы.

Коммутация пакетов

Сети, в которых отправляемые пакеты, исходящие от множества различных пользователей, проходят по различным возможным путям, называются *сетями с коммутацией пакетов*. Это название обуславливается принятым в них способом пакетирования и маршрутизации данных. Пакетная технология характеризуется высокой скоростью, удобством и надежностью; по этой причине она используется для передачи данных на больших пространствах типа городов, штатов и государств. Исходный пакет данных разбивается на пакеты, каждый из которых снабжается меткой с адресом назначения и другой информацией. В результате появляется возможность отдельной сетевой пересылки этих пакетов. Затем пакеты ретранслируются по станциям в компьютерной сети, проходя по оптимальному в текущий момент маршруту между пунктами источника и назначения.

Коммутация каждого пакета происходит отдельно. Это означает, что два пакета, происходящие от одного пакета данных, могут идти совершенно разными путями, но в конечном итоге прийти в один и тот же пункт назначения. Пути для отдельных пакетов выбираются исходя из оптимального маршрута, доступного в любой текущий момент. Даже когда пакеты проходят по разным путям, и пакеты, составляющее одно сообщение, прибывают в пункт назначения не по порядку, принимающий компьютер сохраняет возможность осуществить повторную сборку исходного сообщения. Коммутаторы направляют пакеты по различным соединениям и магистралям, коммутаторы каналов в сети считывают каждый пакет и перенаправляют его по лучшему маршруту, доступному в данный момент. Размер пакетов невелик, так что повторная передача небольшого пакета оказывается операцией более простой, чем повторная передача крупного пакета (небольшие пакеты занимают коммутаторы в течение очень непродолжительного времени).

Виртуальные каналы

Во многих сетях с коммутацией пакетов применяются виртуальные каналы, в рамках которых задействуется ряд логических соединений между отправляющим и прини-

мающим компьютерами. Пропускная способность предоставляется такому каналу по требованию, т. е. за это ответственен не реальный кабель и не постоянный физический канал между двумя станциями. Такое соединение устанавливается после того, как оба компьютера обменялись информацией и достигли соглашения о параметрах связи, которые отвечают за установление и поддержание соединения. Эти параметры включают максимальный размер сообщения и путь прохождения данных. Виртуальные каналы могут сохраняться в течение длительности диалога (временные), или всего времени нахождения общающихся компьютеров в рабочем состоянии (постоянные).

Маршрутизаторы

Создание глобальной сети, по существу, сводится к объединению двух или нескольких локальных сетей. В условиях, когда в различных сегментах сети применяются различные протоколы и архитектуры, вам необходимо устройство, которое не только знает адрес каждого сегмента, но также может определить лучший путь отправки данных и фильтрации широковещательного трафика в локальный сегмент. Такое устройство называется *маршрутизатором* (более подробно они рассматриваются в *гл. 14*).

Маршрутизаторы работают на сетевом уровне модели OSI. Это означает, что они могут коммутировать и маршрутизировать пакеты по различным сетям. Для этого они организуют обмен специфическими протокольными данными между автономными сетями. Маршрутизаторы считывают сложную информацию, связанную с сетевой адресацией, которая размещается в пакете, и пользуются этой информацией для поднятия качества доставки пакетов. Маршрутизаторы применяются в сложных сетях, т. к. они обеспечивают более высокий уровень управления трафиком. Маршрутизаторы способны совместно пользоваться информацией, связанной с состоянием и маршрутизацией, и с ее помощью обходить стороной медленные или неисправные соединения.

Маршрутизаторы не взаимодействуют с удаленными компьютерами. Напротив, они понимают только номера сетей, которые позволяют им связываться с другими маршрутизаторами и локальными адресами сетевых адаптеров. Маршрутизация выполняется посредством таблиц маршрутизации, в которых указываются следующие данные:

- все известные сетевые адреса;
- инструкции по соединению с другими сетями;
- возможные пути между маршрутизаторами;
- эффективность отправки данных по этим путям.

Маршрутизатор пользуется своей таблицей маршрутизации для выбора оптимального маршрута при отправке данных, исходя из эффективности и наличия доступных путей. Когда маршрутизаторы принимают пакеты, направленные в удаленную сеть, они отсылают их тому маршрутизатору, который отвечает за сеть назначения. В этом заключается их преимущество, т..к. маршрутизаторы получают возможность сегментировать крупные сети на более мелкие, выполнять функции защитных ограждений между сегментами и предотвращать появление широковещательных штормов (широковещательные сообщения не подлежат перенаправлению).

Интернет-маршрутизаторы

В то время как пользователи отдельных компьютеров наслаждаются высокоскоростным доступом к Интернету через поставщика DSL или кабельных услуг, получение высокоскоростного обслуживания для многочисленных пользователей может быстро оказаться слишком дорогостоящим. В небольших сетях для подключения локальной сети к кабелю или модему DSL применяется интернет-маршрутизатор (рис. 21.5). С его помощью обеспечивается эффективное совместное использование высокоскоростной службы Интернета множеством пользователей локальной сети Ethernet. Маршрутизатор задействует лишь один IP-адрес, так что поставщику кабельных услуг или DSL он кажется одним устройством; тем не менее маршрутизатор может обеспечивать работу до 253 пользователей локальной сети. Некоторые интернет-маршрутизаторы предусматривают функции четырех- или восьмипортового коммутатора, брандмауэра, DHCP-сервера и т. д. Таким образом, компьютеры можно подключать непосредственно к маршрутизатору, а не к отдельному концентратору или коммутатору.

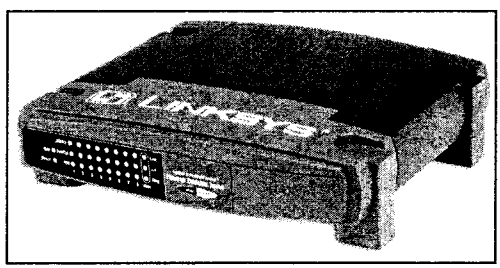


Рис. 21.5. Интернет-маршрутизатор Linksys BEFSR81 с восьмипортовым коммутатором

На рис. 21.6 изображена простейшая сеть со схемой совместного доступа к Интернету. В данном случае применяется однопортовый интернет-маршрутизатор (дело в том, что все имеющиеся рабочие станции подключены к коммутатору). Таким образом, порт локальной сети маршрутизатора просто подключается к свободному порту на коммутаторе. Порт глобальной сети маршрутизатора затем подключается к кабельному/DSL-модему, а тот, в свою очередь, подключается к телефонному или коаксиальному кабелю. Если маршрутизатор грамотно установлен и настроен, каждая рабочая станция в сети будет располагать доступом к Интернету. Более того, все рабочие станции, которые будут подключаться к локальной сети впоследствии, также получат доступ к Интернету.

Естественно, эта схема имеет и практические ограничения. Каждый пользователь, получающий доступ к Интернету, потребляет часть свободной пропускной способности кабельного/DSL-модема. Таким образом, получается, что чем больше пользователей обращаются к Интернету в одно и то же время, тем ниже результирующая производительность. Например, если один пользователь может загружать из Интернета файл на скорости 50 Кбит/с, то два пользователя могут выполнять эту операцию на скорости 25 Кбит/с, четыре пользователя — на скорости 12,5 Кбит/с и т. д. Если вам требуется дополнительная пропускная способность, то имеет смысл обновить каналы связи до более скоростных, например до T1, и задействовать профессиональные маршрутизаторы типа устройств Cisco или Bay Systems.

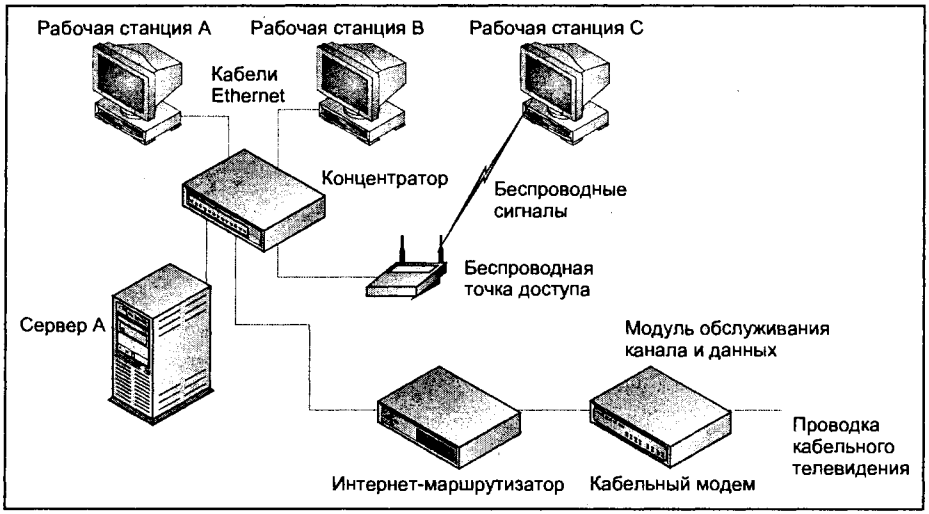


Рис. 21.6. Реализация высокоскоростного доступа к Интернету в простейшей сети

Практические примеры

Теперь, когда вы ознакомились с некоторыми принципами и проблемами, связанными с соединением сетей, пришло время рассмотреть несколько примеров. Вы уже могли убедиться в том, что не существует никакого "правильного" способа проектирования или реализации доступа к глобальной сети, но в представленных ниже примерах на практике воплощаются сформулированные к настоящему моменту основные идеи, воедино сводятся многие проблемы, рассмотренные в предыдущих главах.

Пример: доступ к Интернету из малого офиса/в домашних условиях

Небольшая дизайн-студия в Массачусетсе уже располагает несколькими компьютерами и серверами, объединенными в сеть; это позволяет дизайнерам и сотрудникам отдела продаж совместно пользоваться информацией и документами. Но только на одной из рабочих станций есть доступ к Интернету, который осуществляется через коммутационный модем. Компаньоны-распорядители полагают, что возможность доступа к Интернету будет полезной для фирмы, т. к. пользователи смогут обращаться к электронной почте и искать в Интернете новых производителей и новые материалы, когда это будет нужно. Впрочем, они не хотят устанавливать несколько модемов и выделять для коммутационного доступа несколько телефонных линий. Но они также не могут себе позволить высокоскоростные линии типа T1 (да и не нуждаются в них).

Высокоскоростной доступ к Интернету можно приобрести у местного поставщика кабельных услуг. Если установить кабельный модем, подключить его к интернет-маршрутизатору, а его, в свою очередь, подсоединить к открытому порту на сетевом коммутаторе, все рабочие станции, участвующие в сети, смогут обращаться к Ин-

тернету посредством единой учетной записи (которая допускает выделение отдельных адресов электронной почты для каждого пользователя).

Пример: соединение двух сетей

Издательство, занимающееся выпуском журналов и находящееся в Сиэтле, имеет филиалы во Флориде и Нью-Йорке. В каждом из этих офисов есть внутренние сети, автономные по отношению друг к другу. Эти сети были сформированы пять лет назад, причем каждая из них построена на основе коаксиальной линейно-шинной топологии, обеспечивающей движение трафика Ethernet со скоростью 10 Мбит/с. Взаимодействие между филиалами осуществляется по телефону и средствами курьерской службы Federal Express. Недавно компания приступила к проектам, в разработке которых принимают участие сотрудники из нескольких офисов. В каждом из офисов есть некоторые ресурсы, которых нет во всех остальных, а для выполнения текущих проектов требуются все эти ресурсы сразу. Во внутренних сетях часто случаются неисправности кабелей, и каждый раз при возникновении проблемы сеть целого офиса теряет работоспособность и остается в нерабочем состоянии вплоть до устранения неисправности (так происходит из-за шинной топологии).

Руководство хочет спроектировать сеть, которая характеризуется легкостью поиска неисправностей и меньшими простоями. Она также должна обеспечивать взаимодействие между тремя офисами через глобальную сеть. Желательно, чтобы скорость соединений через глобальную сеть составляла примерно 256 Кбит/с, и при этом они должны поддерживать несколько аналоговых телефонных переговоров между офисами (междугородные переговоры стоят слишком дорого). Глобальная сеть должна устранить затраты как на междугородные телефонные переговоры, так и на доставку корреспонденции Federal Express. Руководство хотело бы, чтобы доступ к глобальной сети был возможным даже в том случае, если один из каналов глобальной сети выйдет из строя.

Модернизация сетей

Чтобы облегчить процесс поиска неисправностей и снизить простои, сети каждого офиса придется немного обновить. Например, желательно, чтобы каждый офис перешел с шинной на звездообразную топологию 100BaseT, подключив каждую станцию к концентратору или коммутатору. В целях обеспечения передачи данных со скоростью 100 Мбит/с на каждом компьютере придется установить плату 10/100 Ethernet, а проложенный в настоящее время коаксиальный шинный кабель обновить до категории 5 (или выше) на 100 Мбит/с.

Каналы глобальных сетей

Так как между отдельными филиалами нужно проводить сеансы голосовой связи и передачу данных, следует установить канал T1 (или менее дорогостоящий усеченный T1). Он поддерживает возможность одновременной передачи голоса и данных. Другим подходящим вариантом является служба ретрансляции кадров. Эти службы предоставляются компаниями-владельцами сетей связи общегосударственного масштаба (такими как AT&T, MCI, Spring и др.). Служба E1 предоставляется вне Соединенных Штатов и обеспечивает примерно аналогичный уровень обслуживания. Для сочетания сигналов голоса и данных в каждом офисе нужно установить по мультиплексору, причем все устройства, призванные обеспечить подключение каж-

дой локальной сети к глобальной сети, включая маршрутизаторы, необходимо установить на один и тот же канал глобальной сети, связывающий офисы.

Настройка сетевого доступа

После плановой реализации физической серверной сети приходит время настройки доступа для каждого из ее пользователей. В условиях клиент-серверной сети совместное использование ресурсов координируется посредством учетных записей. Создавая учетные записи (и организуя отдельные учетные записи в группы), сетевой администратор добивается более высокого уровня защиты. На каждой рабочей станции должно быть установлено клиентское программное обеспечение; каждая рабочая станция должна быть настроена как клиент сети. Вам придется определить идентичность сети, задействовать коллективный доступ и установить права доступа к совместно используемым ресурсам. Детали процедуры установки и настройки клиентского программного обеспечения зависят от операционной системы, которой вы пользуетесь (а также от операционной системы сети, в которой вы предполагаете организовать коллективный доступ к ресурсам). В этой части главы мы рассмотрим пользовательские и групповые учетные записи, отметим типы учетных записей, подходящие для данной сетевой среды, и познакомимся с процессом создания пользовательских и групповых учетных записей.

Введение в учетные записи

Учетная запись дает пользователям доступ к файлам, каталогам и устройствам (типа принтеров). В клиент-серверной сети учетные записи создаются и координируются сетевым администратором. Учетная запись состоит из имени пользователя и регистрационной информации. Эти данные определяются в отношении каждого пользователя. Регистрационная информация может состоять из данных о том, на каком компьютере (компьютерах) данный пользователь может работать, дни и периоды времени, в течение которых доступ к ресурсам разрешен, пользовательские пароли и т. д. Данные учетной записи вводятся администратором и, как правило, хранятся на сервере посредством сетевой операционной системы. Когда пользователь пытается пройти регистрацию, сеть проверяет его имя и другие параметры, сверяя их с его учетной записью.

Пользовательские учетные записи

Первое, что нужно сделать, чтобы разрешить пользователю работать в сети, — это создать для него учетную запись. Для ввода и редактирования учетной информации о пользователе администратору может пригодиться служебная сетевая программа. Для создания новой учетной записи требуется полный комплект информации, представляющей пользователя сетевой системе обеспечения защиты. Среди этой информации числятся имя пользователя и пароль, права доступа к системе и ее ресурсам, а также группа, к которой принадлежит данная учетная запись (если она вообще принадлежит к какой-либо группе). Помимо этого, администраторы имеют возможность настраивать ряд других пользовательских параметров. Они могут вводить время регистрации. Этот параметр ограничивает доступ в определенное время суток. Для хранения личных файлов пользователю можно выделить домашний каталог.

Чтобы ограничить время доступа пользователя к сети (например, для временного сотрудника), можно ввести срок действия.

Вы также должны иметь представление об административной и гостевой учетных записях. При первоначальной инсталляции сетевой операционной системы программа установки автоматически создает учетную запись с полными сетевыми полномочиями. В сетевой среде Microsoft такая учетная запись называется административной. В среде Novell она называется диспетчерской, а UNIX — корневой учетной записью. После регистрации в качестве администратора пользователь получает полный контроль над всеми функциями сети. Например, администратор может запустить работу сети, установить первоначальные параметры безопасности и приступить к созданию других пользовательских учетных записей. Для сравнения, гостевая учетная запись, как правило, представляет собой элементарную учетную запись с параметрами по умолчанию, предназначенную для лиц, не имеющих действительной пользовательской учетной записи, но нуждающихся во временном доступе к какому-либо низкому уровню сети.

Групповые учетные записи

При создании пользовательской учетной записи она, как правило, не получает никаких полномочий. Этот вариант по умолчанию часто применяется в целях обеспечения безопасности. Отдельные полномочия пользовательским учетным записям присваиваются посредством группового членства. Все пользовательские учетные записи в рамках группы имеют определенные права доступа и могут выполнять определенные действия (в соответствии с теми правами, которыми обладает группа в целом). Путем назначения полномочий и прав группе администратор получает возможность обращаться с ней как с одной учетной записью. Группы часто используются для обеспечения доступа к ресурсам. Полномочия, присваиваемые группе, автоматически распространяются на всех ее участников. Группам присваиваются права на выполнение системных заданий (например, на резервирование и восстановление файлов или на изменение системного времени). Группирование пользователей также способствует упрощению обмена информацией, т. к. количество отдельных сообщений, подлежащих отправке, снижается (эти сообщения могут отсылаться группе). Например, если администратор хочет предоставить административные полномочия другому пользователю сети, он может сделать этого пользователя участником группы Administrators.

Недооценивать возможности групповых учетных записей не стоит. В клиент-серверных сетях могут существовать сотни (и даже тысячи) учетных записей. Бывают случаи, когда администраторам нужно отправить сообщения большому количеству пользователей, чтобы оповестить их о событии или сетевой политике, или определить каждую учетную запись с конкретными правами доступа. При необходимости модификации прав доступа 100 пользователей администратору придется внести изменения в 100 отдельных учетных записей. Естественно, что манипуляции с отдельными учетными записями занимают много времени и связаны с риском допущения ошибок. Напротив, если 100 учетных записей поместить в одну группу, администратору останется лишь отослать одно-единственное сообщение, направив его соответствующей групповой учетной записи (при этом каждый участник группы получит это сообщение автоматически). Полномочия можно устанавливать или изменять по отношению к группе в целом. Такие модификации автоматически распространяются на всех участников группы.

Пароли учетных записей

В большинстве случаев каждое имя пользователя сопровождается паролем. Пароли способствуют поддержанию системы сетевой безопасности, обеспечивая аутентификацию каждого имени пользователя с помощью секретного слова, которое обычно состоит из букв, цифр и других символов, известных только данному пользователю, а в рамках сети существует в зашифрованном виде. Первоначально пароль назначается сетевым администратором, но впоследствии часто изменяется пользователем (администратор может потребовать от пользователей делать это регулярно, установив для них интервалы изменения паролей). Имейте в виду, что для сетевой операционной системы пароли не являются необходимыми. В некоторых сетевых средах с низким уровнем защиты существует возможность настройки учетной записи без пароля. При подборе пароля следует избегать очевидных вариантов типа даты рождения, номера страхового полиса, имени супруга, детей, кличек домашних животных и т. п. Ни в коем случае не записывайте пароли — запоминайте их. Если срок действия пароля ограничен, система обычно начинает напоминать пользователю о его истечении примерно за 30 дней до этого. Таким образом, пользователь получает возможность изменить пароль до окончания его действия и избежать блокирования своего доступа к сети.

Удаление учетных записей

Если необходимость в определенной учетной записи исчезает, ее, как правило, можно отключить или удалить. Это действие лишит соответствующего пользователя возможности обращения к сети. Отключение учетной записи удобно в том случае, если планируется временное прекращение ее действия. При этом учетная запись остается в сети, и впоследствии в случае необходимости ее можно восстановить. Например, если сотрудник возьмет отпуск за свой счет или за счет компании, соответствующую учетную запись можно будет отключить вплоть до его возвращения. Учетную запись можно удалить, но вместе с ней из сети исчезнут и данные о пользователе. Удаление учетной записи правомерно, если пользователь увольняется из компании или переходит в другое ее подразделение, в котором необходимость в сетевом доступе отсутствует.

Управление учетными записями в Windows 2000

Теперь, после того как вы ознакомились с элементарными данными об учетных записях, мы рассмотрим пример создания учетной записи и группы в среде Windows 2000. Служебная сетевая программа Microsoft Windows 2000 Server, предназначенная для управления учетными записями и группами, называется Computer Management (Управление компьютером). Чтобы запустить ее, последовательно выберите **Start** (Пуск), **Programs** (Программы), **Administrative Tools** (Администрирование), **Computer Management** (Управление компьютером). В результате откроется диалоговое окно **Computer Management** (Управление компьютером), в котором вы сможете открыть запись **Local Users and Groups** (Локальные пользователи и группы) (рис. 21.7).

Выделите запись **Users** (Пользователи). В результате на правой панели появится список существующих пользователей. Чтобы добавить нового пользователя, щелкните на записи **Users** (Пользователи) правой кнопкой мыши и выберите **New User**

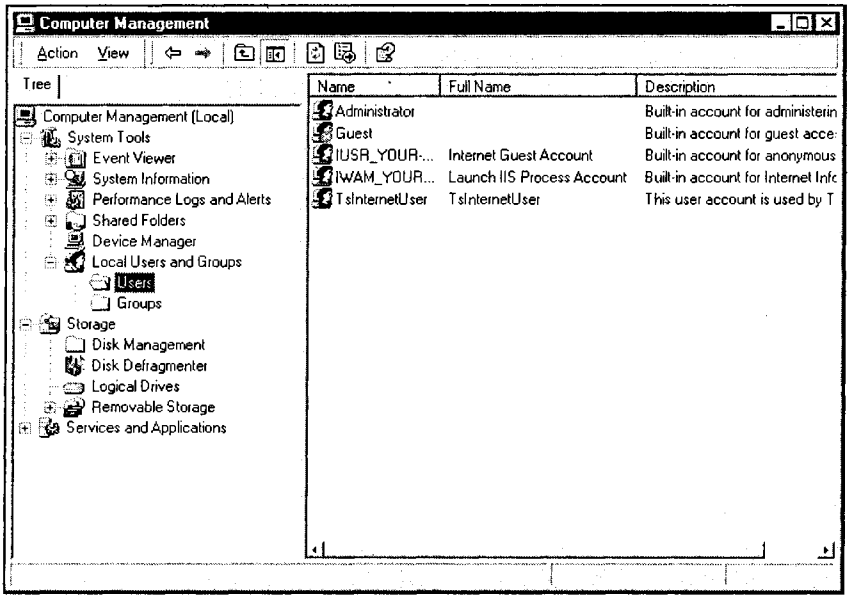


Рис. 21.7. Диалоговое окно **Computer Management** позволяет вам обращаться к параметрам пользователей и групп в среде Windows 2000

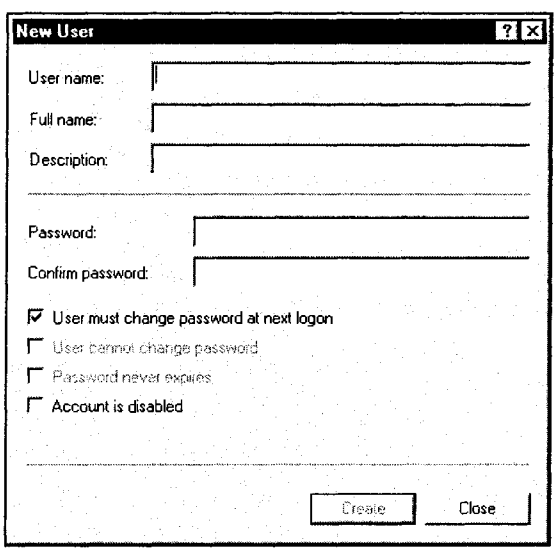


Рис. 21.8. Диалоговое окно **New User** позволяет создавать новых пользователей сети в среде Windows 2000

(Новый пользователь). Появится диалоговое окно **New User** (Новый пользователь) (рис. 21.8), в котором вы сможете ввести имя нового пользователя (**User name**), его полное имя (**Full name**), пароль (**Password**) и другие параметры учетной записи (там

же у вас появится возможность отключить существующую учетную запись). После ввода данных о новом пользователе нажмите кнопку **Create** (Создать). Так вы поместите его учетную запись в список пользователей через диалоговое окно **Computer Management** (Управление компьютером). Аналогичным образом выполняется проверка и внесение изменений в параметры других пользователей. Дважды щелкните на имени нужного пользователя на правой панели диалогового окна **Computer Management** (Управление компьютером) или щелкните на нем правой кнопкой мыши и выберите пункт **Properties** (Свойства).

Управление группами

Управление группами в среде Windows 2000 осуществляется почти столь же просто. Открыв диалоговое окно **Computer Management** (Управление компьютером), выделите запись **Groups** (Группы). В результате на правой панели появится список существующих групп. В таком списке могут присутствовать следующие группы:

- **Administrators** (Администраторы);
- **Backup Operators** (Операторы резервирования);
- **Guests** (Гости);
- **Power Users** (Опытные пользователи);
- **Replicator** (Оператор репликации);
- **Users** (Пользователи);
- **DHCP Administrators** (Администраторы DHCP);
- **DHCP Users** (Пользователи DHCP).

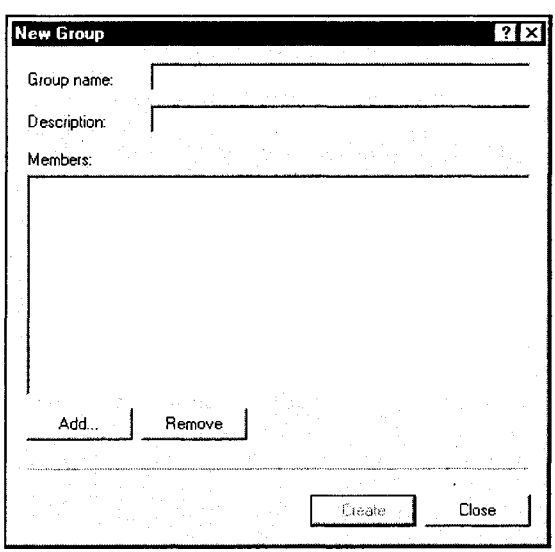


Рис. 21.9. Диалоговое окно **New Group** позволяет вам создавать новые группы в среде Windows 2000

Для создания новой группы следует щелкнуть правой кнопкой мыши на записи **Groups** (Группы) и выбрать пункт меню **New Group** (Новая группа). В результате появится диалоговое окно **New Group** (Новая группа), изображенное на рис. 21.9, с помощью которого вы можете определить имя группы, ее описание, добавить или удалить ее участников. Чтобы сформировать новую группу, нажмите кнопку **Create** (Создать), после чего она будет добавлена в список окна **Computer Management** (Управление компьютером). Добавление участников в группу производится путем двойного щелчка на записи нужного пользователя, перехода на вкладку **Member Of** (Участник) и присоединения его к нужной группе. Вы также можете щелкнуть на имени группы правой кнопкой мыши и выбрать пункт меню **Properties** (Свойства). После этого перед вами появляется список участников данной группы. Чтобы выбрать участника, которого вы планируете ввести в данную группу, нажмите кнопку **Add** (Добавить); затем, чтобы сохранить изменения, нажмите **Apply** (Применить) и **OK**.

Управление учетными записями в Windows NT

В среде NT для обращения к инструментам сетевого управления следует выбрать **Start** (Пуск), **Programs** (Программы), **Administrative Tools (Common)** (Администрирование). Служебная сетевая программа в Microsoft Windows NT Server, посредством которой создаются учетные записи, называется User Manager. После ее запуска в окне **User Manager** (Управление пользователями) нужно открыть меню **User** (Пользователь) и выбрать в нем пункт **New User** (Новый пользователь). В появившемся окне вводится информация о пользователе: его имя, полное имя, описание учетной записи и пароль.

Примечание

В Windows NT Server предусмотрена функция копирования учетных записей, которая позволяет администратору создать шаблон со свойствами и параметрами, общими для многих пользователей. Чтобы создать новую учетную запись с шаблонными свойствами, нужно выделить шаблонную учетную запись, выбрать **User**, **Copy** (<F8>), а затем ввести новое имя пользователя и другие данные, служащие целям идентификации.

Для настройки и сопровождения среды регистрации пользователя (включая сетевые соединения и внешний вид рабочего стола) часто применяются профили. Эта функция очень удобна, т. к. она позволяет работать со знакомым рабочим столом даже в условиях регистрации с других компьютеров сети. В настройках профиля указываются соединения для печати, региональные установки, настройки звука, мыши, монитора и другие параметры, определяемые пользователем. В параметрах пользователя также указываются специальные условия регистрации и информация о том, где пользователь может хранить свои личные файлы. Обращение к профилям производится из **User Manager** (Управление пользователями).

Примечание

По умолчанию, после установки операционной системы Windows NT Server гостевые учетные записи в ней отключаются. Чтобы воспользоваться этой разновидностью учетных записей, сетевой администратор должен активировать их вручную.

Администратор может отключать и удалять пользователей. Для отключения пользователей применяется окно **User Properties** (Свойства пользователей) программы User Manager. Для этого нужно двойным щелчком выбрать имя учетной записи, установить флажок **Account Disabled** (Учетная запись недоступна) и нажать кнопку **OK**. После этого учетная запись находится в заблокированном состоянии. Для удаления учетной записи откройте **User Manager** (Управление пользователями), выберите нужную учетную запись, нажмите сначала клавишу <Delete>, а затем кнопку **OK**. В другом диалоговом окне будет содержаться запрос на подтверждение удаления пользовательской учетной записи. Чтобы удалить учетную запись, нажмите кнопку **Yes** (для отмены операции удаления следует нажать кнопку **No**). Не забывайте о том, что операция удаления учетной записи предполагает ее полное уничтожение (одновременно аннулируются все связанные с ней полномочия и права). Воссоздание пользовательской учетной записи с тем же именем не приведет к автоматическому восстановлению прав или полномочий пользователя. Их нужно будет определить заново.

Управление группами

В Windows NT применяется четыре типа групповых учетных записей: локальные, глобальные, системные и встроенные. Локальные группы создаются в базах данных учетных записей всех локальных компьютеров и содержат пользовательские учетные записи и другие глобальные группы, имеющие возможность обращения к какому-либо ресурсу на локальном компьютере. Локальные группы не могут содержать другие группы того же типа. Глобальные группы распространяются на весь домен. Они создаются на основном контроллере домена (PDC, Primary Domain Controller), в котором действуют соответствующие пользовательские учетные записи. Они могут содержать только те пользовательские учетные записи, которые существуют в данном домене. Глобальные группы не могут содержать локальные или другие глобальные группы. Системные группы выполняют функцию автоматической организации пользователей для применения ими системы. Администраторы не приписывают пользователей к системным группам. Напротив, пользователи становятся их участниками либо по умолчанию, либо в процессе своей деятельности в сети. Встроенные группы — это функция, предусматриваемая многими производителями сетевых продуктов; она включается в сетевую операционную систему. Чем создавать отдельные группы для выполнения элементарных задач, администраторы могут сэкономить время и силы, приписав пользователей к той или иной встроенной группе.

В Windows NT существует множество встроенных групп. В *административную группу* входят локальные администраторы и администраторы доменов. Участники этой группы могут создавать, удалять и координировать пользовательские учетные записи, глобальные и локальные группы. Они также могут коллективно пользоваться каталогами и принтерами, предоставлять полномочия и права на обращение к ресурсам, устанавливать файлы операционной системы и программы. Они также могут обращаться к специально выделенным ресурсам. Правом внесения изменений в пользовательские группы обладают администраторы и операторы учетных записей. Участники *группы операторов серверов* пользуются коллективным доступом к ресурсам, могут блокировать сервер, форматировать его диски, регистрироваться на серверах, проводить операции резервирования и восстановления данных серверов и выключать серверы. Вносить изменения в группы операторов серверов могут только

администраторы. Участники *группы операторов печати* пользуются коллективным доступом к принтерам и могут ими управлять. Они также имеют право локальной регистрации на серверах и их выключения. Участники *группы операторов резервирования* могут регистрироваться локально, резервировать и восстанавливать данные серверов, а также производить их выключение. Участники *группы операторов учетных записей* имеют право создавать, удалять и изменять пользовательские учетные записи, глобальные и локальные группы; при этом они не имеют права вносить изменения в административную группу и группу операторов серверов.

User Manager также применяется для создания и назначения групп в среде Windows NT. Откройте окно **User Manager** (Управление пользователями), выбрав **Start** (Пуск), **Programs** (Программы), **Administrative Tools (Common)** (Администрирование). После запуска User Manager откройте меню **User** (Пользователи) и выберите в нем пункт **New Local Group** (Новая локальная группа). После этого на экране появится диалоговое окно, предназначенное для ввода информации о новой локальной группе. В поле **Group Name** (Имя группы) вводится идентификатор локальной группы. Имя группы не может быть идентичным любой другой группе или имени пользователя в домене или компьютере, выступающем в качестве объекта администрирования. В поле **Description** (Описание) вводится текст описания группы (или пользователей, в ней состоящих). В поле **Members** (Участники) обозначаются имена пользователей всех участников группы. Имейте в виду, что в созданной групповой учетной записи не будет ни одного участника, пока администратор не добавит в нее одного или нескольких существующих пользователей. Эта операция производится в диалоговом окне **New Local Group** (Новая локальная группа) путем нажатия кнопки **Add** (Добавить) и выбора пользовательской учетной записи, которую вы хотите сделать участником группы.

Дополнительные ресурсы

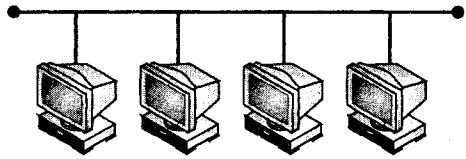
3Com: **www.3com.com**.

CNET: **www.cnet.com**.

IT Toolbox: **www.ittoolbox.com**.

Network Magazine: **www.networkmagazine.com**.

ZDNet: **www.zdnet.com**.



ГЛАВА 22

Сопровождение и модернизация сети

Сети предназначены для обеспечения связи и коллективного использования ресурсов группой пользователей. Когда сетевые устройства теряют работоспособность, в сети прекращаются все операции, кем бы они ни проводились. Вне зависимости от размера вашей сети неисправности участвующих в ней компьютеров, как правило, приводят к потере производительности, а иногда и к потере данных. Чтобы свести воздействие неисправностей в сети к минимуму, необходимо осуществлять сопровождение серверов и рабочих станций, причем делать это оперативно и профессионально. Принцип сопровождения не отличается новизной, но его содержание меняется от одной компании к другой (а иногда и от одной сети в рамках одной и той же компании к другой ее сети) в зависимости от размеров сети и проходящего трафика. Под *сопровождением* мы будем понимать все виды задач по модернизации и плановым заменам, например, обновление BIOS, процессора и памяти, замена дисков и их изъятие из эксплуатации, а также все варианты операций по расширению сети (т. е. операций, связанных с добавлением новых рабочих станций). Эта глава предназначена для того, чтобы вы ознакомились с основными требованиями к сопровождению сети.

Принципы сопровождения серверов

Сопровождение сервера больше походит на искусство, чем на науку. Единственно верного способа здесь не существует. Хороший технический специалист должен иметь представление о сервере, быть знакомым с его компонентами и располагать средствами загрузки и восстановления сервера в случае возникновения неисправностей. Следующие инструкции помогут вам лучше подготовиться к выполнению задач по сопровождению сервера.

Располагайте информацией о сервере

Сетевой сервер — это мощный компьютер с серверным программным обеспечением. Как и в случае с любым другим компьютером, вы должны знать различные компоненты, которые могут присутствовать в составе сервера, а также те, что в нем уже установлены. Например, если на сервер можно установить два процессора Pen-

tium III с частотой до 1,4 ГГц, но фактически установлен только один процессор Pentium III с частотой 1 ГГц, вы должны об этом знать. Такие данные упрощают задачу определения и подбора запасных частей, предоставляют вам возможность справиться с ней с максимальной степенью эффективности. Это особенно актуально, если сервер расположен в физически удаленном месте. Зафиксируйте эти данные в вашем ноутбуке или журнале сопровождения, чтобы их можно было быстро найти. Как минимум, вы должны собрать следующие данные:

- скорость процессора (установленная и максимальная);
- количество установленных/поддерживаемых процессоров;
- степпинг процессора (обозначение версии);
- объем оперативной памяти (установленной и максимальной);
- конфигурация установленной оперативной памяти (например, PC133 SDRAM 256 Мбайт DIMMs);
- производитель и номер версии BIOS;
- производители и размеры дисков, установленных в системе;
- производитель и модель RAID-контроллера (а также номер версии его микропрограммного обеспечения);
- производитель и модель SCSI-контроллера (а также номер версии его микропрограммного обеспечения);
- производитель и модель сетевого адаптера (а также номер версии его микропрограммного обеспечения).

Если сервер был приобретен в полной комплектации, следует также зафиксировать производителя и модель системы, ее сервисную метку/серийный номер и номер телефона службы технической поддержки производителя. Это упростит задачу поиска нужной информации, которая может понадобиться впоследствии.

Располагайте информацией о программах

Сетевое программное обеспечение абсолютно бесполезно без сетевой операционной системы и приложений. Вы должны обязательно знать важнейшее программное обеспечение, установленное на вашем сервере. Эти данные могут быть очень важными при планировании установки служебных пакетов или заплат. Они способны предотвратить появление проблем, связанных с программной совместимостью. Как минимум, вы должны зафиксировать следующее:

- версию операционной системы (а также все установленные служебные пакеты, заплаты и обновления);
- версию сетевой операционной системы (а также все установленные служебные пакеты, заплаты и обновления);
- версии драйверов адаптеров RAID и сетевого адаптера;
- все средства диагностики системы, антивирусные продукты и прочие инструменты, необходимые для сопровождения сети.

Лучше всегда иметь в своем распоряжении все установочные компакт-диски или дискеты с перечисленным программным обеспечением. У вас обязательно должна

быть последняя версия загрузочной дискеты, с помощью которой можно будет запустить сервер в случае фатального отказа диска.

Регулярно проверяйте и настраивайте приводы

В большинстве случаев жесткие диски демонстрируют высокую надежность, но ее нельзя признать абсолютной. Среди распространенных неисправностей дисков можно выделить потерянные кластеры и файлы с разветвленной структурой. Полезно обращать внимание на фрагментацию файлов. Одним из компонентов плановой политики сопровождения должен быть запуск ScanDisk и Disk Defragmenter (или других подходящих дисковых инструментальных средств), с помощью которых можно проверять наличие проблем, связанных с файлами, дефектов поверхности, а также эффективность организации файлов. У вас есть выбор: либо выполнять эти задачи в часы низкого уровня использования сети (например, вечерами или в выходные дни), либо синхронизировать их с другими плановыми процедурами типа установки дисков.

Резервируйте надежно

Систему резервирования следует выбирать исходя из существующих потребностей и степени важности данных. В загруженных корпоративных сетях или в системах регистрации продаж следует проводить резервирование ежедневно (возможно, даже несколько раз в день). Основная сложность в этом случае заключается в том, чтобы последовательно реализовывать разработанный план резервирования. Обязательно проверяйте создаваемые резервные копии. Некачественная или неполная резервная копия даже хуже, чем полное ее отсутствие. Нет ничего хуже, чем попытки восстановления поврежденной или незавершенной резервной копии. В идеале, резервные копии следует хранить вне рабочего места, обеспечивая для них определенные меры безопасности; при этом, чтобы поддерживать свои навыки на высоком уровне, процедуры восстановления нужно проводить регулярно. Помните, что время — деньги, так что способность восстановления после аварийной ситуации является одной из наиболее ценных операций в системе сопровождения.

Проверяйте на вирусы

Сети представляют собой идеальную среду для передачи вирусов, особенно если в них есть доступ к Интернету. Совершенно очевидно, что среди вашего сетевого программного обеспечения должна присутствовать полноценная антивирусная программа, которую нужно регулярно пополнять самыми свежими файлами образов и заплатами. При первоначальной установке антивирусного приложения необходимо проводить операцию поиска по всем файлам, а впоследствии сканировать измененные (или новые) файлы в сети. Пользователи должны быть проинструктированы о процедурах обеспечения безопасности при загрузке файлов и даже при проверке электронной почты.

Соблюдайте условия эксплуатации

Как правило, серверы размещаются в шкафах или помещениях, защищенных от случайного доступа. Серверы могут излучать избыточное тепло, исходящее от не-

скольких процессоров и дисков. Убедитесь, что в помещении, где установлен сервер, обеспечивается достаточное проветривание и присутствует мощный источник питания. Избыток пыли и тепла могут оказаться губительными для системы охлаждения сервера. При наличии большого количества сетевого оборудования для поддержания приемлемых уровней температуры и влажности может потребоваться аппаратура кондиционирования воздуха.

Ведите журналы обслуживания

Каждый раз при проведении операций, связанных с сопровождением сервера, данные о них следует заносить в постоянный письменный журнал. Очень важно, чтобы данные в журналах сопровождения оставались актуальными, чтобы в них были отражены все операции по обслуживанию и модернизации. Точные записи помогают вовремя осуществлять операции по сопровождению сервера, не допускают лишних усилий и служат руководством к последующим обновлениям. Они также делают технических специалистов ответственными за выполнение своей работы. Журналы сопровождения нужно вести для сервера и другого сетевого оборудования.

Модернизация сети

Сети оказываются очень динамичными системами. Они беспрестанно разрастаются, меняются и совершенствуются в зависимости от того, что происходит с пользователями и ресурсами. Необходимость в модернизации часто выражена нечетко, но изменения производительности и отзывы пользователей помогают определить, когда именно следует рассмотреть возможность обновления. Например, о необходимости модернизации свидетельствует ухудшение эффективности передачи данных в сети. Это означает, что значительная часть ваших усилий, связанных с сопровождением, будет направлена на обновления и усовершенствования сети. В большинстве случаев обновления делаются для того, чтобы поднять уровень производительности сети (например, для повышения пропускной способности), увеличить пространства хранения, обеспечить отказоустойчивость и обслужить большее количество пользователей. В этой части главы мы рассмотрим процедуры обновления BIOS, процессора, памяти, сетевого адаптера и систем хранения.

Архитектура и носители сети

В качестве существенных факторов при проектировании и развертывании сети выступают ее архитектура и физический носитель. *Архитектура* — это структура или топология сети (например, кольцо или шина). *Носитель* — это система кабелей, с помощью которой друг к другу подключаются сетевые устройства (в таком качестве могут выступать медь или оптоволокно). Возможны ситуации, когда возникает необходимость в модернизации архитектуры или носителя сети. Подобные процессы модернизации выходят за тематические рамки этой книги, но при необходимости выполнения действий, направленных на существенное повышение производительности сети, вы должны принять их во внимание. Рассмотрим следующие примеры.

- Если сеть спроектирована с использованием щинной топологии (а ее пользователи жалуются на частые сетевые сбои или простой вследствие неисправностей

кабеля), может возникнуть необходимость обновления до звездообразной или кольцевой топологии.

- Если размер и количество зданий, связанных сетью, увеличивается, разумно вложить средства в прокладку сетевой магистрали на основе оптоволоконного носителя. Оптоволокно также может применяться для проведения кабеля между отдаленными зданиями.
- Если сеть сформирована на основе медного носителя (а впоследствии появились устройства, генерирующие электрические помехи), может оказаться необходимым переход на оптоволоконный носитель.
- При проведении сетевых конференций или выполнении сложных настольных Web-приложений сеть также может выиграть от перехода на оптоволоконный кабель.
- Пользователи сети, для которых важна мобильность и возможность частого перемещения своих рабочих станций, могут выиграть от применения беспроводных технологий.

Есть и другие факторы, которые следует рассмотреть, прежде чем принимать конкретное решение, связанное с обновлением архитектуры или носителя сети (скажем, таким фактором являются издержки). Несмотря на то, что стоимость оптоволоконных носителей падает, для монтажа оптоволоконного кабеля требуется привлечение квалифицированного технического специалиста, а это предполагает дополнительные издержки. Помните, что в то же самое время нужно будет обновить сетевые адаптеры, концентраторы и другое сетевое оборудование, т. е. возможны дополнительные, синхронные процедуры модернизации.

Аппаратная совместимость

Одной из наиболее важных проблем, связанных с модернизацией сети, является аппаратная совместимость. Особенно это актуально при работе с операционными системами, подобными Windows NT или 2000, предназначенными для решения коммерческих задач. Так как производительность сетей в значительной степени определяется используемым в них оборудованием, правильный выбор аппаратуры оказывается важным этапом сетевого планирования. В противном случае приобретенное оборудование может работать совсем не так, как ожидалось (а может и не работать вообще). В этой части главы обсуждается значение проверки на совместимость, которую нужно проводить до проведения модернизации. Здесь также представлены некоторые предложения по разрешению проблем, связанных с совместимостью.

Выявление неисправностей

В современной компьютерной индустрии случаи аппаратной и программной несовместимости встречаются довольно часто. Разработкой аппаратного и программного обеспечения занимаются сотни производителей. Даже при наличии установленных стандартов и протоколов каждый разработчик по-своему видит оптимальный способ достижения одной и той же задачи и поэтому предлагает необычное решение. Последствия такого подхода неоднозначны. С одной стороны, конкуренция между разработчиками поддерживает низкий уровень цен и широкий выбор, но, с другой стороны, не все оборудование может работать совместно. Следовательно, оценка и

подбор подходящих комплектующих и программ является основным этапом планирования развертывания сети.

Если вы можете себе позволить переделать сеть от начала до конца, то, вероятно, вы можете также выбирать производителей продуктов и возлагать бремя ответственности за совместимость на них. Лучший способ избежать неприятности — исследовать предполагаемые ключевые комплектующие перед их приобретением. Возможно, стоит предоставить производителям перечень аппаратного и программного обеспечения, которым вы предполагаете пользоваться, и попросить их подтвердить совместимость этих компонентов с их собственными продуктами. Например, если вы решили приобрести два устройства, спросите об их совместимости у обоих производителей. Сравните полученные ответы, потому что они могут позволить выявить случай несовместимости, который в противном случае вам обнаружить не удастся.

В большинстве случаев перед вами стоит задача проектирования сети исходя из существующего комплекта аппаратного обеспечения; в такой ситуации вероятность проблем, происходящих из несовместимости аппаратуры, очень высока. Чаще всего фиксируется несовместимость между существующим аппаратным и новым программным обеспечением, а также между новым аппаратным и существующим программным обеспечением. Замена или обновление компьютера или сетевой операционной системы может привести к серьезным проблемам, связанным с совместимостью. Например, Windows 98/SE предусматривает полную поддержку портов USB, а Windows NT — не предусматривает. Если для создания сети вам потребуется Windows NT, но в этой сети вы надеетесь задействовать USB-принтер, вполне возможно, что установка Windows NT полностью лишит вас возможности применения этого принтера.

Проверка документации и требований

В сопроводительных руководствах к продукту может содержаться ценная информация о проблемах совместимости. Это еще в большей степени касается Web-сайтов продуктов, на которых их производители могут оперативно публиковать данные о зафиксированных проблемах (а также обо всех известных способах их обхода). Разнообразные проблемы и сбои рассматриваются в сетевых списках часто задаваемых вопросов (FAQ), посвященных продукту.

Вы также должны обеспечить соответствие вашей системы минимальным (а еще лучше — рекомендуемым) системным требованиям, предъявляемым любым аппаратным или программным обеспечением, которое вы планируете установить. При этом особенно важны параметры быстродействия процессора, объема оперативной памяти (RAM) и свободного дискового пространства. Например, в табл. 22.1 приводятся некоторые минимальные системные требования для разных распространенных сетевых операционных систем.

Таблица 22.1. *Системные требования, предъявляемые распространенными сетевыми операционными системами*

	Netware 5	**Windows NT Server 4.0**	**Windows 98**	**Red Hat Linux 7.2**
Процессор	Pentium	486 с частотой 33 МГц или выше	486 с частотой 66 МГц или выше	Pentium с частотой 200 МГц

Таблица 22.1 (окончание)

	Netware 5	Windows NT Server 4.0	Windows 98	Red Hat Linux 7.2
Память	64 Мбайт	16 Мбайт	16 Мбайт	64 Мбайт
Свободное пространство на диске	200 Мбайт	125 Мбайт	225 Мбайт	650 Мбайт
Привод	CD-ROM	CD-ROM	3,5" с высокой плотностью записи	CD-ROM
Монитор	VGA	VGA	VGA	VGA
Сетевой адаптер	Да	Да	Да	Да

Проверка списка совместимого оборудования

Операционные системы, включая простые и сетевые версии, проходят тщательное тестирование на самых разнообразных аппаратных устройствах. Если вы планируете проведение модернизации аппаратного обеспечения или если вам нужно убедиться в том, что после обновления сетевой ОС она продолжит взаимодействовать с существующим оборудованием, полезно ознакомиться со списком совместимого оборудования (HCL, Hardware Compatibility List) для этой сетевой операционной системы. Например, компания Microsoft ведет всеобъемлющий список совместимого оборудования для операционной системы Windows 2000 и публикует его по адресу: **http://www.microsoft.com/WINDOWS2000/upgrade/compat/default.asp**. Если ваша аппаратура отсутствует в списке совместимого оборудования, она может работать при наличии сторонних драйверов или драйверов от производителя, но, по крайней мере, это известит вас о возможности возникновения трудностей.

При монтаже нового компьютера или установке новой ОС программа установки, как правило, пытается обнаружить аппаратное обеспечение, присутствующее в системе, еще в процессе инсталляции. Затем происходит загрузка драйверов, подходящих для каждого из устройств. Просмотрите список обнаруженного аппаратного обеспечения и убедитесь в том, что он совпадает с фактическим перечнем компонентов компьютера. Например, если вы устанавливаете Novell IntranetWare, служебная программа установки автоматически осуществляет поиск и определение различных устройств, в число которых входят жесткие диски, приводы CD-ROM и сетевые адаптеры. Процедура обнаружения должна также запускаться при установке нового устройства в условиях, когда сетевая ОС уже функционирует. Если устройства идентифицируются, для них загружаются соответствующие драйверы. Если же обнаружить устройство не удается, узнайте, существует ли специальный драйвер от его производителя или программная поддержка иного рода. В противном случае вы, вероятно, не сможете пользоваться этим устройством.

Обновление BIOS

BIOS представляет собой микропрограммное обеспечение, т. е. программу, полностью зафиксированную на одном или нескольких кристаллах памяти и применяе-

мую для управления работой компьютера. Когда дефекты устранены, вопросы совместимости улажены, а в коде BIOS выполнены настройки, связанные с производительностью, вам может понадобиться обновить BIOS сервера до новейшей версии. Раньше для обновления BIOS требовалась физическая замена микросхем(ы) или даже установка новой материнской платы. Сегодня почти во всех компьютерах BIOS записывается во флэш-памяти, что позволяет ее перепрограммировать, не извлекая кристалл из системы. Это означает, что вы можете загрузить обновленный файл BIOS вместе с утилитой флэш-загрузчика с Web-сайта производителя материнской платы, а затем установить его собственными силами.

Определение установленной версии BIOS

Прежде чем перейти к обновлению BIOS, важно узнать, какая версия этой системы установлена на вашем компьютере в данный момент. Узнав номер этой версии, вы получаете возможность обеспечить установку более поздней/прогрессивной версии. Идентификация BIOS выполняется после процедуры первоначального включения питания, но еще до начала загрузки операционной системы. Обычно это происходит во время подсчета памяти. Имейте в виду, что строка идентификатора BIOS появляется на экране лишь на несколько секунд, так что для фиксации всего кода может потребоваться несколько циклов перезагрузки системы. Идентификатор BIOS производит впечатление беспорядочного нагромождения кодов, но вы должны обратить особое внимание на производителя системы BIOS и дату ее выпуска. Идентификатор BIOS может, например, выглядеть следующим образом:

```
Sample BIOS 4.65 12/25/2000
```

При планировании обновления BIOS проверьте, подходит ли новая версия именно для вашего сервера. В случае установки неверной версии BIOS ваша система может работать некорректно (а может не работать вообще).

Подготовка к процессу обновления

К проведению обновлений BIOS нужно немного подготовиться. Вам придется скачать соответствующий флэш-файл на загрузочную дискету, а затем распаковать этот файл для получения его составляющих (обычно в нем содержится утилита флэш-загрузчика, новый файл данных BIOS и файл readme). Ниже приводится простейший пример этой процедуры.

Примечание

Прежде чем выполнять обновление BIOS, обязательно ознакомьтесь с инструкциями, сопровождающими утилиту флэш-загрузчика.

1. Создайте чистую загрузочную дискету средствами DOS или Windows 98/SE.
2. Файл обновления BIOS обычно представляет собой сжатый самораспаковывающийся архив, содержащий все файлы, необходимые для проведения процедуры модернизации BIOS. Скопируйте файл обновления BIOS во временный каталог на жестком диске.
3. Из командной строки C: перейдите в этот временный каталог.
4. Чтобы извлечь файл обновления BIOS, введите его имя, например, `10006BC1.EXE`.

5. Нажмите клавишу <Enter>. После этого произойдет распаковка файла. Из первоначального файла будет извлечен примерно следующий набор файлов: LICENSE.TXT, README.TXT и BIOS.EXE.
6. Ознакомьтесь с содержимым файла LICENSE.TXT. Он содержит инструкции по обновлению BIOS в условиях вашей системы.
7. Поместите в дисковод A: загрузочный гибкий диск.
8. Распакуйте флэш-загрузчик (например, BIOS.EXE) на этот гибкий диск, для этого перейдите во временный каталог, в котором хранится файл флэш-загрузчика, и введите `BIOS A:`.
9. Нажмите клавишу <Enter>.
10. Теперь на загрузочной дискете хранятся файлы, с помощью которых можно выполнить как обновление BIOS, так и восстановление предыдущей версии.

Завершение процесса обновления

После подготовки дискеты к процессу обновления системы BIOS приступайте к инсталляции ее новой версии. В качестве руководства вы можете воспользоваться приведенными ниже шагами.

1. Загрузите компьютер с гибкого диска, находящегося в приводе A:. Появится экран **BIOS upgrade utility** (Утилита обновления BIOS).
2. Выберите **Update Flash Memory From a File** (Обновить флэш-память из файла).
3. Выберите **Update System BIOS** (Обновить системный BIOS) и нажмите клавишу <Enter>.
4. Чтобы указать нужный файл с расширением BIO, воспользуйтесь клавишами стрелок; затем нажмите <Enter>.
5. Когда утилита запросит подтверждение вашего намерения провести флэш-обновление системы BIOS в памяти, выберите пункт **Continue with Programming** (Продолжить программирование) и нажмите клавишу <Enter>.
6. Когда утилита выведет сообщение **Upgrade is Complete** (Обновление выполнено), извлеките гибкий диск и нажмите клавишу <Enter>.
7. Когда компьютер загрузится вновь, посмотрите на идентификатор системы BIOS (обозначение ее версии). Так вы сможете убедиться в успешности обновления.
8. Чтобы узнать, как войти в программу CMOS Setup, найдите сообщение BIOS, которое должно выглядеть примерно так:

```
Press <F2> Key if you want to run SETUP
(Нажмите клавишу <F2> для запуска SETUP)
```

9. Чтобы обеспечить корректное функционирование системы, загрузите настройки по умолчанию программы CMOS Setup и для их подтверждения нажмите клавишу <Enter>.
10. Переустановите все важные параметры CMOS Setup.

11. Подтвердите изменения и сохраните их; затем выключите компьютер и перезагрузите его.

Примечание

Не забывайте о том, что в большинстве компьютеров BIOS защищается от перезаписи посредством одной или нескольких перемычек (например, перемычка BIOS Write Enable). Прежде чем загружать систему, вы должны настроить сервер на принятие нового файла BIOS.

Восстановление BIOS

В большинстве случаев обновление BIOS проходит безо всяких сбоев. Впрочем, установка неподходящей версии BIOS или нарушение электропитания может привести к серьезному повреждению BIOS, и в результате сервер потеряет работоспособность. К счастью, многие современные материнские платы поддерживают свойства "блока начальной загрузки", сохраняющие важнейшие функции BIOS. Даже если система BIOS повреждена, минимальный блок защищенного кода BIOS (блок начальной загрузки) способен обеспечить считывание данных с гибкого диска и предоставить возможность повторной установки исходной (или корректной) версии BIOS. Ниже представлена типичная процедура восстановления BIOS в случае неудачного обновления.

Примечание

Учитывая то, что в области блока начальной загрузки сосредоточен лишь незначительный объем кода, видеоизображение в ходе восстановления не выводится. На экране вы ничего не увидите. Следить за ходом процедуры можно, слушая сигналы, исходящие из динамика, и наблюдая за сигналами светодиода флоппи-дисковода.

1. Выключите все подключенные к компьютеру периферийные устройства, а затем выключите компьютер.
2. Снимите крышку системного блока и найдите перемычку восстановления BIOS.
3. Установите перемычку восстановления в положение перепрограммирования.
4. Вставьте загрузочный гибкий диск обновления BIOS во флоппи-дисковод A:.
5. Включите компьютер и дайте ему загрузиться. Процесс восстановления займет несколько минут.
6. Прислушайтесь к динамику.
7. Два звуковых сигнала (и завершение активности), исходящих от дисковода A:, указывают на успешное завершение процедуры восстановления BIOS. Если вы слышите непрерывную последовательность звуковых сигналов, значит, восстановление BIOS не удалось (если процесс восстановления закончится неудачей, возвратитесь к шагу 1 и попробуйте запустить весь процесс заново).
8. Если восстановление прошло успешно, выключите компьютер и установите перемычку восстановления в положение защиты.
9. Установите крышку системного блока на место, перезагрузите систему и зайдите в CMOS Setup. Установите значения по умолчанию и заново укажите все важные параметры.
10. Перезагрузите систему в нормальном режиме.

Замена сетевых адаптеров

Когда к сети присоединяются новые пользователи и уровни трафика повышаются, может появиться необходимость в увеличении полосы пропускания данных. Для этого придется заменить ваш сетевой адаптер. Процесс его модернизации почти идентичен установке любого другого устройства Plug-and-Play PCI и предполагает прохождение четырех основных этапов: демонтаж старого адаптера, монтаж нового, подключение сетевого кабеля и настройка нового адаптера.

Удаление старых драйверов

Если вы решили заменить или модернизировать сетевой адаптер (или обновить его драйверы), вполне возможно, что сначала вам придется удалить драйверы старого адаптера. Так вы сможете гарантировать отсутствие конфликта между старым и новым программным обеспечением. Приведенный ниже пример демонстрирует процесс удаления драйверов сетевого адаптера Adaptec DuraLAN для Windows NT.

1. Дважды щелкните на пиктограмме **My Computer** (Мой компьютер) на рабочем столе.
2. Двойным щелчком выберите **Control Panel** (Панель управления).
3. Дважды щелкните на пиктограмме **Network** (Сеть).
4. Находясь в окне **Network**, перейдите на вкладку **Adapters** (Адаптеры).
5. В списке **Network Adapters** (Сетевые адаптеры) выберите сетевой адаптер, который предполагается демонтировать (в нашем случае это Adaptec DuralLAN NIC), и нажмите кнопку **Remove** (Удалить).
6. Чтобы подтвердить продолжение, нажмите кнопку **Yes**.
7. Повторите два предыдущих действия до полного удаления всех родственных драйверов (например, Adaptec DuraLAN).
8. Покончив с удалением, нажмите кнопку **OK**.
9. Чтобы закрыть окно **Network** (Сеть), нажмите кнопку **Close** (Закрыть).
10. Чтобы перезагрузить компьютер, нажмите кнопку **Yes**.

Примечание

При перезагрузке Windows NT может появиться сообщение о том, что, по меньшей мере, одна служба не запустилась. После установки нового драйвера это сообщение появляться не будет, так что просто нажмите кнопку **OK**.

Демонтаж старой сетевой платы

После удаления всех старых драйверов вы можете приступать к демонтажу старого сетевого адаптера. Чтобы извлечь из системы сетевой адаптер, сделайте следующее.

1. Отключите компьютер от источника питания и выньте шнур питания из стенной розетки. В ходе процесса удаления вы должны заземлить себя, прикоснувшись к любой неокрашенной поверхности корпуса компьютера.
2. Следуя инструкциям производителя, снимите кожух системного блока вашего компьютера.

3. Отключите от старой сетевой платы все кабели.
4. Открутите винт, фиксирующий сетевой адаптер, а затем плавно извлеките его из разъема.

Примечание

Прежде чем отключать компьютер для демонтажа сетевого адаптера, вам, возможно, потребуется удалить старые драйверы этого адаптера и другие средства программной поддержки.

Установка нового сетевого адаптера

После извлечения из системы старого сетевого адаптера приступайте к установке нового, следуя нашим инструкциям.

1. Вы должны заземлить себя, прикоснувшись к любой неокрашенной поверхности (корпусу) системного блока компьютера.
2. Осторожно извлеките новый сетевой адаптер из его антистатического контейнера. Уточните модель устройства, сверившись с его именем, обозначенным на корпусе. Можете поместить старый адаптер в антистатический контейнер.
3. Убедитесь в отсутствии видимых повреждений устройства, которые могли быть нанесены во время доставки или транспортировки. В случае обнаружения повреждения вы должны немедленно оповестить вашего поставщика и службу доставки, чтобы заменить устройство.
4. Так как системный блок уже вскрыт, найдите свободный разъем (в нашем случае — разъем PCI). Открутите винт и снимите заглушку разъема.

Примечание

Разъемы PCI и сетевые платы существуют в двух вариантах: 3,3-вольтовом и 5-вольтовом. Сетевые адаптеры PCI, как правило, поддерживают напряжение 5 В. Некоторые модели, помимо этого, обеспечивают поддержку 3,3-вольтовых разъемов. Чтобы повысить производительность при использовании многопортовых сетевых адаптеров, устанавливайте такие платы в разъем 0 шины PCI.

5. Поместите сетевой адаптер в разъем PCI. Вставляйте его плавно, но с усилием до тех пор, пока контакты не будут плотно соприкасаться в разъеме.
6. Зафиксируйте плату в разъеме с помощью снятого ранее винта.
7. Установите кожух системного блока.
8. Подключите все прочие устройства, которые вы отсоединили в ходе монтажа.

Повторное подключение и настройка

Тщательно подключите к новому сетевому адаптеру сетевые кабели (после установки драйверов сетевого адаптера он автоматически выбирает кабели). При определенных параметрах системы вам придется настроить адаптер посредством CMOS Setup сервера. Возможно, потребуется конфигурирование сетевого адаптера через его встроенную программу настройки.

Установка новых драйверов

После монтажа, подключения и настройки нового сетевого адаптера необходимо установить его драйвер, подходящий для вашей сетевой операционной системы. Прежде чем приступать к выполнению этой задачи, разумно проверить наличие очередных обновлений и заплат драйверов от производителя сетевой платы. В этом разделе главы мы рассмотрим типичный процесс инсталляции драйвера сетевого адаптера Adaptec DuraLAN для Windows NT.

1. Запустите операционную систему Windows NT.
2. Выберите **Start** (Пуск), **Settings** (Настройка), **Control Panel** (Панель управления).
3. В **Control Panel** дважды щелкните на пиктограмме **Network** (Сеть).
4. В окне **Network** перейдите на вкладку **Adapters** (Адаптеры).
5. На вкладке **Adapters** нажмите кнопку **Add** (Добавить).
6. В окне **Select Network Adapter** (Выбор сетевого адаптера) нажмите кнопку **Have Disk** (Есть диск).
7. В окне **Insert Disk** (Вставьте диск) вставьте дискету с драйвером (например, дискету с Duralink64 для Windows NT), а затем нажмите кнопку **OK**.
8. В окне **Select OEM Option** укажите установленную модель сетевого адаптера (например, DuraLAN NIC) и нажмите кнопку **OK**.
9. В появившемся окне установки (например, **Adaptec DuraLAN NIC Driver Installation**) выберите желаемый драйвер и нажмите кнопку **OK**.
10. Переходите к установке стандартного драйвера, драйвера восстановления после отказа и драйвера агрегации портов.

Проверка драйверов

После установки драйверов нижеперечисленные действия помогут проверить корректность инсталляции стандартного драйвера в Windows NT.

1. Выберите **Start** (Пуск), **Settings** (Настройка), **Control Panel** (Панель управления).
2. На вкладке **Control Panel** дважды щелкните на пиктограмме **System** (Система).
3. На вкладке **Device Manager** (Диспетчер устройств) просмотрите перечень **Network Adapters** (Сетевые адаптеры).
4. Обозначение вашего сетевого адаптера должно присутствовать в списке **Network Adapters**. Нажмите кнопку **OK**. Если обозначение сетевого адаптера отсутствует в этом списке, значит, его установка прошла с нарушениями.
5. Если рядом с записью сетевого адаптера отображается желтый восклицательный знак, вполне возможно, что драйверы установлены неверно. Удалите драйвер сетевого адаптера и проведите его повторную инсталляцию (если это возможно, проверьте, нет ли для него обновлений).
6. Если в окне **Network** (Сеть) приводятся и старый, и новый сетевой адаптер, вы должны удалить в **Device Manager** (Диспетчер устройств) запись, соответствующую старой плате.

Модернизация накопителей

Для хранения всех необходимых файлов и приложений в сетях используют накопители большого объема. Таким образом, стараясь удовлетворить потребности сервера, связанные с хранением, вам придется устанавливать новые и заменять старые диски. Как правило, в качестве устройств хранения на серверах применяются съемные носители и диски с горячим подключением (рис. 22.1). В число съемных носителей входят флоппи-дисководы, накопители на магнитной ленте и приводы типа CD-ROM. В число дисков с горячим подключением входят все виды жестких дисков SCSI, которые обычно настраиваются на использование RAID.

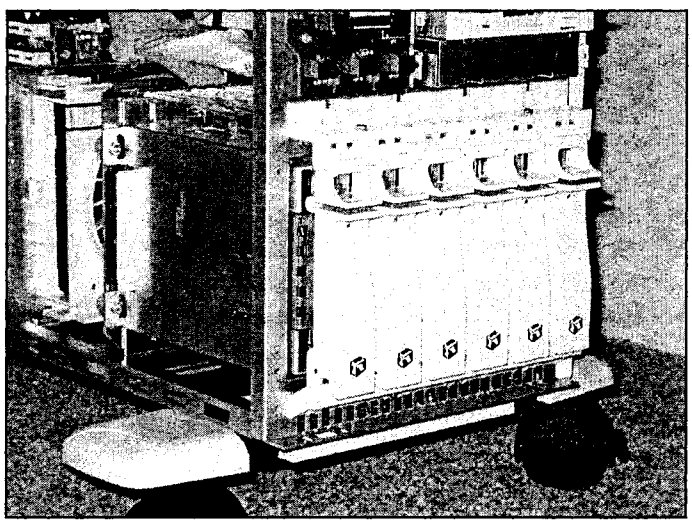


Рис. 22.1. На сервере Gateway 7400 в качестве устройств хранения применяются диски с горячим подключением

Съемные носители

Как правило, демонтаж съемных носителей из стоечных серверов производится следующим образом.

1. Выдвиньте сервер из стойки, установите его в фиксированном положении и снимите крышку.
2. Снимите Y-образное крепление и крепление кронштейна платы.
3. Откатите несущую раму назад, чтобы получить доступ к кабелям в каркасе для диска.
4. Поднимите защитную крышку и отключите от диска силовые и сигнальные кабели.
5. Открутите винты, фиксирующие накладку носителя (два из них), с передней фальш-панели.
6. Открутите винты, фиксирующие устройство хранения (два из них) и выньте диск.

Чтобы установить диск, повторите эти действия в обратном порядке. Важно запомнить, что не во всех отсеках можно устанавливать любые дисководы. Например, флоппи-дисковод 3,5 на 1,44 Мбайт можно установить только в отсеках 5 и 6, а привод CD-ROM, вероятно, будет работать только в отсеке 5; в то же время дисковод TurboDAT будет работать только в отсеке 7. Чтобы точно определить, какие из ваших дисководов совместимы с каждым из отсеков сервера, вы должны свериться с документацией по серверу.

Диски с горячим подключением

Демонтаж и замена дисков с горячим подключением может производиться при включенном сервере. В большинстве случаев на новом жестком диске с горячим подключением устанавливать перемычки идентификации SCSI не нужно. Они автоматически устанавливаются материнской платой и отсеком для дисков с горячим подключением при монтаже такого устройства. После замены старого диска (настроенного на отказоустойчивость) новый диск автоматически запускает процесс восстановления. В процессе восстановления диска светодиод подключения сигнализирует зеленым светом. Этот светодиод мигает вплоть до полного завершения восстановления данных на диске. При замене жестких дисков с горячим подключением необходимо следовать инструкциям, приведенным ниже.

- Никогда не демонтируйте несколько дисков одновременно. При замене диска для восстановления данных на новом диске контроллер пользуется данными, записанными на других дисках-участниках массива. В случае удаления нескольких дисков получение полного набора данных для восстановления информации на этих дисках становится невозможным.
- Никогда не демонтируйте работающий диск, когда другой диск неисправен. Диски, признанные контроллером поврежденными, обозначаются посредством желтого светодиода неисправности диска на лотке дисков. В случае замены работающего диска при одновременной замене неисправного диска происходит невосстановимая потеря данных.
- Никогда не демонтируйте диск во время восстановления другого диска. О проходящем процессе восстановления сигнализирует светодиод мигающим зеленым светом. Данные на диске, установленном вместо неисправного, восстанавливаются на основе данных, содержащихся на других дисках.
- Никогда не отключайте систему дисков (хранения) при включенном управляющем сервере. В такой ситуации SMART-контроллер сервера определяет все диски как неисправные. В результате может произойти фатальная потеря данных.
- Если в системе установлен оперативный (онлайн) резервный диск, подождите, пока он завершит процесс восстановления, и только после этого приступайте к замене неисправного диска. Когда диск выходит из строя, активизируется оперативный резерв. Он запускает процесс восстановления, чтобы подменить неисправный диск. По окончании этого процесса поврежденный диск необходимо заменить новым. Не следует заменять неисправный диск оперативным резервным диском.
- Если замена диска производилась в условиях отключенного питания системы, то при загрузке сервера появится сообщение об ошибке POST (например, код 1786). При этом у вас будет выбор: либо продолжить загрузку и восстановить данные на

новом диске, либо продолжить загрузку без восстановления (в последнем случае данные будут потеряны).

Процесс замены жесткого диска с возможностью горячего подключения довольно прост. В большинстве случаев доступ к дискам производится в передней части стойки; при этом выдвигать сервер из стойки не приходится. Чтобы демонтировать диск, разблокируйте рычаги эжектора и отогните эти рычаги (рис. 22.2). Этим вы высвободите диски из коннектора. Выньте жесткий диск с горячим подключением из корпуса. Чтобы установить новый жесткий диск, вставьте его в каркас. Установите диск в коннектор и закрепите его с помощью рычагов. При прокладке кабелей следите, чтобы они не проходили в местах, где они могут быть сжаты или сломаны.

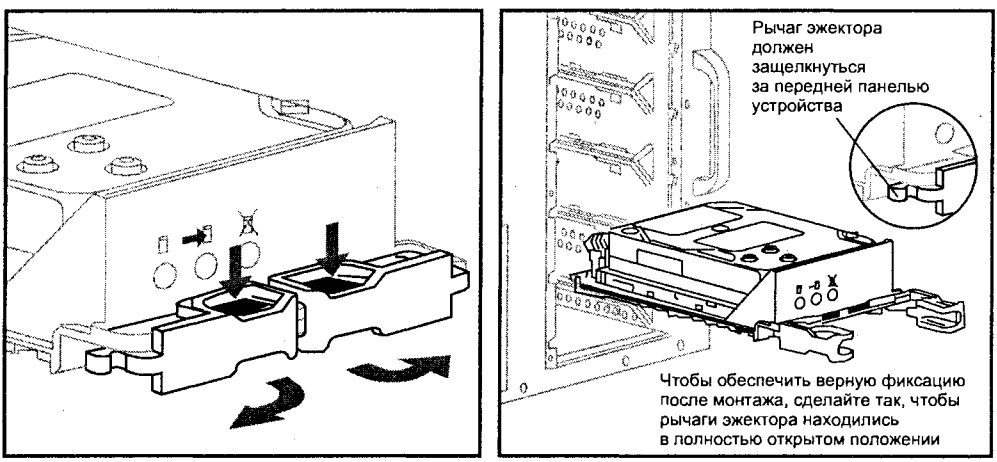


Рис. 22.2. Монтаж жесткого диска с горячим подключением (публикуется с разрешения Compaq)

Примечание

Во многих случаях требуется, чтобы жесткие диски SCSI, установленные на одной шине SCSI, принадлежали только к внутреннему (внутри сервера) или к внешнему типу системы хранения, т. к. смешение этих типов не допускается. Для совместного монтажа внутренних и внешних жестких дисков SCSI одного одноканального контроллера SCSI становится недостаточно. Многоканальный контроллер (например, Compaq SMART SCSI Array Controller) предусматривает возможность монтажа внутренних и внешних жестких дисков SCSI на отдельных шинах SCSI.

Замена модулей памяти

Серверная память часто устанавливается в виде модулей DIMM (модулей памяти с двухрядным расположением выводов), а типичная серверная материнская плата поддерживает от 768 Мбайт до 1 Гбайт (или более) быстрой памяти Synchronous DRAM (SDRAM) при ее установке в разъемы DIMM количеством до четырех (т. е. в виде четырех модулей DIMM по 256 Мбайт каждый). В некоторых серверах применяется память Rambus (RDRAM), которая устанавливается в разъемах RIMM (Rambus Inline Memory Module — модуль памяти с линейным расположением выво-

дов Rambus). По мере повышения степени сложности и объемов трафика на сервере для обработки большого количества открытых файлов могут потребоваться большие объемы памяти. Так как вам, вероятно, придется модернизировать память в рамках существующей конфигурации, мы в первую очередь рассмотрим процесс снятия модулей DIMM.

Примечание

Все виды памяти крайне чувствительны даже к несущественным электростатическим зарядам. Поэтому при работе с модулями DIMM или RIMM следует соблюдать все антистатические меры предосторожности.

1. Откройте сервер (если он еще не открыт) и найдите разъемы DIMM.
2. Аккуратно переместите рычаги пластикового эжектора вперед и вниз. В результате нужный модуль DIMM будет вытолкнут из разъема.
3. Удерживая модуль DIMM только за края (не трогайте его микросхемы и золотые краевые соединители), осторожно выньте его из разъема. Поместите старый модуль DIMM в антистатическую упаковку и храните его в упаковке.
4. При необходимости демонтажа других модулей DIMM повторите все вышеприведенные действия.

Примечание

При снятии и установке модулей DIMM или RIMM следует соблюдать предельную осторожность. В результате слишком сильного нажима может быть поврежден разъем (и материнская плата выйдет из строя). Прилагайте к рычагам пластикового эжектора только усилие, необходимое для снятия или фиксации модуля. Модули снабжаются ключами, которые предусматривают лишь один способ их установки.

Чтобы оснастить сервер достаточным объемом памяти, обратитесь к документации по материнской плате и выберите один или несколько модулей DIMM. Выбор DIMM должен производиться исходя из емкости (например, 128 Мбайт), типа памяти (например, SDRAM), скорости (например, цикл памяти длительностью 8 нс) и вида проверки ошибок (например, с контролем четности, без контроля четности, с кодом корректировки ошибок или без него). Ниже рассмотрен процесс установки модуля DIMM.

Примечание

В коннекторах модулей DIMM и разъемах может применяться олово или золото, причем смешение разных металлов (например, установка модуля DIMM с позолоченными контактами в разъем DIMM с оловянными контактами) может приводить к последующим сбоям в работе памяти, которые, в свою очередь, обуславливают нарушение целостности данных. Модули DIMM с позолоченными краевыми соединителями следует устанавливать исключительно в позолоченные разъемы.

1. Откройте корпус системного блока (если он еще не открыт) и найдите разъем DIMM.
2. Удерживая модуль DIMM только за края, извлеките его из антистатической упаковки.

3. Расположите модуль DIMM таким образом, чтобы два выреза на нижнем крае DIMM совпали с ключами в разъеме.
4. Вставьте нижний край DIMM в разъем и с некоторым усилием нажмите на модуль. Он должен правильно и полностью зафиксироваться в разъеме.
5. Аккуратно переведите рычаги пластикового эжектора на обоих краях разъема в вертикальное (фиксированное) положение.
6. При необходимости повторите все вышеперечисленные действия для установки других модулей DIMM.

Модернизация процессора

Серверная материнская плата обычно предусматривает установку двух или четырех (иногда и более) процессоров. Для большинства конечных пользователей одного процессора вполне достаточно, однако на сетевых серверах для координации множества пользователей и обработки большого количества открытых файлов требуются дополнительные процессоры. К каждому устанавливаемому процессору необходимо подключить подходящий теплоотвод/вентилятор, а во все свободные процессорные разъемы нужно устанавливать заглушки. Обратитесь к документации, сопровождающей серверную материнскую плату, и ознакомьтесь с типами и скоростными характеристиками совместимых с ней процессоров (например, совместимыми могут быть один или два процессора Pentium III с частотой 1 ГГц). Если вы хотите установить второй процессор, не забудьте, что он должен быть идентичным существующему (иногда требуется даже соответствие производственных версий) или подходить для совместной работы с исходным процессором.

Примечание

Все процессоры в высшей степени подвержены действию даже незначительных электростатических разрядов. При манипуляциях с процессором вы должны соблюдать все антистатические меры предосторожности.

Выберите один или несколько процессоров, подходящих к вашей материнской плате, и проверьте надежность присоединения их теплоотводов/вентиляторов. Найдите подходящие процессорные разъемы на материнской плате, а также миниатюрные коннекторы для вентиляторов, расположенные рядом с каждым разъемом. Практически все современные серверные материнские платы поддерживают автоматическое обнаружение процессора и настройку его скорости шины, множителя и напряжения. Это означает, что установка перемычек в целях подготовки материнской платы к монтажу новых процессоров оказывается необходимой не так уж часто. Теперь мы рассмотрим основные действия, необходимые для монтажа процессора.

Примечание

Если сервер только что прекратил работу, установленные процессоры и теплоотводы сохраняют высокую температуру. Чтобы избежать ожогов, подождите хотя бы 15 минут после отключения системы и после этого приступайте к манипуляциям с процессорами.

1. Откройте крышку системного блока (если она еще не открыта) и найдите процессорные разъемы.

2. Если на вашем сервере уже установлен один процессор, и вы намереваетесь поставить еще один, необходимо снять заглушку с ближайшего процессорного разъема. Аккуратно потяните язычок механизма фиксации назад. Его нужно переставить в такое положение, чтобы заглушку можно было выкрутить. Возьмите заглушку за сторону, расположенную ближе всего к язычку механизма фиксации, и вращательным движением извлеките эту сторону из разъема. Как только эта сторона будет снята, вы сможете вытащить из разъема другую сторону заглушки.

Примечание

Как правило, чтобы обеспечить надежность функционирования всей системы, требуется установка заглушек на все свободные процессорные разъемы. Заглушка состоит из оконечной схемы AGTL+ и механизма терминирования тактовых импульсов. Если заглушки установлены не на всех свободных процессорных разъемах, сервер может не загрузиться.

3. Если на вашем сервере установлен один процессор, и вы намереваетесь его заменить, не снимайте заглушку со свободного второго разъема. Демонтируйте процессор, который вы хотите заменить.
4. Если на вашем сервере установлено два процессора, и вы собираетесь заменить один из них или оба, демонтируйте его (их).
5. Извлеките новый процессор из антистатической упаковки и предельно осторожно расположите его в разъеме таким образом, чтобы точно совместить вывод 1. Если вы устанавливаете слотовый процессор, плавно поместите его в механизм фиксации. Равномерно надавите на процессор с двух концов, чтобы зафиксировать его в разъеме. Когда он будет установлен в нужном положении, раздастся щелчок.
6. Сокетный процессор следует надежно расположить в разъеме, а затем зафиксировать рычаг ZIF.

Примечание

Механизмы фиксации GRM не совместимы с компоновкой процессора типа SECC. Новые заземленные механизмы фиксации поддерживают только процессоры с типом компоновки SECC2 (например, Pentium II/III Xeon). Если вы планируете использовать тип компоновки SECC (например, он применяется в обычных процессорах Pentium II/III), вам нужен универсальный механизм фиксации (URM).

7. Подключите силовой кабель вентилятора к трехвыводному коннектору на серверной плате.
8. Закройте системный блок сервера и закрепите его наружный корпус (переключатель проникновения необходимо установить в закрытое положение).
9. Подключите все оставшиеся внешние кабели и подведите шнур питания от источника переменного тока.
10. Включите монитор, а затем питание сервера. Запустите программу CMOS Setup и с ее помощью настройте новую материнскую плату сервера, память и процессоры.

Замечания о процессорных платах

В некоторых случаях в стоечных серверах (особенно в старых моделях типа Compaq ProLiant 4500) процессоры устанавливаются на съемной плате, показанной на рис. 22.3. Подобная процессорная плата, как правило, содержит BIOS и многие базовые обрабатывающие элементы, которые обычно размещаются на простых материнских платах. Такой подход позволяет проектировщикам упростить структуру материнской платы в стойке и предусматривает возможность монтажа процессорной платы в качестве платы расширения, замена которой для ремонта или модернизации не представляет сложности. На сегодняшний день система высокочастотного тактирования, применяемая в процессорах, плохо приспособлена к технологии процессорных плат, и именно по этой причине процессоры устанавливаются на материнские платы (примерно таким же образом, как процессоры монтируются на настольных компьютерах).

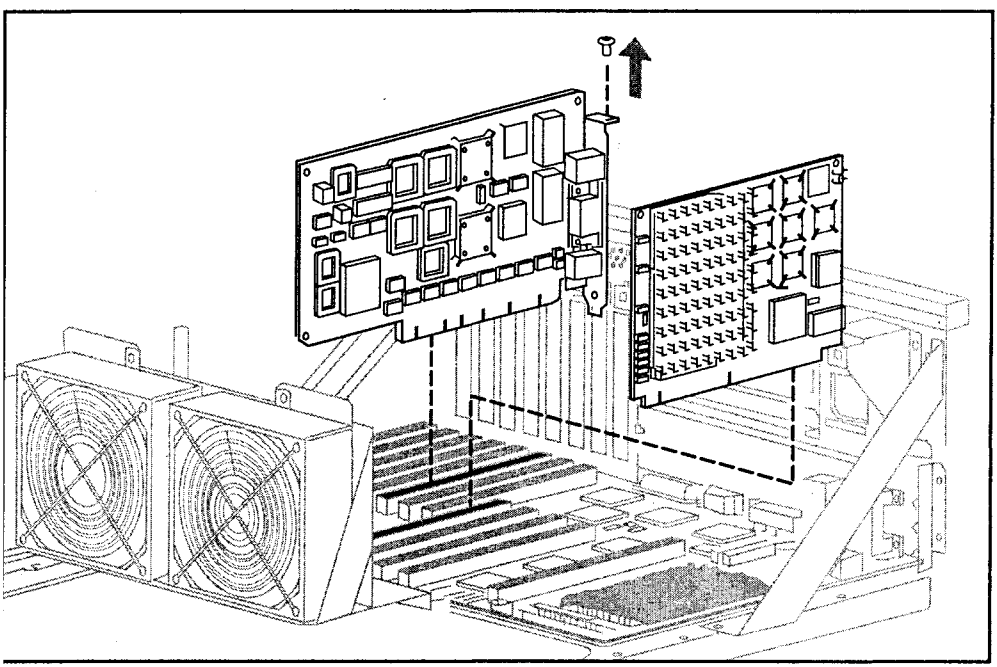


Рис. 22.3. Снятие процессора и других плат со стоечного сервера (публикуется с разрешения Compaq)

Замечания о сочетаниях процессоров

Даже процессоры с одинаковыми параметрами скорости и номинального напряжения могут незначительно отличаться по своей внутренней структуре. Такие изменения происходят при исправлении дефектов и улучшении производительности процессоров. Во многих случаях процессоры, применяемые в типичных сетях, должны сочетаться друг с другом. Так, процессоры должны не только характеризоваться идентичной скоростью и напряжением, но и иметь одинаковые уровни технической

реализации (Revision). Например, в процессорах Intel для обозначения такого уровня применяются числа "S-spec". Требования по соответствию предъявляются не всеми материнскими платами (новейшие серверные материнские платы более терпимы по отношению к несовпадению процессоров), однако сочетание обычно рассматривается как наиболее оптимальная конфигурационная политика по умолчанию. Если в условиях вашего сервера соответствие процессоров является жестким требованием, но обеспечить его для новых процессоров не представляется возможным (например, из-за устаревшего технического уровня установленных процессоров, аналоги которых уже отсутствуют в продаже), то вам, вероятно, придется установить полностью обновленный комплект из сочетаемых процессоров.

Обнаружение конфликтов и их разрешение

Каждое устройство, установленное на сервере (будь то сетевой адаптер или видеокарта), потребляет системные ресурсы. Тем самым оно привлекает к себе внимание системы и обменивается данными с памятью или процессором. Любые компьютеры (в том числе серверы) поддерживают ограниченный объем ресурсов, причем одни и те же ресурсы не могут использоваться двумя разными устройствами; при несоблюдении последнего требования происходит аппаратный конфликт. Программное обеспечение низкого уровня (например, драйверы устройств), потребляющее системные ресурсы, также может конфликтовать, работая в нормальном режиме. В этой части главы представлены основные понятия из области системных ресурсов; здесь же демонстрируются методики обнаружения и устранения конфликтов программного и аппаратного обеспечения.

Введение в сетевые ресурсы

Чтобы устранять конфликты, необходимо иметь представление о значимости всех доступных системных ресурсов. Персональные компьютеры и серверы поддерживают три типа ресурсов: прерывания (или IRQ), каналы DMA и области ввода/вывода (I/O). Многие контроллеры и сетевые устройства пользуются системой BIOS, которая также требует некоторого пространства в памяти. Важность этих ресурсов не следует недооценивать, т. к. конфликты могут возникать где угодно, а их последствия для системы плачевны.

Прерывания

Прерывание, вероятно, является наиболее известным и понятным типом ресурсов. Прерывания управляют запросами на использование ресурсов процессора. Они позволяют устройству или подсистеме работать в фоновом режиме до того момента, когда какое-либо событие не потребует системной обработки. В качестве примера такого события может выступать получение символа через последовательный порт, нажатие клавиши на клавиатуре и другие реальные ситуации. Прерывание активизируется путем утверждения логического уровня на одной из физических линий запроса прерывания (IRQ, Interrupt Request), обращение к которой осуществляется через любой разъем шины материнской платы. AT-совместимые компьютеры поддерживают 16 линий IRQ (которым соответствуют обозначения от IRQ 0 до IRQ 15). Они приведены в табл. 22.2, в которой перечислены только обычные аппаратные прерывания. Существуют также процессорные и программные прерывания.

Таблица 22.2. *Перечисление типичных назначений прерываний*

Прерывание	Функция
0	Микросхема системного таймера
1	Микросхема контроллера клавиатуры
2	Микросхема второго контроллера прерываний
3	Последовательный порт 2 (COM2: 2F8h-2FFh и COM4: 2E8h-2EFh)
4	Последовательный порт 1 (COM1: 3F8h-3FFh и COM3: 3E8h-3EFh)
5	Параллельный порт 2 (LPT2: 378h или 278h)
6	Контроллер флоппи-дисковода
7	Параллельный порт 1 (LPT1: 3BCh [моно] или 378h [цвет])
8	Часы реального времени (RTC, Real-Time Clock)
9	Не используется (перенаправление на IRQ 2)
10	Шина USB (в системах, оборудованных ею, можно отключить)
11	Система звуковоспроизведения Windows (в системах, оборудованных ею, можно отключить)
12	Порт для подключения мыши на материнской плате (PS/2)
13	Математический сопроцессор
14	Первичный контроллер жесткого диска AT/IDE
15	Вторичный контроллер жесткого диска AT/IDE (в системах, оборудованных им, можно отключить)

После активизации прерывания программа обработки прерываний сохраняет текущие состояние регистров процессора в небольшой области памяти (которая называется стеком), а затем адресует процессор к таблице векторов прерываний. Таблица векторов прерываний представляет собой перечень местоположений программ, соответствующих каждому прерыванию. При запуске прерывания процессор переходит к программе обработки прерываний, расположение которой указывается в таблице векторов прерываний, и исполняет эту программу. В большинстве случаев обработчик прерываний представляет собой драйвер устройства, связанный с платой, активирующей данное прерывание. Например, IRQ, исходящее от сетевого адаптера, вероятнее всего, вызовет для управления им драйвер сетевого устройства. Что касается контроллера жесткого диска, то в данном случае IRQ вызывает код BIOS ROM, который в свою очередь осуществляет управление диском. После завершения работы обработчика исходное содержимое регистров процессора извлекается из стека, и процессор сразу находит место, на котором он остановился.

Как техническому специалисту, вам нет необходимости прекрасно разбираться в механизме инициализации и активизации прерываний, но вы должны знать основные термины, связанные с этой темой. Термин *назначенный* означает то, что устройство настроено на вывод определенного сигнала IRQ. Например, типичная плата

контроллера жесткого диска IDE назначается на IRQ 14 (для первичного контроллера) и IRQ 15 (для вторичного контроллера). Обычно назначения IRQ производятся посредством одной или нескольких перемычек или DIP-переключателей. С помощью технологии Plug-and-Play можно производить их автоматическую настройку. Затем под программным управлением прерывания могут выборочно включаться или отключаться. *Включенное прерывание* — это прерывание, которое программируемый контроллер прерываний передает процессору. Одно лишь то обстоятельство, что прерывание включено, еще не означает, что на него назначено какое-либо устройство. Наконец, *активное прерывание* — это линия, на которой генерируются реальные прерывания. Учтите, что термин *активный* не синонимичен *назначенному* или *включенному*.

Каналы прямого доступа к памяти

Процессор — специалист по перемещению данных. Он способен двунаправленно передавать данные между ячейками памяти, адресами ввода/вывода или из памяти в устройство ввода/вывода. Конструкторы персональных компьютеров пришли к выводу, что передача больших объемов данных (по одному слову за раз) через процессор впустую тратит его время. Дело в том, что во время передачи данных процессор на самом деле ничего не обрабатывает, а просто перемещает информацию из одного места в другое. Если бы существовал способ освободить процессор от выполнения этих лишних задач, данные можно было бы перемещать быстрее, чем при участии процессора. Такой методикой является *прямой доступ к памяти* (DMA). Он предназначен для перемещения больших объемов данных из памяти на адрес ввода/вывода или обратно, без прямого участия процессора. Теоретически, микросхема контроллера DMA функционирует как автономный процессор данных, освобождая центральный процессор для выполнения других задач.

Передача DMA начинается с сигнала запроса DMA (DMA Request, DRQ), который генерируется запрашивающим устройством (например, платой контроллера флоппи-дисковода). Если данный канал был предварительно включен посредством программных драйверов или подпрограмм BIOS, этот запрос достигнет соответствующей микросхемы контроллера DMA на материнской плате. Затем контроллер DMA отправляет процессору запрос на захват (Hold); тот отвечает сигналом подтверждения захвата (Hold Acknowledge, HLDA). Когда контроллер DMA получает сигнал HLDA, он указывает контроллеру шины на необходимость фактического отключения процессора от шины расширения и разрешения микросхеме контроллера DMA принять управление этой шиной на себя. Контроллер DMA отправляет запрашивающему устройству сигнал подтверждения DMA (DMA Acknowledge, DACK); после этого процесс передачи может начинаться. После завершения передачи контроллер DMA вновь подключает процессор и удаляет свой запрос HOLD. После этого процессор незамедлительно возобновляет свою деятельность. В табл. 22.3 приводятся обычные назначения каналов DMA.

Как и в случае с прерываниями, выбор канала DMA производится путем установки перемычки или DIP-переключателя на плате расширения (или средствами Plug-and-Play). Когда в разъем вставляется плата, настройка канала устанавливает соединение между этой платой и микросхемой контроллера DMA. Довольно часто складывается ситуация, при которой сопровождающие программные драйверы должны задействовать ключ командной строки, который направляет их на соответствующее аппарат-

ное назначение DMA. Совместное использование каналов DMA двумя или несколькими устройствами не допускается. При одновременных попытках использования одного и того же канала DMA несколькими устройствами происходит конфликт.

Таблица 22.3. *Перечисление типичных назначений DMA*

DMA	Традиционная функция	Современные функции
0	Динамическое обновление оперативной памяти	Система звуковоспроизведения
1	Не используется	Система звуковоспроизведения или параллельный порт
2	Контроллер флоппи-дисковода	Контроллер флоппи-дисковода
3	Не используется	Параллельный порт ECP или система звуковоспроизведения
4	Зарезервировано (внутреннее применение)	Зарезервировано (внутреннее применение)
5	Не используется	Не используется
6	Не используется	Не используется
7	Не используется	Не используется

Пространство ввода/вывода

Во всех компьютерах предусматривается пространство для портов ввода/вывода (Input/Output, I/O). Порт ввода/вывода действует во многом аналогично ячейке памяти, но предназначен не для хранения. Напротив, порт ввода/вывода обеспечивает для компьютера возможность прямого взаимодействия с устройством. Таким образом, компьютер может эффективно передавать команды и данные между системой и разными устройствами. Каждому устройству необходимо присваивать уникальный адрес (или диапазон адресов). В табл. 22.4 приводятся некоторые типичные назначения портов ввода/вывода.

Таблица 22.4. *Типичные назначения портов ввода/вывода*

Диапазон адресов	Типичное назначение
0000h–000Fh	PIIX4-DMA 1
0020h–0021h	PIIX4-контроллер прерываний 1
002Eh–002Fh	Регистры конфигурации суперконтроллера ввода/вывода
0040h–0043h	PIIX4-счетчик/таймер 1
0048h–004Bh	PIIX4-счетчик/таймер 2
0060h	Байт контроллера клавиатуры — сброс IRQ
0061h	PIIX4 — немаскируемое прерывание (NMI), управление динамиком

Таблица 22.4 (продолжение)

Диапазон адресов	Типичное назначение
0064h	Контроллер клавиатуры, байт CMD/STAT
0070h	(Бит 7) PIIX4 — включение немаскируемого прерывания
0070h	(Биты 6–0) PIIX4 — таймер реального времени, адрес
0071h	PIIX4 — таймер реального времени, данные
0078h	Зарезервировано — конфигурация платы
0079h	Зарезервировано — конфигурация платы
0081h–008Fh	PIIX4 — регистры страниц DMA
00A0h–00A1h	PIIX4 — контроллер прерываний 2
00B2h–00B3h	Управление интерфейсом APM
00C0h–00DEh	PIIX4-DMA 2
00F0h	Ошибка сброса числа
0170h–0177h	Вторичный IDE-контроллер
01F0h–01F7h	Канал первичного IDE-контроллера
0200h–0207h	Звуковой/игровой порт
0220h–022Fh	Звук (Sound Blaster-совместимый)
0240h–024Fh	Звук (Sound Blaster-совместимый)
0278h–027Fh	LPT2
0290h–0297h	Управляющее расширительное аппаратное обеспечение
02E8h–02EFh	COM4/видео (8514A)
02F8h–02FFh	COM2
0300h–0301h	MPU-401 (MIDI)
0330h–0331h	MPU-401 (MIDI)
0332h–0333h	MPU-401 (MIDI)
0334h–0335h	MPU-401 (MIDI)
0376h	Командный порт вторичного канала IDE
0377h	Командный порт вторичного канала флоппи-дисковода
0378h–037Fh	LPT1
0388h–038Dh	Звуковой адаптер AdLib (FM-синтезатор)
03B4h–03B5h	Видео (VGA)
03BAh	Видео (VGA)
03BCh–03BFh	LPT3

Таблица 22.4 (окончание)

Диапазон адресов	Типичное назначение
03C0h–03CAh	Видео (VGA)
03CCh	Видео (VGA)
03CEh–03CFh	Видео (VGA)
03D4h–03D5h	Видео (VGA)
03DAh	Видео (VGA)
03E8h–03EFh	COM3
03F0h–03F5h	Основной канал флоппи-дисковода
03F6h	Командный порт первичного канала IDE
03F7h	Командный порт первичного канала флоппи-дисковода
03F8h–03FFh	COM1
04D0h–04D1h	Запускаемый фронтом/уровнем программируемый контроллер прерываний
0530h–0537h	Звуковая подсистема Windows
0604h–060Bh	Звуковая подсистема Windows
LPT n + 400h	Порт принтера с расширенными функциональными возможностями (ECP), базовый адрес порта LPT n + 400h
0CF8h–0CFBh	Адресный регистр конфигурации PCI
0CF9h	Регистр управления ускоренным режимом и сбросом
0CFCh–0CFF	Регистр данных конфигурации PCI
0E80h–0E87h	Звуковая подсистема Windows
0F40h–0F47h	Звуковая подсистема Windows
0F86h–0F87h	Конфигурация Yamaha OPL3-SA
FF00h–FF07h	Регистры управления шиной IDE
FFA0h–FFA7	Регистры управления первичной шины IDE
FFA8h–FFAFh	Регистры управления вторичной шины IDE

Назначения портов ввода/вывода обычно осуществляются вручную путем установки перемычек или DIP-переключателей на самой плате расширения (эти операции также могут проводиться автоматически посредством Plug-and-Play). Как и в случае с прочими системными ресурсами, совершенно необходимо убедиться в отсутствии двух устройств, одновременно использующих один и тот же порт (порты) ввода/вывода. При наложении одного или нескольких адресов ввода/вывода происходит аппаратный конфликт. В случае такого конфликта команды, предназначенные для одного устройства, могут быть ошибочно интерпретированы другим устройст-

вом. Имейте в виду, что большинство устройств могут быть настроены на применение нескольких адресов, но в то же время некоторые устройства не поддерживают такую возможность.

Распределение памяти

Память — это еще один жизненно важный ресурс компьютера. Более ранние устройства полагались на назначение IRQ, каналов DMA и портов ввода/вывода, но большинство современных устройств (в число которых входят, например, контроллеры SCSI, сетевые адаптеры, видеокарты, модемы и т. д.) требуют выделения пространства в памяти, которое необходимо им для поддержания встроенных ПЗУ BIOS (микропрограммного обеспечения). Совмещение адресов двух таких ПЗУ не допускается. Если оно произойдет, конфликта не избежать. В табл. 22.5 приводится распределение памяти в современном компьютере.

Таблица 22.5. *Типичная схема распределения памяти в системах PC*

Диапазон адресов (десятичные значения)	Диапазон адресов (шестнадцатеричные значения)	Размер	Описание
1024K–262144K	100000–10000000	255 Мбайт	Extended Memory (Дополнительная память)
960K–1024K	F0000–FFFFF	64 Кбайт	BIOS
944K–960K	EC000–EFFFF	16 Кбайт	Boot block (Блок начальной загрузки) (доступен как UMB[1])
936K–944K	EA000–EBFFF	8 Кбайт	ESCD[2] (конфигурация PnP/DMI)
932K–936K	E9000–E9FFF	4 Кбайт	Зарезервирован для BIOS
928K–932K	E8000–E8FFF	4 Кбайт	Логотип OEM
896K–928K	E0000–E7FFF	32 Кбайт	POST BIOS (доступна как UMB)
800K–896K	C8000–DFFFF	96 Кбайт	Доступная для DOS верхняя память (UMB)
640K–800K	A0000–C7FFF	160 Кбайт	Видеопамять и BIOS
639K–640K	9FC00–9FFFF	1 Кбайт	Расширенные данные BIOS
512K–639K	80000–9FBFF	127 Кбайт	Расширенная (Extended) обычная память
0K–512K	00000–7FFFF	512 Кбайт	Стандартная (Conventional — обычная) память

[1] Upper Memory Block — блок верхней памяти. — *Ред.*

[2] Extended Static Configuration Data — расширенные данные статической конфигурации. — *Ред.*

Выявление конфликтов и действия по их устранению

К счастью, конфликты почти всегда оказываются результатом неверно выполненного обновления системы. Следовательно, технический специалист может приготовиться к вероятности возникновения конфликтов, применив *правило последнего обновления*. Это правило состоит из трех частей:

- устройства и/или программы, установленные в системе совсем недавно;
- неисправности, произошедшие после того, как это устройство и/или программа была установлена в системе;
- система, работавшая нормально до установки этого аппаратного и/или программного обеспечения.

При наличии всех трех компонентов, скорее всего, вы столкнулись с аппаратным или программным конфликтом (а не с дефектом устройства). В отличие от большинства других типов неисправностей компьютеров, которые обычно характерны для конкретной поврежденной подсистемы, конфликты обычно производят впечатление гораздо более глобальных проблем. Типичными для серьезных аппаратных или программных конфликтов являются следующие симптомы.

- Система блокируется во время выполнения самотестирования при включении питания (POST) или при загрузке операционной системы.
- Система блокируется при запуске конкретного приложения.
- Система блокируется при использовании конкретного устройства (например, сканера TWAIN).
- Система блокируется случайным образом или без предупреждения, независимо от какого-либо приложения.
- Система не отказывает, но установленное устройство не функционирует (хотя оно как будто правильно настроено). Устройства, установленные в системе ранее, при этом могут работать без сбоев.
- Система не отказывает, но устройство или приложение, работавшее ранее, теперь не функционирует. Недавно установленное устройство (и сопровождающее его программное обеспечение) может работать нормально, а может и со сбоями.

Серьезность и частота сбоев (а также точка их возникновения) зависят от того, какие именно устройства и какие применяемые ими ресурсы (например, IRQ, DMA или адреса ввода/вывода) конфликтуют, а также от функции, выполняемой системой в то время, когда конфликт обнаруживается. Так как между оборудованием и настройками каждого компьютера есть некоторые различия, предсказать симптомы конфликта с большей степенью точности практически невозможно.

Подтверждение наличия конфликтов и их разрешение

Нередко при обнаружении конфликта устранить его оказывается намного сложнее. Но в вашем распоряжении есть несколько очень эффективных методик. Первое правило разрешения конфликтов выражено фразой "последним пришел — первым обслужен" (LIFO, Last In First Out). Принцип LIFO означает, что самым оперативным средством устранения конфликта является удаление аппаратного или программного обеспечения, которое привело к его возникновению. Другими словами,

если вы установили плату *X*, после чего плата *Y* перестала работать, то, вероятно, с системой конфликтует плата *X*, и демонтаж платы *X* должен привести к восстановлению нормальной работы платы *Y*. Аналогичный принцип применим и к программному обеспечению. Если вы установили в системе новое приложение, а после этого обнаружили, что одно из приложений, установленных ранее, отказывается работать в нормальном режиме, то, вероятнее всего, неисправно именно новое приложение. К сожалению, удалением элемента-нарушителя дело не ограничивается. Вам в любом случае придется установить новое устройство или программу таким образом, чтобы избежать появления системных конфликтов.

Разрешение программных конфликтов

Причиной конфликтов могут быть драйверы устройств. Для проведения некоторых аппаратных обновлений требуется установка одного или нескольких драйверов реального режима (они также называются DOS-драйверами). Подобные драйверы вызываются из файла CONFIG.SYS во время инициализации системы (или загружаются вместе с Windows). Для обозначения применяемых системных ресурсов они пользуются рядом параметров командной строки. Часто это бывает необходимо для того, чтобы гарантировать корректное управление устройством со стороны его драйвера, причем эта схема особенно распространена в серверах на базе NetWare. Если опции командной строки, применяемые драйвером устройства, не совпадают с аппаратными настройками (или накладываются на настройки драйвера другого устройства), в системе могут возникать трудности. Если вы подозреваете, что источником неисправности является драйвер устройства, найдите ссылку на него в файле CONFIG.SYS и отключите его, поместив перед его командной строкой команду `REM`. Например, так:

```
REM DEVICE = C:\DRIVERS\NEWDRIVE.SYS /A360 /I:5
```

Команда `REM` превращает соответствующую строку в комментарий (REMark). Впоследствии, если вы решите восстановить строку, комментарий можно будет без труда удалить. Не забывайте, что такое отключение драйвера устройства приведет к тому, что это устройство перестанет работать. Но если причина неисправности станет ясной, вы сможете манипулировать с настройками драйвера вплоть до ее устранения. Чтобы изменения вступили в действие, необходимо перезагрузить компьютер. Наконец, можно предположить, что программа содержит дефекты или повреждения. Попробуйте связаться с ее производителем. Возможно, существует исправление или недокументированная функция, о которой вы ничего не знаете, либо есть заплата или обновление, которое поможет устранить неисправность.

Разрешение аппаратных конфликтов и коды ошибок

Рассмотрим пример. Пользователь установил в свою систему привод CD-ROM и плату адаптера. Процесс инсталляции с применением умолчаний прошел безо всяких проблем, заняв всего десять минут. Несколько дней спустя при попытке провести резервирование системы пользователь обнаружил, что система резервирования на магнитной ленте, подключенная к параллельному порту, не отвечает (хотя принтер, также подключенный к параллельному порту, работает в нормальном режиме). Пользователь попытался загрузить систему с чистого загрузочного гибкого диска (файлов CONFIG.SYS или AUTOEXEC.BAT, которые могли бы отключить драйверы устройств, нет), но неисправность не исчезла. Немного поразмыслив, пользователь

выключил систему, демонтировал плату адаптера CD-ROM и загрузил компьютер с чистого загрузочного гибкого диска. Естественно, устройство резервирования на магнитных дисках, подключенное к параллельному порту, вновь заработало.

Подобные примеры напоминают техническим специалистам о том, что аппаратные конфликты не всегда так сокрушительны, как о них думают. Во многих случаях последствия конфликтов оказываются малозначительными и уж точно не катастрофичными. Так как последним установленным устройством оказался привод CD-ROM, его и нужно было демонтировать в первую очередь. Для того чтобы понять суть неисправности и устранить ее, потребовалось пять минут. Впрочем, устранение неисправности не является единственным компонентом разрешения конфликтов. Значительно труднее установить то же устройство таким образом, чтобы оно не вызывало конфликты.

К счастью, в Windows есть Device Manager (Диспетчер устройств), который следит за устройствами, установленными в системе, идентифицирует ресурсы и драйверы, назначенные для каждого устройства. Например, откройте Device Manager в Windows 2000 и дважды щелкните на записи **Computer** вверху перечня устройств. В результате откроется диалоговое окно **Device Manager**. Выберите **View** (Вид), отсортируйте ресурсы (**Resources**) по типу и разверните список ресурсов (рис. 22.4). Здесь можно просмотреть назначения IRQ, DMA, I/O и распределение памяти. Проанализировав эти записи, вы можете оперативно определить, какие ресурсы распределены, а какие — свободны.

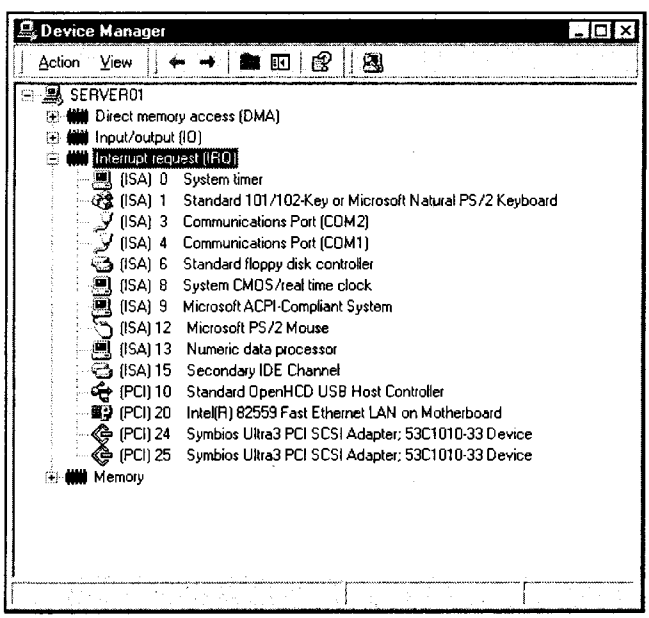


Рис. 22.4. Просмотр назначений ресурсов в операционной системе Windows 2000

Device Manager в операционных системах Windows 95/98/2000 — это очень мощное средство, которое помогает анализировать конфигурацию и настройки почти всех

устройств, установленных в системе. При возникновении проблемы Device Manager часто идентифицирует ее, он способен предоставить ценные данные, с помощью которых ее можно устранить. Прежде чем приступить к процессу разрешения конфликтов, мы выделим некоторое время на изучение типичных ошибок, отображаемых в Device Manager. Вы можете проверить Device Manager на наличие кодов ошибок. При работе в системе Windows 2000 это делается следующим образом.

1. Щелкните на пиктограмме **My Computer** (Мой компьютер) правой кнопкой мыши.
2. Выберите **Properties** (Свойства).
3. Перейдите на вкладку **Hardware** (Оборудование) и нажмите кнопку **Device Manager** (Диспетчер устройств).
4. Дважды щелкните на нужном типе устройства (например, на **Network adapters** (Сетевые адаптеры)). Так вы сможете просмотреть устройства, находящиеся в соответствующей категории.
5. Чтобы просмотреть диалоговое окно **Properties** (Свойства) со свойствами устройства, дважды щелкните на его записи (рис. 22.5).

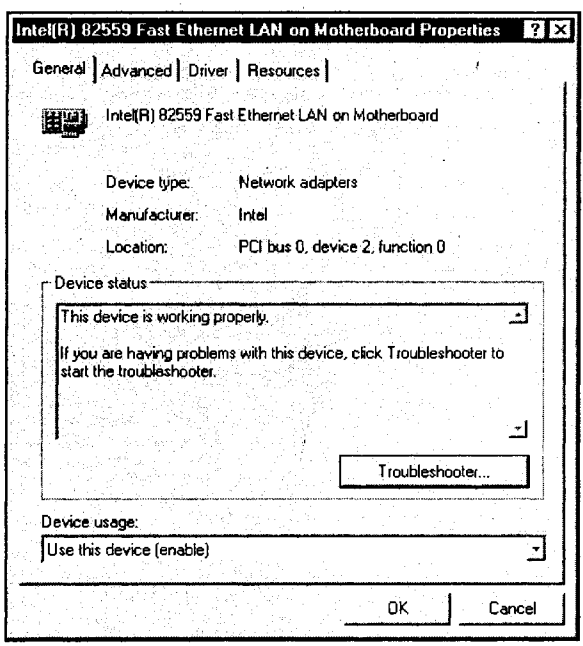


Рис. 22.5. Типичное диалоговое окно свойств устройства (**Properties**) в операционной системе Windows 2000

6. В случае генерации кода ошибки он выводится в окне состояния **Device** (Устройство) на вкладке **General** (Общие). Если с данным устройством связана неисправность, нажмите кнопку **Troubleshooter** (Средство устранения неисправности).

Интерпретация кодов Device Manager

Открыв Device Manager в системе Windows 98/ME, вы можете просмотреть состояние каждого устройства. При наличии неисправности устройства оно обозначается в перечне устройств в категории **Computer**. Рядом с неисправным устройством ставится символ, обозначающий характер сбоя.

- Черный восклицательный знак (!) на желтом поле означает, что устройство неисправно (хотя оно, тем не менее, может продолжать работать). Выводится код неисправности, указывающий на ее характер.
- Красный "X" обозначает отключенное устройство. Отключенным является устройство, физически присутствующее в системе и потребляющее ресурсы, но не располагающее загруженным драйвером защищенного режима.
- При просмотре ресурсов устройств в свойствах **Computer** синяя буква "i" на желтом поле (вокруг ресурса устройства) указывает на то, что для данного устройства не активирована функция применения автоматических настроек **Use Automatic Settings**, и данный ресурс был выбран вручную. Это не означает, что устройство неисправно или отключено.
- Зеленый вопросительный знак (?) в Device Manager означает, что для данного устройства установлен только совместимый драйвер. Существует вероятность, что доступны не все функции устройства.

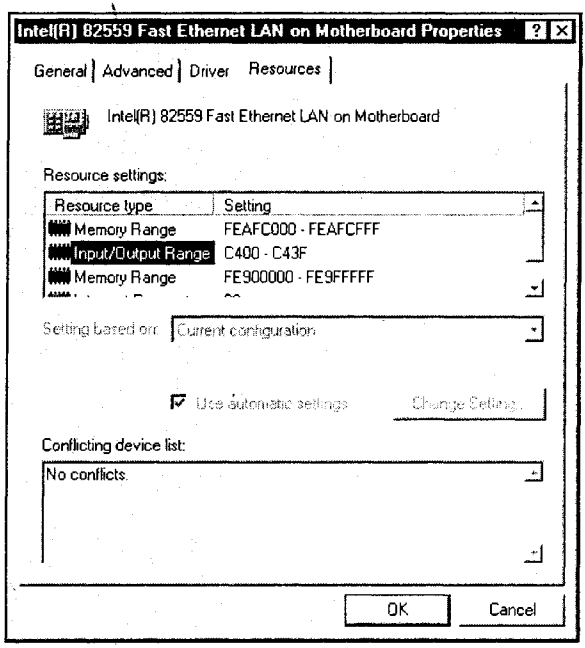


Рис. 22.6. Регулирование назначений ресурсов в операционной системе Windows 2000

Выберите одно из устройств в Device Manager и нажмите кнопку **Properties** (Свойства). В результате появится диалоговое окно **Properties**. После перехода на вкладку **Resources** (Ресурсы) (рис. 22.6) в окне настроек **Resource**, выведенном в середине

диалогового окна, обозначаются типы ресурсов, потребляемые данным устройством. Окно в нижней части этого диалогового окна содержит список конфликтующих устройств **Conflicting**, в котором обозначаются конфликты вместе с кодами ошибок. Взгляните на флажок **Use automatic settings** (Автоматическая настройка). Если Windows удалось обнаружить устройство, его флажок установлен. Это устройство должно работать в нормальном режиме. Впрочем, если настройки ресурсов основываются на **Basic Configuration x** (Текущая конфигурация x) (где x — это число от 0 до 9), то вам придется изменить настройки, выбрав из списка другую конфигурацию. Если конфигурация, которую вы хотите применить к устройству, не приведена в этом списке, можно нажать кнопку **Change Setting** (Изменить) и вручную отрегулировать значения ресурсов. Например, чтобы отредактировать настройки диапазона ввода/вывода, сделайте следующее.

1. Выделите настройку **Input/Output Range** (Диапазон ввода/вывода), которую предполагается изменить, и снимите флажок **User automatic settings** (Автоматическая настройка).
2. Нажмите кнопку **Change Setting** (Изменить).
3. Выберите для данного устройства подходящий диапазон ввода/вывода.

Не забывайте о сохранении изменений и перезагрузке системы (если в этом есть необходимость). Если в устройстве применяются перемычки или DIP-переключатели, то это устройство необходимо настраивать не через диалоговые окна **Properties**, а вручную.

Дополнительные ресурсы

APC: **www.apcc.com**.

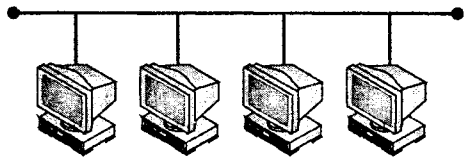
Dell: **support.dell.com**.

Gateway: **www.gateway.com**.

Intel: **www.intel.com**.

Kingston: **www.kingston.com**.

Microsoft: **support.microsoft.com**.



ГЛАВА 23

Введение в Web-серверы

Стремительный рост популярности Интернета в последние несколько лет в значительной степени обуславливается его доступностью. Возникновение Интернета относится к 1989 г., когда Европейская организация по ядерным исследованиям (CERN, European Center for Nuclear Research) в Женеве запустила проект публикации и связывания исследовательских данных в сети Интернет. С тех пор Web-технологии успели стать краеугольным камнем любительских и профессиональных публикаций. В современном мире лишь с большим трудом можно найти компанию, не присутствующую в Интернете, и даже простые люди регулярно помещают на свои семейные Web-сайты новые фотографии и видеоролики. Сегодня в Интернете работают сотни тысяч Web-серверов, представляющих многие миллионы Web-страниц активным покупателям, читателям, исследователям, студентам и другим категориям населения. Вполне возможно, что и ваша корпоративная сеть содержит один или несколько Web-серверов. В этой главе мы обсудим функции типичного Web-сервера, в качестве примера возьмем Microsoft Internet Information Server (IIS) 5.0 для Windows 2000 и рассмотрим некоторые общие проблемы, связанные с работой Web-сервера в современном Интернете.

Основы программного обеспечения Web-серверов

В Web-серверах функции принятия запросов браузеров и извлечения файлов (как правило, Web-страниц) выполняются серверным программным обеспечением. После этого происходит исполнение всех соответствующих CGI-сценариев, и, наконец, результаты отсылаются обратно клиенту. В ранних Web-программах применялся интерфейс командной строки. С развитием технологии в дело включилась графика. В начале 1993 г. в Национальном центре по применению суперкомпьютеров (NCSA, National Center for Supercomputing Applications) под руководством Марка Андреесена был разработан полностью графический браузер Mosaic. Впоследствии Андреесен работал в компании Netscape и спроектировал браузер Netscape Navigator, возвестивший наступление эпохи современных Web-браузеров под Windows, которыми мы пользуемся сегодня. На сегодняшнем этапе Web-страницы создаются с помощью языка разметки гипертекста (Hypertext Markup Language, HTML), а для их передачи

по сети Интернет применяется протокол передачи гипертекста (Hypertext Transfer Protocol, HTTP). Web-сервер функционирует безостановочно. Он работает через порт (обычно 80) на серверном компьютере. Браузеры отсылают на такие порты свои запросы. Некоторые серверные программы, присутствующие на рынке, поддерживают дополнительные функции сетевого обслуживания типа FTP или мультимедийных служб.

За последние несколько лет очень быстро развивались браузеры, но значительным изменениям подверглось и серверное программное обеспечение. В него были добавлены новые функции, поддерживающие различные виды информации (в особенности это касается мультимедийных средств); были разработаны и новые инструменты управления. Более того, некоторые серверные программы можно загрузить из Интернета совершенно бесплатно. На сегодняшний день распространено несколько типов серверного программного обеспечения.

- *Apache.* Свободно распространяемый Web-сервер Apache можно загрузить с сайта **www.apache.org**. Судя по подсчетам, Apache задействован более чем на 50% всех Web-серверов. Web-сервер Apache перенесен на многие компьютерные платформы, среди которых Windows NT/2000, UNIX/Linux и Novell NetWare.
- *Microsoft IIS.* Microsoft IIS бесплатно поставляется в комплекте операционных систем Windows NT и Windows 2000. Дополнительный пакет (Option Pack) для Windows NT (который можно загружать без ограничений) содержит компоненты, необходимые для обновления IIS до версии 4.0, хотя систему Windows 2000 сопровождает бесплатная версия IIS 5.0. Кроме того, компания Microsoft разработала Personal Web Server, предназначенный для семейства операционных систем Windows 9x. Его можно загрузить с Web-сайта по адресу **www.microsoft.com**.
- *iPlanet Web Server.* Ранее, еще до объединения компаний Netscape и Sun, он был версией Web-сервера Netscape для предприятий; теперь он поддерживается компанией iPlanet. Информацию о серверах iPlanet можно найти по адресу: **http://www.iplanet.com/products/iplanet_web_enterprise/home_web_server.html**.
- *Jigsaw Web Server.* Так называется Web-сервер на базе Java, созданный и сопровождаемый консорциумом W3C. Web-сервер Jigsaw распространяется бесплатно. Его можно загрузить с сайта **http://www.w3.org/Jigsaw/**.

Польза Интернета

Причина популярности Интернета заключается в его универсальности. Публикация текста и графики — это традиционные задачи, но они составляют лишь малую часть основных возможностей Интернета. Усовершенствование Web-языков и увеличение скорости обмена информацией привели к тому творческому буму, который продолжается и по сей день. На современных Web-сайтах можно проводить виртуальные встречи (они еще называются Web-конференциями), производить удаленное обращение к устройствам и управлять ими, получать удаленный доступ к базам данных и потоковым данным (например, к радио и телевидению), загружать библиотеки, обращаться к услугам автоматических справочных столов и выполнять огромное количество других творческих задач. Ниже приводятся лишь некоторые наиболее общие способы использования Интернета.

Распространение и сбор информации

За счет данных, хранящихся в Интернете, можно сэкономить много бумаги. Вместо того чтобы печатать уведомления, сообщая сотрудникам об изменении в политике компании, или приглашая их прийти на корпоративный праздник, вы можете создать Web-страницу и опубликовать на ней эту информацию. В результате вы не только избавитесь от необходимости раздавать уведомления, но также сможете прибегнуть к элементам оформления, применение которых не всегда оказывается возможным в формате электронной почты. При этом читателям не нужно будет обращаться к программе, в которой создавался исходный документ (например, к Adobe Acrobat). Публикация документов на Web-сайтах также устраняет возможность повреждения оригинального документа.

Другим преимуществом, связанным с публикацией документов в Интернете, является то, что у вас появляется возможность убедиться в том, что люди их читают. Вы можете не ограничиваться простой публикацией данных в надежде на то, что они дойдут до людей, которым нужны. Создайте раздел с кнопкой "Да, я действительно все прочел и понял". Тогда те, кто будет знакомиться с содержанием документа, смогут нажать на нее и таким образом отправить коммерческому директору (или любому другому лицу, которое должно об этом знать) подтверждение прочтения документа по электронной почте. Ничто не мешает вам создать некое подобие RSVP (Repondez, S'il Vous Plait — "ответьте, пожалуйста") в отношении рабочего совещания. Создайте форму, с помощью которой люди могли бы указывать, придут ли они, сколько гостей приведут, и сообщать любую другую относящуюся к делу информацию.

Обмен информацией и сотрудничество

Сеансы в чате вполне могут быть средством организации людей с целью проведения совещаний, когда собрать всех участников в одном месте физически невозможно. Диалоговые приложения являются одним способом выполнения такой задачи, а Web-чат — совершенно другим, причем Web-чатом может пользоваться любой человек, у которого есть браузер (а не только пользователи с установленным диалоговым приложением). Проведение видеоконференций также возможно посредством Web-интерфейса. Службы сетевых совещаний (например, WebEx по адресу **www.webex.com**) позволяют пользователям Интернета просматривать презентации, получать коллективный доступ к приложениям и рабочим столам. При наличии Web-программ планирования Интернет можно задействовать в целях группового планирования на случай, когда виртуальные совещания не справляются с этой задачей. К примеру, в Lotus Organizer есть сменный модуль для Интернета, с помощью которого люди могут составлять свои расписания на персональных или карманных компьютерах, а затем загружать эту информацию на Web-календарь. Таким образом, сотрудники точно знают, кто и где находится.

Другим примером может стать корпоративный Web-сайт, помогающий сотрудникам компании найти друг друга. Многие крупные предприятия состоят из лабиринтов небольших помещений и кабинетов. В такой компании далеко не все сотрудники знают друг друга в лицо. Одним из решений этой проблемы могла бы стать подготовка сетевой карты офисов компании с указанием кабинета каждого сотрудника. Как только пользователь вводит имя нужного работника, на карте выделяется расположение его кабинета и отображается его фотография.

Повышение уровня сопровождения

Наличие справочного стола на основе Интернета может значительно упростить процесс сопровождения. Во-первых, многие заявки пользователей предсказуемы. Они желают получить права доступа к определенному каталогу, у них не получается проверить электронную почту, они не могут найти файл и т. д. Вы можете создать форму, включив в нее объяснение распространенных проблем, и указать пользователям на необходимость обращения к ней. Если трудность, с которой столкнулся пользователь, отсутствует в этом списке, он может ввести ее описание в текстовом окне, помещенном на Web-странице. Кроме того, на этой странице могут указываться ссылки на FAQ, файлы с заплатами и обновлениями и на другие востребованные сопроводительные ресурсы.

Письменная фиксация содержания проблемы или необходимость выбора из ряда вариантов побуждают пользователей к анализу произошедшего и к составлению более полной характеристики неисправности, в сравнении с объяснением по телефону или при личной встрече. Зачастую перед вами ставится задача пройти первоначальный этап локализации проблемы, перейдя от объяснения типа "WordPerfect не работает" до "WordPerfect закрывается после появления сообщения о том, что компьютеру не хватает ресурсов". На локализацию неисправности может уйти несколько минут и даже больше. Для всех оказывается значительно проще и спокойнее предоставить пользователю возможность написать о возникшей трудности или выбрать ее из существующего списка. Необходимость в локализации некоторых проблем не исчезнет полностью, но задача значительно облегчится. Если нужно получить дополнительную информацию, это всегда можно сделать по телефону.

Сообщение о неисправности по электронной почте через Web-интерфейс также экономит время заявителя (время, затрачиваемое на описание проблемы) и сотрудника службы поддержки (время, затрачиваемое на выяснение сущности проблемы). Кроме того, к электронной почте можно обратиться почти всегда. Человеку, пытающемуся заявить о неисправности, не приходится дожидаться освобождения телефонной линии, чтобы дозвониться до центра поддержки.

Доступ к базам данных

Все более популярной в корпоративных внутренних сетях становится практика предоставления специалистам по продажам и менеджерам интерфейса для работы с базами данных. По сравнению с ежемесячной распечаткой стандартных отчетов, это значительное усовершенствование. Заготовленный отчет может не содержать ответов на вопросы специалистов по продажам или менеджеров. Более того, в данном случае опять возникает проблема распространения. Создание и доставка этих отчетов всем получателям в компании с рассредоточенной структурой связаны со значительными усилиями.

В некоторых корпорациях пользователи могут отсылать запросы на сервер баз данных посредством электронной почты. Для этого они не должны знать синтаксис языка структурированных запросов (SQL, Structured Query Language). Пользователи формулируют вопросы с помощью стандартного языка, который активирует заранее заготовленный запрос. Более подготовленные пользователи, знакомые с синтаксисом SQL, получают возможность отправлять по электронной почте запросы на SQL и, следовательно, получать специальные ответы. Кроме того, если людям нужно внести изменения в базу данных или создать отчет, тщательно спроектированное

Web-приложение позволяет им это делать. Для этого совершенно не обязательно уметь работать с внешним интерфейсом базы данных (например, с Access). Вполне возможно создать внешний интерфейс, который будет преобразовывать запросы, сформулированные пользователями, в запросы на языке SQL, применяемом в базах данных.

Распространение файлов

Вполне возможно, что вы захотите предоставить пользователям право доступа к определенным файлам, но не к каталогам, в которых они хранятся. Быть может, эти каталоги расположены в области медленного соединения глобальной сети, или же в них хранятся файлы, о существовании которых посторонним знать не следует. В таком случае вы можете настроить FTP-узел таким образом, чтобы он превратился в централизованное хранилище входящих и исходящих файлов. При этом пользователи смогут загружать файлы как в "общедоступный" каталог, так и из него. Уровень защиты зависит от того, как вы его настроите (будет ли уровень доступа зависеть от пароля, будет ли он ограничен для определенных пользователей или, напротив, открыт для всех зарегистрированных пользователей). К примеру, если в вашей сети есть пользователи, разбирающиеся в компьютерах, имеет смысл хранить программные обновления в одном месте. В таком случае пользователи смогут получать установочные файлы с FTP-узла, не тратя время на их поиск на собственных дисках и не обращаясь к службе поддержки для проведения обновлений собственных приложений.

Публикация исследований

Еще один способ применения Интернета предполагает совместное использование исследовательских данных отделами крупных организаций. Например, предположим, что некоторые учреждения в структуре Министерства обороны США располагают совместной внутренней сетью. В этой внутренней сети есть база данных с Web-интерфейсом под названием IntelLink, в которой публикуются данные, собранные аналитическими отделами. Пользователи IntelLink (включая стратегических руководителей, военнослужащих, управленцев и всех прочих пользователей, имеющих права доступа) могут обращаться к базе данных за отчетами по странам, изображениям, картам и военному оборудованию. Не будь такой Web-программы, всем этим людям пришлось бы прибегать к услугам аналитиков, чтобы те составляли для них отчеты. Аналитики, несмотря ни на что, будут выполнять специальные доклады и проводить совещания, однако часто запрашиваемая информация не потребует с их стороны дополнительных усилий.

Языки разметки

Если вы когда-нибудь работали в Интернете, то знаете, что Web-страница состоит не только из элементов текста и графики, выводимых на экран. Нельзя просто сбросить текст на Web-страницу, чтобы он сам по себе выглядел так, как нужно. Его надо закодировать, чтобы браузер мог представить страницу в соответствии с первоначальным замыслом. Это часто называется Web-программированием, но правильнее будет сказать, что страница "размечается" в расчете на браузер. По существу, *язык разметки* — это совокупность кодов, которые помещаются в тело документа. Эти коды определяют то, как текст, графика и другие визуальные элементы должны

выглядеть при печати или выводе на экран (или определяют их логическую структуру, например, абзацы и маркеры). Не будь языка разметки, данные выводились бы в виде необработанного текста безо всякого форматирования символов или абзацев.

Язык разметки определяет внешний вид документа посредством кодов (называемых тегами) в форме <tag>...</tag>. Первый тег обозначает точку начала форматирования, а второй тег (с косой чертой) — точку завершения кодирования. Стоит лишь забыть проставить второй тег, и кодирование, соответствующее первому тегу, будет применяться вплоть до конца документа. К примеру, при необходимости выделить предложение полужирным начертанием, воспользовавшись для этого элементарным языком разметки, соответствующий синтаксис нужно представить следующим образом:

```
<strong>
Это - приложение, написанное полужирным шрифтом
</strong>
```

При просмотре этого текста в браузере предложение действительно оказывается выделенным полужирным начертанием. Язык разметки может применяться к необработанному тексту как с помощью текстового редактора (например, Notepad), так и посредством графических инструментальных средств (например, FrontPage), которые кодируют текст по мере того, как вы визуально структурируете его в соответствии со своими предпочтениями. Во время обучения работать с графическими инструментами легче, но они далеко не всегда оказываются такими же точными и действенными, как средства текстового редактирования. Ниже перечислено несколько типов языков разметки, о которых вам нужно иметь представление.

Примечание

Мы не собираемся детально рассматривать Web-дизайн и языки разметки на этих страницах, но вы сможете оценить степень важности каждого языка разметки.

Язык разметки гипертекста (HTML)

Язык разметки гипертекста (HTML) — это основное средство кодирования Web-страниц, базис большинства из них. HTML позволяет публиковать текст и рисунки, отображать содержимое таблиц стилей и даже создавать отчеты по базам данных для их прочтения прямо в сети. Этот язык хорошо справляется со структурированием и форматированием всех видов статической информации. Коды HTML дают возможность:

- устанавливать размеры текста и шрифтов;
- применять к тексту форматирование в виде полужирного, курсивного или подчеркнутого начертаний;
- обозначать ссылки на другие страницы (они называются гиперссылками);
- помещать на страницы изображения (например, файлы JPG или GIF);
- создавать отдельный заголовок для каждой страницы;
- создавать таблицы;
- помещать на страницы данные, применяемые поисковыми системами.

Примечание

Метаданные — это скрытые данные, которые не отображаются на Web-странице, но могут потребоваться поисковой системе для направления посетителей на данный сайт.

Есть три типа тегов HTML: теги, отвечающие за форматирование текста или отдельных символов; теги, выполняющие форматирование абзацев или других блоков текста, и, наконец, невидимые теги, поддерживающие другие функции (например, метаданные для проведения поиска). Пример исходного кода HTML показан на рис. 23.1. Довольно часто для дополнения HTML применяются более современные языки разметки, но сам он располагает практически повсеместной поддержкой, что, несомненно, является преимуществом. Текущая версия HTML поддерживается почти всеми браузерами (и совершенно точно любым современным графическим браузером), хотя, что касается других языков типа Dynamic HTML (DHTML), XML, Java и ActiveX, это не всегда так. При необходимости организовать доступ к Web-сайту из браузеров различных типов имеет смысл воспользоваться именно HTML.

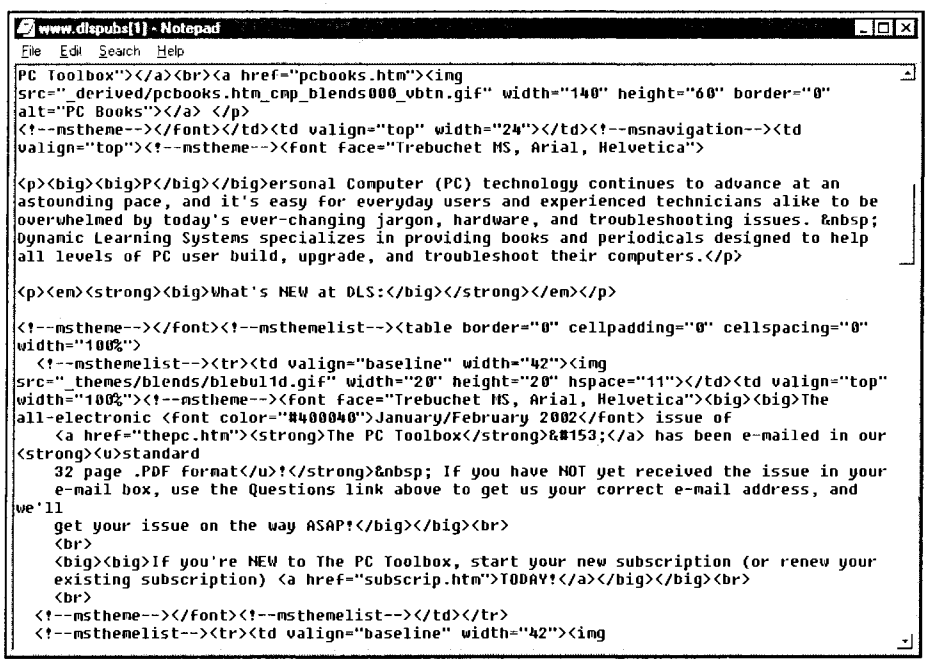


Рис. 23.1. Браузер может вывести исходный код HTML, из которого и состоит Web-страница

Динамический HTML (DHTML)

Язык Dynamic HTML (или DHTML) привносит в HTML большую степень гибкости. Вместо того чтобы предоставлять посетителям статическую Web-страницу, посредством DHTML можно создать страницу, настраиваемую пользователем, при этом не повреждая исходный документ. К примеру, страница, подготовленная с помощью

DHTML, может содержать перемещаемые элементы, позволяющие пользователю перегруппировать ее содержимое. Впрочем, при обновлении страницы все изменения теряются, и происходит восстановление ее первоначального внешнего вида. DHTML поддерживает следующие функции, которые отсутствуют в HTML:

- динамические стили;
- точное позиционирование;
- привязка данных;
- динамическое содержимое.

Динамические стили основываются на правилах каскадных таблиц стилей (Cascading Style Sheets, CSS). Они применяются к странице, избавляя от необходимости ручного форматирования ее разделов. Если вы пользуетесь современным текстовым редактором, то, вероятно, имеете представление о таблицах стилей, которые автоматически форматируют блоки текста определенным образом (в зависимости от назначенного стиля). Форматирование может содержать цвет текста, его шрифт, позиционирование, обозримость и практически любые другие свойства, влияющие на представление текста. Таблицы CSS (через расширенные возможности языка DHTML) выполняют точно такие же функции, но применяются не к документам текстового процессора, а к Web-страницам. Динамические стили DHTML предусматривают некоторые возможности, отсутствующие в текстовых процессорах. Например, вы можете разметить текст так, чтобы при помещении курсора мыши над ссылками их цвет автоматически менялся, или чтобы появлялся текст при перемещении курсора над определенным незаполненным пространством. Единственная трудность, связанная с этими стилями, заключается в том, что большинство документов приходится связывать с таблицами стилей. Эта задача требует немалых усилий, в особенности от новичков или от людей, которые выполняют преобразование документов. При условии корректной реализации таблицы стилей Web-издатель может с легкостью изменять внешний вид одной или нескольких страниц. Динамическое содержимое страниц предоставляет пользователю возможность изменить ее внешний вид путем запуска сценария, например, для выполнения следующих задач:

- вставки или скрытия элементов страницы;
- изменения текста;
- изменения компоновки страницы;
- извлечения данных из серверных источников и их отображения на основе пользовательского запроса.

В отличие от языка HTML, который предусматривает возможность изменения содержимого страницы лишь перед ее загрузкой в браузер пользователя, DHTML может принимать изменения в любой момент. Вместе со сценариями, позволяющими пользователю просматривать лишь нужные элементы, динамическое содержимое обеспечивает высокий уровень интерактивности.

Другой возможностью DHTML является точное указание положения элемента на странице, которое задается с помощью координат x (горизонтальной), y (вертикальной) и даже z (трехмерное расположение объектов предусматривает возможность их наложения друг на друга). Точное позиционирование делает возможным расположение текста вокруг иллюстраций и изменение положения объектов в соответствии

с размером окна браузера. HTML без CSS не поддерживает точное размещение. При этом позиционирование элементов зависит от браузера.

Для того чтобы пользователи могли обратиться к серверной информации (например, к базе данных), обычные страницы HTML должны связаться с сервером, на котором хранятся эти исходные данные, и запросить для пользователей разрешение на манипулирование ими. DHTML предусматривает привязку данных к определенной странице, благодаря чему пользователи получают возможность работать с нужными данными, не обращаясь к источнику исходных данных и даже не связываясь с сервером, на котором хранятся оригинальные данные. Напротив, источник данных является компонентом страницы, и, подобно базе данных, его можно сортировать и фильтровать. В результате снижается нагрузка на серверы, а пользователи могут просматривать и манипулировать данными, не обращаясь к их источнику.

Расширяемый язык разметки (XML)

Расширяемый язык разметки (Extensible Markup Language, XML) — это сравнительно новое средство Web-кодирования, поддерживающее HTML, но делающее Web-страницы несколько более гибкими. При форматировании страницы средствами HTML вы можете изменить внешний вид текста, пользуясь тегами полужирного или курсивного начертания, конца абзаца и т. п. Но эти теги ничего не сообщают о содержимом текста. Они лишь определяют его внешний вид. XML не ограничивается тегами, с помощью которых задается предполагаемый внешний вид текста. Напротив, средствами этого языка маркируется смысловое содержание текста (обозначаются имена, адреса, названия продуктов и т. д.)

Подобные метаданные могут значительно упростить задачу обнаружения заданных элементов поисковыми системами. Если вы попытаетесь выполнить поиск на корпоративном Web-сайте (созданном средствами HTML) по ключу "name", желая получить данные обо всех упомянутых на нем именах, в результатах поиска будут возвращены все случаи включения в текст слова "name", но не сами имена. С другой стороны, если бы сайт был закодирован с помощью XML, в качестве результатов поиска был бы выведен любой текст, обозначенный как `name` (имена). Маркирование частей текста удобно, если вы хотите применить какое-либо правило (связанное, например, с цветом или языком) только к определенным частям Web-документа. Предположим, что в документе приводится небольшой рассказ на испанском языке и его перевод на английский. Вместо того чтобы переключаться между поддержкой испанского и английского в рамках одного документа, вы могли бы обозначить все части рассказа тегом `<story></story>` и применить правило испанского языка только к ним, а перевод оставить на английском. В конечном счете преимущество от применения XML появляется в том случае, если оформление вашей Web-страницы выиграет от изолирования некоторых ее текстовых элементов.

Языки приложений и сценариев

Вплоть до настоящего момента мы рассматривали языки разметки, которые определяют внешний вид страницы и представляют на ней данные. Впрочем, сами страницы не выполняют никаких функций, кроме вывода информации. Разработчики объединили под маркой Web-дизайна языки составления приложений и сценариев. С их помощью Web-страницы запрашивают данные и различными способами взаи-

модействуют с пользователями. На клиентской стороне в качестве таких средств выступают элементы управления ActiveX и Java-апплеты. Клиентские Web-приложения и программы могут загружаться с Web-сервера и выполняться с использованием ресурсов клиентского компьютера. На клиентской стороне постоянно содержатся чат-программы и другие приложения, которые могут быть задействованы многократно, пока страница остается открытой.

Что касается серверной стороны, указанные программы могут воспользоваться общим шлюзовым интерфейсом (Common Gateway Interface, CGI) для обращения к программам, хранящимся на сервере, или задействовать серверный сценарий, встроенный в страницу средствами активных серверных страниц от Microsoft (Active Server Pages, ASP). Web-приложения серверной стороны выполняются на сервере с использованием его рабочей среды и ресурсов. Приложения на сервере более подходят для разовых обращений (например, это касается поисковых систем).

Преимуществом приложений, работающих на сервере, является их совместимость. Браузеру не приходится поддерживать язык приложений на компьютере клиента. Методики хранения и загрузки таких программ могут отличаться друг от друга. К примеру, в CGI происходит обращение к приложению, которое хранится на сервере, в то время как технология Active Server Pages предполагает хранение исполнимого сценария на самой странице HTML.

Java и ActiveX

Java — это межплатформенный язык, разработанный компанией Sun Microsystems. Важнейшей концепцией Java является межоперабельность — апплеты Java (мини-программы) выполняются на любой платформе (включая DOS, Windows, UNIX, NT и т. д.)[1]. При запуске Java-апплета он в первую очередь создает для себя среду исполнения (которую называют "песочницей"), а затем работает в ее контексте. Теоретически, песочница позволяет апплету работать на любой платформе, т. к. создает такую рабочую среду, которая нужна апплету в определенных условиях. Кроме того, песочница не допускает воздействие апплета на собственную рабочую среду.

Возможно, вы уже встречались с такими Java-апплетами, как Netcaster браузера Netscape Communicator, а также с планировщиками поездок, применяемыми на некоторых туристических Web-сайтах. Netcaster представляет собой внешний интерфейс технологии сбора данных Netscape (т. е. извлечения информации с Web-сайтов без их фактического посещения). Планировщики поездок получают введенные вами данные о предпочтениях, проводят поиск по базе данных авиарейсов в списках записей, отвечающих вашим потребностям, а затем возвращают все возможные соответствия.

Технология ActiveX похожа на Java тем, что она также является методом прикрепления мини-программ к Web-страницам; впрочем, они не идентичны. Вместо того чтобы предоставить платформенно-независимый язык программирования, технология ActiveX предлагает множество элементов управления, доступных через браузер, написанных на различных языках (например, на C++, Delphi, J++ и Visual Basic), из которых можно создавать приложения. Элементы управления ActiveX не работа-

[1] При условии, что на ПК установлена виртуальная машина Java. — *Ред.*

ют в "песочнице". Они запускаются в пользовательской рабочей среде точно так же, как и любое другое приложение.

CGI и ASP

Общий шлюзовой интерфейс (CGI) — это стандартный метод передачи информации, введенной пользователем, серверному приложению или сценарию с последующей передачей ответных данных браузеру клиента. К примеру, когда вы заполняете сетевую форму регистрации и нажимаете кнопку **Submit** (Передать), переданная вами информация может перейти в базу данных посредством CGI. После обработки введенных данных вы получаете ответ в виде благодарности ("Thank You!"), и это происходит с помощью CGI. Большим преимуществом CGI является устойчивость. Вне зависимости от того, на основе какой платформы работает сервер, данные в любом случае передаются от пользователя приложению. Принципиальных отличий от результата, получаемого с помощью языка сценариев, нет. Но принцип работы другой. Сценарий прикрепляется к определенной Web-странице, а программа, обращение к которой происходит через CGI, не привязана ни к одной странице (скорее к определенному шлюзу), так что ассоциировать себя с данным шлюзом может любая Web-страница.

Активные серверные страницы (Active Server Pages, ASP) — это еще одно средство обеспечения работы Web-страниц. В некоторые Web-страницы встраиваются сценарии, которые запускаются, когда того требуют создавшиеся условия (к примеру, когда пользователь нажимает кнопку **Find** поисковой системы или кнопку **OK** после заполнения формы). Для создания файла ASP нужно встроить в документ HTML сценарий, написанный на VBScript или другом поддерживаемом языке сценариев, а затем сменить расширение получившегося документа на asp. Когда пользователь загрузит такую страницу и выполнит заданные условия, сценарий активируется.

Публикация информации

Создание информации для публикации в Интернете — это лишь начало. В любом случае необходимо сделать так, чтобы эта информация хранилась на сервере (т. е. опубликовать данные в Интернете). Возможность организации HTTP-сервера (а значит — создания интранет- или интернет-сайта) присутствует почти во всех операционных системах. Существует большое количество вариантов публикации документов HTML как внутри (интранет), так и вне (Интернет) вашей сети. По существу, публикация документов HTML заключается в помещении их копий на сервер. Посетители (с помощью браузера) указывают серверу на те материалы, которые им нужны, и сервер реагирует, отображая запрошенные страницы. Как правило, публикация документов HTML может проходить тремя способами:

- с помощью вашего поставщика услуг или службы Web-хостинга в Интернете;
- с помощью информационной службы вашей компании во внутренней сети или в Интернете;
- на вашем сервере в интранете.

Виртуальные домены

В ранний период существования Интернета URL-адрес должен содержать имя сервера поставщика услуг Интернета (Internet service provider, ISP). К примеру, если бы

ваша компания называлась SuperWidgets, и вы сотрудничали с поставщиком услуг под названием myweb.com, то адрес вашей домашней страницы, вероятно, выглядел бы следующим образом:

```
http://www.myweb.com/~superwidgets/home.htm
```

Чтобы оказаться на вашей домашней странице, пользователь должен был ввести такой URL-адрес в адресной строке браузера (некоторые поставщики услуг Интернета, оказывающие их на безвозмездной основе, работают таким образом до сих пор). С технической точки зрения, в этом нет ничего плохого, но такой адрес не нагляден, и вряд ли пользователям придет на ум искать ваш сайт на чужом сервере. К счастью, имя сервера, на котором размещен сайт, не обязательно должно составлять хостовую часть URL-адреса. Вместо этого можно приобрести виртуальный домен. В результате вы получите собственное имя хоста, но файлы, составляющие ваш сайт, тем не менее, будут расположены на сервере (серверах) поставщика услуг Интернета. Если создать виртуальный домен типа superwidgets.com, пользователи смогут попасть на ваш сайт, наугад набрав адрес

```
http://www.superwidgets.com
```

На сегодняшний день виртуальные домены очень часто применяются небольшими компаниями и организациями. Получается, что их данные размещаются у поставщика услуг Интернета, но у пользователей создается впечатление о наличии у компании собственного сервера (кроме того, клиентам становится легче их найти). Но обладание виртуальным доменом — это не только вопрос тщеславия и индивидуальности. Есть и более существенные преимущества. К примеру, виртуальный домен обеспечивает вашу устойчивость. Доменное имя (и URL-адрес) сохраняется даже в случае перехода к другому поставщику услуг. Не будь виртуального домена, смена поставщика услуг (или организация собственного Web-сервера) потребовала бы изменения адреса и усложнила бы для клиентов задачу поиска сайта вашей компании.

Проще всего приобрести виртуальный домен, попросив своего поставщика услуг Интернета о его установке. Как правило, за первоначальную установку выплачивается от 20 до 100 долларов; к этому нужно прибавить $50, которые уходят в информационный центр InterNIC (**http://www.internic.net** — самая главная служба регистрации доменных имен) за регистрацию доменного имени сроком на два года. Если отношения с поставщиком услуг не сложились, вы можете создать виртуальный домен самостоятельно, тем самым сэкономив несколько долларов. Для проверки доменного имени, выполните следующие действия.

1. Зайдите на сайт **www.networksolutions.com**.
2. Введите доменное имя, которое предполагается зарегистрировать, в поле **Enter a domain name**. К примеру, можно ввести что-нибудь вроде **breakfastbuffetatnight.com** или **eatmoreofjoesgreatburgers.com**. Если вам повезет, на экране появится список возможных имен, включая то, которое вы указали. Это значит, что указанный домен свободен.
3. Зарегистрируйте выбранное имя самостоятельно или попросите поставщика услуг Интернета сделать это за вас. Большинство поставщиков услуг не взимают плату за регистрацию доменных имен при условии, если они же будут их размещать. В противном случае они просят за такую услугу приемлемую плату (обычно $100 или менее) плюс стоимость размещения. Если вы решите провести реги-

страцию самостоятельно, всю необходимую информацию и инструкции можно получить на сайте Network Solutions.

Естественно, как только соответствующий Web-сервер заработает, вам придется обслуживать каждый виртуальный домен. С одной стороны, каждому домену можно присвоить IP-адрес, а затем привязать все эти IP-адреса к одному и тому же хосту, на котором работает нужная Web-служба. При подключении через порт 80 IP-адрес будет перенаправлять посетителя на нужную страницу. Другой способ заключается в том, чтобы задействовать единственный IP-адрес, а серверное программное обеспечение в таком случае определит нужную страницу исходя из имени, указанного в рамках URL-адреса. Это и есть основные сведения, которые необходимо знать любому администратору Web-сервера.

Поставщики услуг Интернета и Web-хостинг

Довольно часто документы HTML публикуются на Web-пространстве, которое предоставляется поставщиком услуг Интернета (ISP). Поставщики обычно оказывают массу интернет-услуг (включая предоставление Web-пространства) и помогают своим клиентам удовлетворить их потребности, связанные с Web-разработкой. У каждого ISP есть собственный диапазон услуг, и для того, чтобы узнать, какие услуги предоставляются каждым поставщиком, каковы первоначальные взносы и помесячная плата, вам потребуется провести некоторые исследования. Впрочем, как правило, большинство поставщиков услуг предлагает либо индивидуальные, либо корпоративные пакеты услуг.

Также можно воспользоваться службой Web-хостинга. Такие службы не предоставляют коммутируемый доступ к Интернету. Они лишь выделяют клиентам пространство для сопровождения их Web-публикаций. Как правило, услуги Web-хостинга приобретаются вместе с услугами Интернета (тем самым выгодная сделка по Web-хостингу сопровождается надежным коммутируемым доступом). Вполне возможно, что удовлетворить все ваши потребности сможет одна компания, но нелишне и присмотреться к разным компаниям.

Примечание

Вполне возможно, что вы намереваетесь установить собственные Web-серверы, однако для новых предприятий, которые хотят передать издержки по сопровождению сервера сторонней организации, обращение к поставщику услуг Интернета представляется вполне приемлемым вариантом.

Индивидуальные пакеты услуг

Частные лица и небольшие предприятия могут выиграть от низкой стоимости и доступности индивидуальных пакетов услуг. Обычно поставщики услуг Интернета снабжают индивидуальных клиентов доступом к сети Интернет, одним или несколькими почтовыми учетными записями и относительно небольшим пространством на Web-сервере (оно составляет 5—50 Мбайт). Помимо этого, многие поставщики услуг Интернета предоставляют другие службы (например, перенаправление данных, введенных в форму, по электронной почте). Конкретный набор служб, который вам нужно заказать, зависит от того, что вы намереваетесь делать со своими

HTML-страницами. К примеру, если вы планируете создать и опубликовать несколько простых документов HTML, для этого требуется лишь крайне ограниченное Web-пространство. С другой стороны, если вы намереваетесь разработать Web-сайт, гигантский по своим масштабам или заполненный мультимедийными и загружаемыми файлами, вам, вероятно, понадобится дополнительное Web-пространство. Если предполагается задействовать формы или возможности, характерные для конкретного сервера, потребуется доступ к серверу или наличие на нем определенных программ. Сначала определитесь с тем, что вы хотите сделать, а затем уже найдите поставщика услуг, который сможет удовлетворить ваши потребности. Помимо прочего, необходимо принять во внимание еще несколько факторов.

- *Выберите сервер и платформу.* Решив, каким сервером и какой платформой вы хотите воспользоваться, можно определить, какие сценарии окажутся в вашем распоряжении. К примеру, если сервер Apache работает на станции Sun SPARC (Scalalable Processor Architecture — наращиваемая архитектура процессора), такая конфигурация встречается у многих поставщиков услуг Интернета, у вас есть основания попросить администратора сервера установить определенные сценарии Perl. С другой стороны, если вы размещаетесь во внутренней сети с сервером Netscape на базе Windows NT и хотите перейти на сервер WebStar на базе Macintosh, знайте, что эти две конфигурации несовместимы.
- *Узнайте о системе защиты.* Например, всей планете совершенно не обязательно знать о том, что вы на своем сервере проводите тестирование страниц. Избежать этой проблемы помогает организация доступа к сайту на основе паролей. Кроме того, если на сайте есть некоторые страницы, к которым должны обращаться лишь отдельные лица (или все, кроме некоторых лиц), вы должны иметь возможность задать пароли (в идеале, эта задача должна выполняться быстро и с легкостью). Если вам нужна безопасность, необходимо знать возможности каждой службы и ее ограничения.
- *Узнайте о сценариях.* Если вы можете устанавливать и выполнять собственные сценарии, то степень гибкости и возможности, которыми вы обладаете, оказываются значительно выше. Если же вы ограничены тем, что предварительно установил поставщик услуг Интернета, то у вас будет доступ лишь к некоторым ограниченным возможностям (например, к чатам), но осуществить все то, что вам нужно, видимо, не получится.
- *Узнайте о функциях отчетности и регистрирования.* Если вы занимаетесь обслуживанием, рекламируете свою компанию или вовлечены в любой другой вид деятельности, предполагающий ознакомление с вашими сообщениями большого количества людей, вы должны проверить, регистрируются ли случаи доступа, и научиться самостоятельно обращаться к соответствующим журналам регистрации. Если ваш поставщик услуг Интернета не предусматривает ведение журналов регистрации доступа и активности, то вам придется выбрать другую компанию.
- *Узнайте об уровне обслуживания и поддержки.* Информация, опубликованная в Интернете, должна быть постоянно доступна. Следовательно, поставщик услуг Интернета должен обеспечивать достаточно высокий уровень надежности. На случай возникновения неисправностей вы должны знать, как связаться со службой поддержки поставщика услуг. Кроме того, вы должны уметь создавать резервные копии, а при необходимости и проводить восстановление данных.

Корпоративные пакеты услуг

Если ваше предприятие работает (или, согласно вашим планам, будет работать) в Интернете, лучше заказать у поставщика услуг Интернета корпоративный пакет услуг. Обычно он стоит дороже, чем индивидуальный пакет, но почти всегда предполагает выделение более значительного Web-пространства (100—500 Мбайт), более полный доступ к программам, работающим на сервере (например, к сценариям CGI для обработки сложных форм), а также предоставление комплексных услуг, в число которых иногда включено оформление Web-страниц. Кроме того, некоторые корпоративные пакеты услуг обеспечивают гарантированный период работоспособности, проведение регулярных операций резервирования, а также более внимательное отношение к потребностям бизнеса.

Корпоративные серверы

Web-документы также можно разместить на корпоративном сервере, который обычно располагается на вашем рабочем месте. Если вы работаете на крупную компанию или образовательное учреждение, а также если вы сотрудничаете с организацией или группой, которая выполняет задачи, связанные с системным администрированием, то у вас должен быть доступ к Web-серверу. Все необходимые компоненты (такие как права доступа, администрирование и система защиты), скорее всего, присутствуют, и вам остается лишь начать пользоваться сервером.

Уровень доступа и контроля, которым вы располагаете, зависит от конкретной компании. В идеальной ситуации работоспособность сервера обеспечивает кто-то другой, но он же предоставляет вам обширные возможности по использованию этого сервера. Если вам повезет, то при настройке и запуске программ, работающих на сервере, вам окажут помощь, и вы сможете делать все, что будет необходимо в целях предоставления информации. В худшем случае вам придется придерживаться строго определенного процесса представления информации во внутреннюю сеть. Вы будете подавать документы HTML, но впоследствии вряд ли сможете следить за тем, где они будут размещены и как связаны. Вполне возможно, что позиция вашей компании будет находиться где-то между этими крайностями. В ней будет существовать стандартная процедура доступа в корпоративную внутреннюю сеть, но при этом вам будет предоставлена значительная свобода действий. Если же процесс предоставления информации находится под жестким контролем, лучше создать собственный сервер.

Ваши собственные серверы

Предположим, что вам захочется публиковать свои Web-документы на собственном сервере. Если вы обладаете достаточными техническими знаниями, и в вашем распоряжении есть существующая сетевая инфраструктура, то, запустив свой собственный сервер, вы сможете добиться наибольшей гибкости и получить самый широкий диапазон ресурсов для Web-разработки. Одним из преимуществ, связанным с наличием собственного сервера, является то, что он является более аутентичной средой разработки и тестирования страниц. У вас появляется возможность исполнять страницы "вживую", не демонстрируя их остальным сотрудникам компании (и пользователям Интернета). К примеру, если URL-адреса, задействованные в ваших ссылках, относятся к определенному серверу, они будут работать при загрузке соответствую-

щих файлов с сервера, и не будут работать при загрузке тех же файлов в локальном режиме.

При наличии относительно современного настольного компьютера вы сможете использовать его в качестве Web-сервера. К примеру, устаревший компьютер Pentium или Pentium II с 32—64 Мбайт оперативной памяти (или с большим ее объемом) на базе Windows NT/2000 как сервер может оказаться вполне достаточным для проведения тестирования (именно для тестирования, т. к. такой сервер не предназначен для обслуживания значительного трафика). Если вы предпочитаете Linux, на этом Web-сервере можно установить и эту операционную систему. Для того чтобы организовать общедоступный сервер на работе или в домашних условиях, вам понадобится выделенная линия. Для этих целей подойдет как постоянная линия ISDN, так и прямое кабельное/DSL-соединение (этого вполне достаточно для тестирования).

IIS 5.0 для Windows 2000 Server

Теперь, когда вы имеете некоторое представление об основах функционирования Интернета, самое время приступить к анализу функций, установки и применения настоящего Web-сервера. На рынке существует несколько Web-серверов, но мы рассмотрим только IIS 5.0, входящий в пакет Windows 2000. Он представляет собой Web-службу на базе Windows 2000, позволяющую публиковать данные во внутренних сетях и в Интернете. В IIS 5.0 появилось множество новых функций, помогающих Web-администраторам создавать масштабируемые, гибкие Web-приложения.

Установка IIS

Web-сервер IIS по умолчанию поставляется вместе с операционной системой Windows 2000 Server, хотя установить и запустить его придется вручную. С помощью программы **Add/Remove Programs** (Установка и удаление программ), обращение к которой производится через **Control Panel** (Панель управления), вы можете удалить IIS или установить его дополнительные компоненты. Чтобы выполнить инсталляцию Web-сервера IIS, добавить или удалить его компоненты в системе Windows 2000, сделайте следующее.

1. Выберите **Start** (Пуск), **Settings** (Настройка), **Control Panel** (Панель управления), **Add/Remove Programs Wizard** (Установка и удаление программ).
2. Нажмите кнопку **Add/Remove Windows Components** (Добавление и удаление компонентов Windows), а затем, чтобы инсталлировать IIS, установить или удалить его компоненты, следуйте инструкциям на экране (рис. 23.2).

Примечание

Если вы выполнили обновление системы до Windows 2000, IIS 5.0 должен быть установлен по умолчанию лишь в том случае, если другая его версия была установлена в предыдущей версии Windows.

Что касается удаления IIS, нужно иметь в виду, что оно не всегда выполняется полностью (особенно если на сервере была размещена пользовательская информация). Нижеследующие каталоги, содержащие пользовательские данные, останутся в системе даже после полного удаления IIS:

- \Inetpub;
- \%systemroot%\Help\iisHelp;
- \%systemroot%\system32\inetsrv.

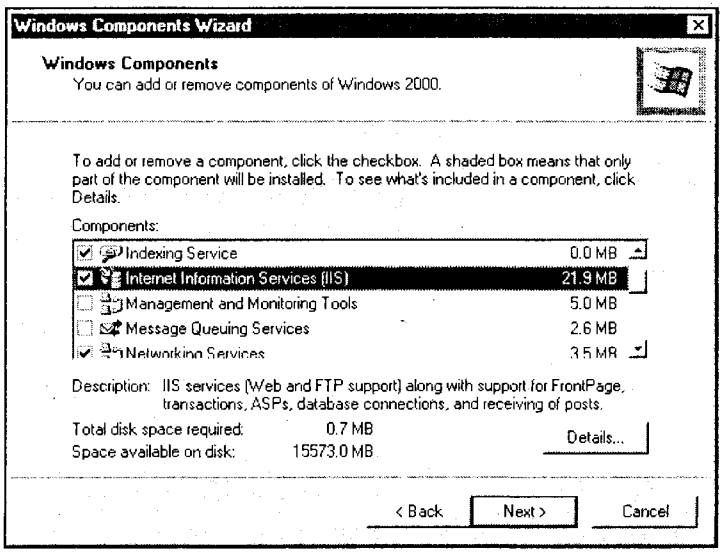


Рис. 23.2. Установка, удаление и изменение состава IIS в Windows 2000 производится при помощи мастера Components Wizard

Быстрая настройка сайта средствами IIS

При установке Windows 2000 Server IIS создает Web-сайт и FTP-сайт по умолчанию. После установки IIS публикация данных на сайте (сайтах) по умолчанию производится с помощью общих процедур, представленных ниже. Для публикации данных на Web-сайте необходимо выполнить следующие действия.

1. С помощью программы авторской разработки (например, Microsoft FrontPage) создайте домашнюю страницу Web-сайта.
2. Назовите файл домашней страницы default.htm, default.html или default.asp.
3. Скопируйте домашнюю страницу в принимаемый по умолчанию каталог Web-публикаций IIS. Каталог Web-публикаций по умолчанию иногда называется домашним каталогом. Программа установки (Setup) предлагает разместить его по адресу \Inetpub\Wwwroot.
4. Если в вашей сети есть система разрешения имен (обычно эту функцию выполняет DNS), то для перехода на ваш сайт посетителю достаточно ввести в адресной строке браузера имя вашего компьютера (например, author1.example.net). Если же система разрешения имен в сети отсутствует, пользователям придется вводить числовой IP-адрес вашего компьютера.

Публикация данных на FTP-сайте также не представляет трудности.

1. Скопируйте или переместите файлы в принимаемый по умолчанию каталог FTP-публикаций. Программа установки (Setup) предлагает для этого каталог \Inetpub\Ftproot.
2. Если в вашей сети есть система разрешения имен (обычно эту функцию выполняет DNS), то для перехода на ваш сайт посетителю достаточно ввести в адресной строке браузера префикс **ftp://**, а за ним имя вашего компьютера. В противном случае посетителям придется вводить **ftp://** и числовой IP-адрес вашего компьютера.

Добавление сайтов

Web-сервер способен обеспечить работу нескольких сайтов. Размещение в системе новых сайтов производится путем запуска мастера сайтов. Для добавления нового сайта на Web-сервере необходимо выполнить следующие действия.

1. Выберите компьютер (или сайт) в оснастке IIS[1] и нажмите кнопку **Action** (Действие).
2. Для запуска мастера сайтов (рис. 23.3) выберите **New** (Создать), **Web Site** (Веб-узел) (или **New**, **FTP Site**).

Рис. 23.3. Организация новых Web-сайтов на сервере осуществляется с помощью мастера Web Site Creation Wizard

3. Чтобы указать данные, идентифицирующие новый сайт, следуйте инструкциям на экране. Необходимо ввести адрес порта и путь к домашнему каталогу сайта.

[1] Эта оснастка доступна через последовательность команд: Пуск, Программы, Администрирование, Диспетчер служб IIS. — *Ред.*

Если вы пытаетесь воспользоваться заголовками хоста, чтобы связать с единственным IP-адресом дополнительные сайты, необходимо указать имя заголовка хоста.

Примечание

Все записи Unassigned (не назначен) относятся к IP-адресам, связанным с определенным компьютером, но не связанным с конкретными сайтами. Web-сайт по умолчанию пользуется всеми IP-адресами, не присвоенными другим сайтам. Пользоваться неназначенными IP-адресами может только один сайт.

Основы администрирования сайтов

После создания Web-сайта вам придется администрировать IIS. Для этого используется оснастка IIS. Она размещается в консоли управления Microsoft (Microsoft Management Console, MMC). Это мощный инструмент администрирования сайта, предусматривающий возможность обращения ко всем настройкам вашего сервера. Оснастка IIS очень полезна при управлении сложным сайтом, размещенным в корпоративной внутренней сети, а также при публикации данных в сети Интернет.

Примечание

Оснастка IIS — это инструмент управления IIS 5.0, интегрированный с прочими административными функциями Windows 2000. В предшествующих версиях IIS этот инструмент назывался ISM (Internet Service Manager — диспетчер служб Интернета).

Управление сайтом

Принципы публикации содержимого универсальны и не зависят от того, где размещен ваш сайт: во внутренней сети или в Интернете. Вы помещаете файлы, составляющие сайт, в каталоги на сервере, а пользователи получают возможность установить HTTP-соединение и просмотреть эти файлы в Web-браузере. Впрочем, размещением файлов на сервере ваши задачи не ограничиваются. Вы должны определить, как ваш сайт будет использоваться и, что еще более важно, как он будет развиваться. В сегодняшних условиях привлекательные Web-сайты редко представляют собой статическую подборку страниц. Самые успешные Web-администраторы занимаются сбором информации, которая в условиях Интернета постоянно меняется. В этой части главы вы получите представление о принципах управления инфраструктурой Web-сайта.

Запуск и остановка

По умолчанию сайты активируются автоматически, одновременно с перезапуском компьютера. Остановка сайта подразумевает остановку работы интернет-служб и их выгрузку из памяти компьютера. В случае приостановки сайта интернет-службы прекращают устанавливать новые соединения, но продолжают обслуживать существующие запросы. Запуск сайта приводит к перезагрузке или возобновлению работы интернет-служб. Чтобы произвести запуск, остановку или приостановку сайта, откройте интегрируемое приложение IIS, выберите нужный сайт и нажмите кнопку **Start**, **Stop** или **Pause** на панели инструментов.

Примечание

В случае неожиданной остановки сайта интегрируемое приложение IIS может некорректно отображать состояние сервера. Прежде чем выполнять перезагрузку, сначала нажмите кнопку **Stop**, а потом уже **Start**.

В IIS 5.0 любые интернет-службы можно остановить и перезапустить непосредственно из консоли IIS. Это делает лишней перезагрузку компьютера в случае некорректного функционирования или недоступности приложений. Чтобы перезапустить IIS, выделите пиктограмму компьютера в интегрируемом приложении IIS, нажмите кнопку **Action** (Действие), а затем выберите **Restart IIS** (Перезапуск IIS). Открыв выпадающее меню (рис. 23.4), выберите пункт **Restart Internet Services** (Перезапуск служб Интернета), **Stop Internet Services** (Остановка служб Интернета), **Start Internet Services** (Запуск служб Интернета) или **Reboot server** (Перезагрузка компьютера). Конкретный выбор зависит от того, что вы хотите сделать.

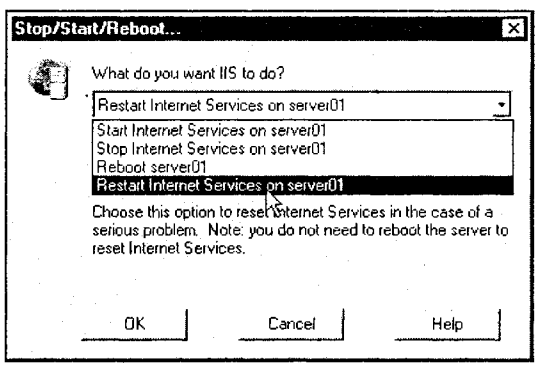


Рис. 23.4. Остановка, запуск и перезапуск Web-служб производится через IIS

Примечание

При перезапуске IIS в целях перезагрузки интернет-служб все процессы drwtsn32.exe, mtx.exe и dllhost.exe будут остановлены.

Каталоги

Следует настроить Web-сайты, указав каталоги, содержащие те документы, которые вы планируете опубликовать. Web-сервер не может публиковать документы, расположенные вне указанных каталогов. Таким образом, первым этапом процесса развертывания Web-сайта должно быть определение способа организации файлов. После этого с помощью интегрируемого приложения IIS указываются каталоги, которые должны стать компонентами сайта. Приступить к действиям вы можете сразу, даже не создавая специальную структуру каталогов. Если все файлы, предназначенные для публикации, расположены на одном жестком диске (или только на сервере с IIS), вы можете опубликовать документы немедленно. Для этого их нужно скопировать в принимаемый по умолчанию домашний каталог C:\InetPub\Wwwroot (при работе с FTP-сайтом файлы следует копировать в каталог C:\InetPub\Ftproot).

Для каждого Web- или FTP-сайта должен существовать один домашний каталог. Домашний каталог представляет собой централизованное хранилище всех опубликованных страниц. Он содержит домашнюю страницу или индексный файл с приветствием к пользователям и со ссылками на другие страницы сайта. Домашний каталог привязан к доменному имени сайта или к имени вашего сервера. К примеру, если доменным именем вашего сайта в Интернете является **www.dlspubs.com**, а домашним каталогом C:\Website\Dlspubs, в браузерах для доступа к этому домашнему каталогу используется URL-адрес **http://www.dlspubs.com**. Во внутренней сети для обращения к файлам в домашнем каталоге на сервере с именем acct_server в браузерах применяется URL **http://acct_server**. Чтобы изменить домашний каталог, откройте интегрируемое приложение IIS, выберите нужный Web- или FTP-сайт и откройте страницу его свойств. Перейдите на вкладку **Home Directory** (Домашний каталог) (рис. 23.5) и укажите местоположение домашнего каталога. При этом можно выбрать:

- каталог, расположенный на жестком диске вашего компьютера;
- совместно используемый каталог, расположенный на другом компьютере;
- перенаправление на другой адрес URL (браузеры, запрашивающие URL данные сайта, будут переходить на другой URL), хотя установить перенаправление на каталог FTP нельзя.

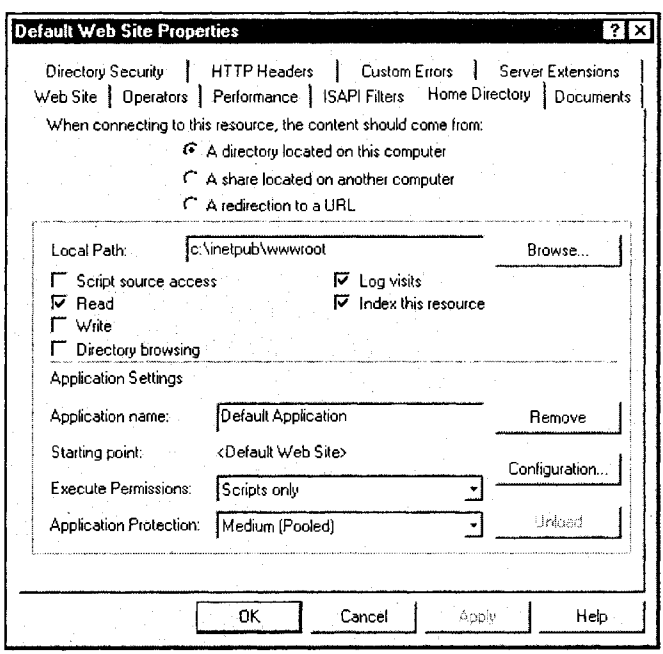


Рис. 23.5. На вкладке **Home Directory** указывается новый домашний каталог Web-сайта

В текстовом окне этой вкладки нужно ввести путь к файлу, имя совместно используемого ресурса или URL каталога. В случае выбора совместно используемого сетевого каталога вам, возможно, придется ввести имя пользователя и пароль, позво-

ляющие обращаться к данному ресурсу. Если вы пользуетесь учетной записью с административными правами на сервере, клиенты получат возможность доступа к операциям сервера. В результате система защиты вашей сети будет серьезно скомпрометирована.

Виртуальные каталоги

Чтобы опубликовать содержимое любого каталога, находящегося вне домашнего каталога, вам придется создать *виртуальный каталог*. Виртуальный каталог содержится вне домашнего каталога, но браузеры клиентов рассматривают его так, как будто именно там он и расположен. Виртуальный каталог имеет псевдоним (имя, применяемое Web-браузерами для получения доступа к нему). Так как псевдоним обычно оказывается короче полного пути к каталогу, пользователям удобнее вводить именно его. Кроме того, псевдоним лучше защищен. Пользователи не знают, где именно на сервере расположены файлы, к которым они обращаются, и, следовательно, не могут воспользоваться этими данными для их изменения. Псевдонимы упрощают задачу перемещения каталогов сайта. Вместо того чтобы менять URL-адрес каталога, вы можете изменить соответствие псевдонима и физического расположения каталога.

Примечание

Создавать виртуальные каталоги для простого Web-сайта обычно не имеет смысла Ничто не мешает вам поместить все файлы сайта в его домашний каталог. Если же вы работаете со сложным сайтом или хотите создать разные адреса URL для разных его частей, разумно создавать виртуальные каталоги по мере необходимости.

Чтобы создать виртуальный каталог, откройте интегрируемое приложение IIS и выберите Web- или FTP-сайт, в рамках которого предполагается создать каталог. Нажмите кнопку **Action** (Действие), выделите **New** (Создать) и выберите **Virtual Directory** (Виртуальный каталог). Для завершения этой задачи воспользуйтесь мастером New Virtual Directory Wizard (Мастер нового виртуального каталога). Чтобы удалить виртуальный каталог, укажите его в интегрируемом приложении IIS. Нажмите кнопку **Action** (Действие) и выберите **Delete** (Удалить). Удаление виртуального каталога не приводит к удалению соответствующего физического каталога и содержащихся в нем файлов.

Примечание

Если вы пользуетесь файловой системой NTFS, то для создания виртуального каталога можно щелкнуть на каталоге, отображаемом в Windows Explorer, правой кнопкой мыши, выбрать **Sharing** (Доступ), а затем указать страницу свойств **Web Sharing** (Доступ через веб).

Название сайта и имена заголовков

Каждый Web-сайт (он же — виртуальный сервер) имеет описательное имя и может поддерживать одно или несколько имен заголовков хостов. Имена заголовков хостов обеспечивают возможность размещать на одном компьютере несколько доменных имен. Применение имен заголовков хостов поддерживают не все браузеры. Internet Explorer 3.0, Netscape Navigator 2.0 и последующие версии этих браузеров поддерживают имена заголовков хостов, но более ранние их версии не предусматривают их

применения. К примеру, если посетитель попытается обратиться к вашему сайту с помощью устаревшего браузера, который не поддерживает заголовки хостов, он будет перенаправлен на Web-сайт по умолчанию, которому присвоен данный IP-адрес (это произойдет лишь в том случае, если сайт по умолчанию активирован). Но совершенно не обязательно, что это именно тот сайт, который хотел увидеть посетитель. Кроме того, если запрос, каким бы браузером он ни отсылался, относится к остановленному в данный момент сайту, посетитель взамен перенаправляется на Web-сайт по умолчанию. По этой причине вы должны тщательно продумать содержание Web-сайта по умолчанию. Как правило, поставщики услуг Интернета выставляют в качестве сайта по умолчанию свою собственную домашнюю страницу, а не домашнюю страницу Web-сайтов своих клиентов. В результате исключается перенаправление запроса с остановленного сайта на сторонний сайт. Кроме того, сайт по умолчанию может содержать сценарий, обеспечивающий поддержку применения имен заголовков хостов старыми версиями браузеров.

Чтобы присвоить Web-сайту имя, откройте интегрируемое приложение IIS, выберите нужный сайт и откройте страницу его свойств. На вкладке **Web Site** (Веб-узел) введите описательное имя сайта в поле **Description** (Описание). Чтобы назначить имя заголовка хоста, в первую очередь необходимо ввести в систему разрешения имен (в качестве которой обычно выступает DNS) соответствие нового имени сайта и статического IP-адреса. В интегрируемом приложении IIS выберите нужный Web-сайт и откройте страницу его свойств. На вкладке **Web Site** (Веб-узел) нажмите кнопку **Advanced** (Дополнительно). В диалоговом окне свойств **Advanced Multiple Web Site Configuration** (Дополнительная настройка веб-узлов) (рис. 23.6) нажмите кнопку **Add** (Добавить). Так вы сможете указать имя заголовка хоста, IP-адрес и порт Web-сайта.

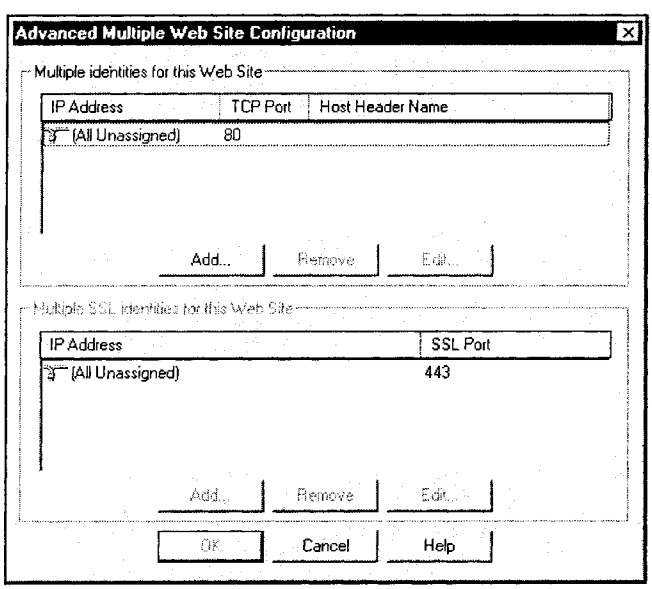


Рис. 23.6. Для Web-сайта можно указывать имена и другие конфигурационные данные

Перенаправления

Когда браузер запрашивает страницу, расположенную на вашем Web-сайте, Web-сервер находит ее по URL-адресу, а затем возвращает ее браузеру. При перемещении страницы Web-сайта исправить все ссылки, указывающие на ее старый URL-адрес, удается не всегда. Чтобы гарантировать нахождение браузером страницы по ее новому URL-адресу, следует настроить Web-сервер таким образом, чтобы он предоставлял браузеру новый URL. Именно им браузер будет пользоваться при повторном запросе страницы. Этот процесс называется перенаправлением запроса браузера (или перенаправлением на другой URL-адрес). Перенаправление запроса на страницу аналогично адресу пересылки, применяемому почтовыми службами. Перенаправление URL оказывается полезным при обновлении Web-сайта, когда определенную его часть приходится делать временно недоступной, а также после изменения имени виртуального каталога, когда ссылки в первоначальном каталоге должны указывать на файлы в новом виртуальном каталоге.

Чтобы перенаправить запросы на другой каталог или Web-сайт, откройте интегрируемое приложение IIS, выберите нужный Web-сайт или каталог и зайдите на страницу его свойств. Перейдите на вкладку **Home Directory** (Домашний каталог), **Virtual Directory** (Виртуальный каталог) или **Directory** (Каталог) и установите переключатель в положение **A redirection to a URL** (Постоянный адрес URL) (рис. 23.7). В поле **Redirect to** (Адрес) введите URL каталога или Web-сайта назначения. К примеру, чтобы перенаправить все запросы на файлы, расположенные в каталоге /Catalog, на каталог /NewCatalog, введите /NewCatalog.

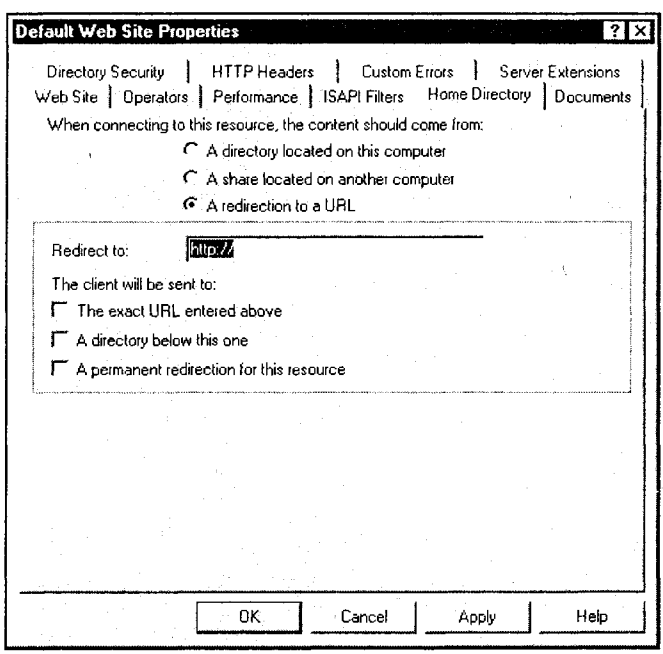


Рис. 23.7. Задание перенаправления с Web-сайта производится на вкладке **Home Directory**

Чтобы перенаправить все запросы на отдельный файл, откройте интегрируемое приложение IIS, выберите нужный Web-сайт или каталог и зайдите на страницу его свойств. Перейдите на вкладку **Home Directory** (Домашний каталог), **Virtual Directory** (Виртуальный каталог) или **Directory** (Каталог) и установите переключатель в положение **A redirection to a URL** (Постоянный адрес URL). В поле **Redirect to** (Адрес) введите URL файла назначения. Чтобы избежать присоединения Web-сервером имени исходного файла к URL-адресу назначения, пометьте флажок **Exact URL Entered Above** (На введенный выше адрес URL). Для получения точного контроля над преобразованием исходного URL в URL назначения можно пользоваться групповыми символами и переменными перенаправления.

Наконец, вы можете перенаправить все запросы на файлы, расположенные в указанном каталоге, на определенную программу. Как правило, при этом имеет смысл передавать программе все параметры, присоединенные к исходному URL-адресу. Это делается с помощью переменных перенаправления. Чтобы перенаправить запросы на программу, откройте интегрируемое приложение IIS, выберите нужный Web-сайт или каталог, а затем откройте страницу с его свойствами. Перейдите на вкладку **Home Directory** (Домашний каталог), **Virtual Directory** (Виртуальный каталог) или **Directory** (Каталог) и установите переключатель в положение **A redirection to a URL** (Постоянный адрес URL). В поле **Redirect to** (Адрес) введите URL нужной программы (с указанием всех переменных перенаправления, необходимых для передачи программе параметров). К примеру, чтобы перенаправить все запросы на сценарии, размещенные в каталоге Scripts, программе регистрации, которая будет фиксировать запрошенный URL-адрес и все переданные с ним параметры, введите

```
/Scripts/Logger.exe?URL=$V+PARAMS=$P
```

где `$V` и `$P` являются переменными перенаправления. Кроме того, чтобы избежать присоединения Web-сервером имени исходного файла к URL-адресу назначения, установите флажок **Exact URL Entered Above** (На введенный выше адрес URL).

Истечение срока действия содержимого сайта

Если на сайте присутствует информация, актуальность которой ограничена по времени, вы можете активировать настройки, предотвращающие публикацию устаревших данных. С помощью страницы свойств **HTTP Headers** (Заголовки HTTP) содержимое сайта настраивается на автоматическое истечение в любой момент времени. При активизации настроек, связанных с истечением срока действия информации, Web-браузер сравнивает текущую дату со сроком действия и на основании полученного результата определяет, стоит ли выводить кэшированную страницу или же необходимо запросить с сервера ее обновленный вариант. Чтобы определить срок годности данных, опубликованных на Web-сайте, откройте интегрируемое приложение IIS, выберите нужный Web-сайт, виртуальный каталог, каталог или файл (по отношению к которому предполагается установить срок годности). Щелкните на записи Web-сайта (виртуального каталога, каталога или файла) правой кнопкой мыши и выберите пункт **Properties** (Свойства). Выберите вкладку **HTTP Headers** (Заголовки HTTP) (рис. 23.8) и установите флажок **Enable Content Expiration** (Включить срок действия содержимого). Установите переключатель в положение **Expire Immediately** (Истекает немедленно), **Expire after** (Истекает через...) или **Expire on** (Истекает на...) и введите в соответствующем поле подходящие данные о сроках действия.

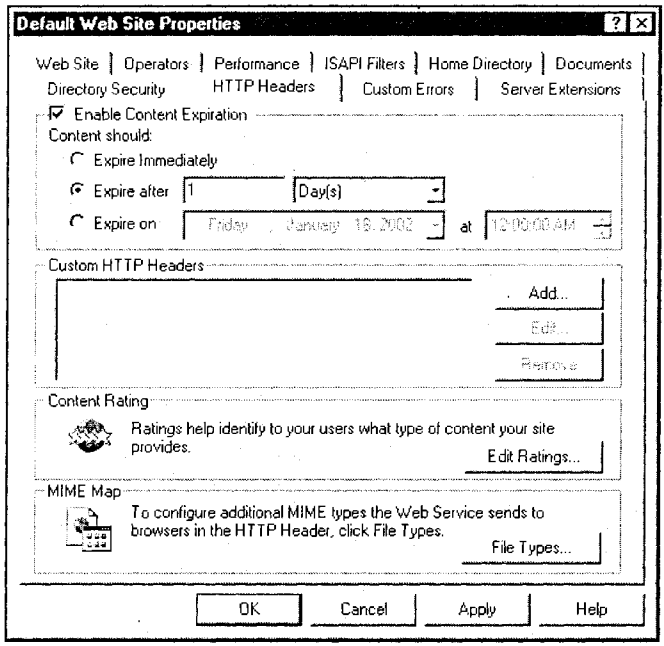


Рис. 23.8. Для удаления с Web-сайта устаревшего материала существуют настройки истечения срока действия содержимого

Рейтинги содержимого

Для встраивания описательных меток в HTTP-заголовки Web-страниц в Web-сервере IIS 5.0 существуют функции присвоения рейтингов содержимого. Некоторые Web-браузеры (например, Internet Explorer 3.0 и последующих версий) способны считывать такие информационные метки и помогать пользователям при определении нежелательного содержимого. По умолчанию в вашем Web-сервере применяется рейтинговая система на основе платформы для отбора информации в Интернете (Platform for Internet Content Selection, PICS). В ней применяется методика, разработанная консультативным советом по развлекательному программному обеспечению (Recreational Software Advisory Council, RSAC), предполагающая ранжирование информации по уровням насилия, порнографии и оскорбительных выражений. Прежде чем настраивать рейтинги Web-информации, вы должны заполнить анкету RSAC. Это позволит получить рекомендуемые рейтинги содержимого, подходящие именно к вашей информации. Чтобы настроить рейтинги содержимого, выполните следующие действия.

1. Откройте оснастку IIS, выберите нужный Web-сайт, каталог или файл и зайдите на страницу его свойств.
2. Перейдите на вкладку **HTTP Headers** (Заголовки HTTP) и выберите **Content Rating** (Оценка содержимого), **Edit Ratings** (Изменить).
3. На странице свойств **Ratings** (Оценки) установите флажок **Enable Ratings for this resource** (Включить оценки для данного ресурса) (рис. 23.9).

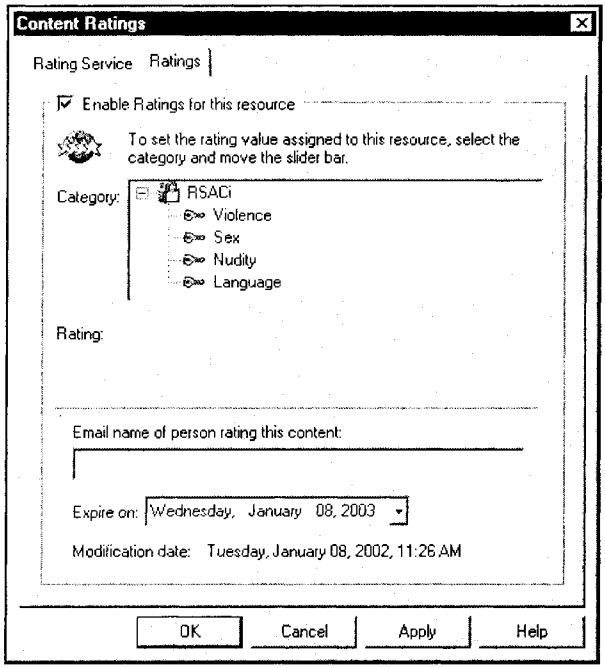


Рис. 23.9. Для выявления сайтов с нежелательной информацией применяются рейтинги содержимого

4. В области **Category** (Категория) выберите категорию рейтингов. Чтобы установить уровень нежелательного материала для данной категории, воспользуйтесь рейтинговым ползунком. Для каждой настройки выводится описание уровня рейтинга.
5. В области **Email name of person rating this content** (Введите адрес электронной почты лица, оценивающего содержимое) введите адрес, затем откройте выпадающий список **Expire on** (Срок действия) и с помощью календаря выберите срок годности рейтингов.
6. Нажмите кнопку **OK**.

Защита конфигурации IIS

Текущую конфигурацию IIS можно резервировать. Впоследствии, в случае ошибки при настройке или конфигурации, вы сможете без труда возвратиться к предшествующему состоянию. Ниже представлены процедуры создания резервной копии конфигурации IIS и ее восстановления (осуществление последней операции зависит от того, был ли Web-сервер деинсталлирован или переустановлен). Чтобы создать резервную копию конфигурации IIS, сделайте следующее.

1. Откройте оснастку IIS и выберите пиктограмму **Computer**.
2. Нажмите кнопку **Action** (Действие) и выберите **Backup/Restore Configuration** (Архивирование и восстановление конфигурации).

3. Нажмите кнопку **Create Backup** (Создать архив), выберите имя файла с резервной копией и нажмите **OK** (по умолчанию файл резервной копии сохраняется в каталоге \Winnt\system32\inetsrv\MetaBack).
4. Нажмите кнопку **Close** (Закрыть).

Примечание

Этот метод резервирования предусматривает возможность восстановления настроек IIS, но не файлов с данными. Вам в любом случае придется поддерживать полную резервную копию всей информации, предназначенной для Web-публикации.

Чтобы выполнить восстановление настроек IIS, сделайте следующее.

1. Откройте оснастку IIS и выберите пиктограмму **Computer**.
2. Нажмите кнопку **Action** (Действие) и выберите **Backup/Restore Configuration** (Архивирование и восстановление конфигурации).
3. Укажите местоположение файла с резервной копией и нажмите кнопку **Restore** (Восстановить). При необходимости подтвердить восстановление настроек конфигурации нажмите кнопку **Yes**.

Примечание

На любом Web-сервере важно обеспечение безопасности. Обязательно ознакомьтесь со всеми рисками, связанными с защитой, а также с функциями безопасности, предусмотренными вашей программой Web-сервера.

Назначение операторов

Если вы не планируете управлять Web-сервером только собственными силами, вам придется назначить одного или нескольких операторов. Операторы Web-сайтов — это пользовательские (или групповые) учетные записи Windows с ограниченными административными правами в рамках Web-сайтов, владельцам которых вы можете поручать выполнение повседневных задач, связанных с сопровождением сайта (например, публикацию новых данных), при этом сохраняя полные административные полномочия за собой. Для назначения оператора Web-сайта необходимо выполнить следующие действия.

1. Откройте оснастку IIS, выберите нужный Web-сайт и зайдите на страницу его свойств.
2. Перейдите на вкладку **Operators** (Операторы) и нажмите кнопку **Add** (Добавить). В результате откроется окно **Add Users and Groups** (Добавление пользователей и групп).
3. Либо укажите пользователя или группу из списка **Names** (Имя), либо выберите другой список имен в области **List Names From** (Список имен из...).
4. Укажите участника группы пользователей, нажав кнопку **Members** (Участники), или с помощью кнопки **Search** (Поиск) выполните поиск пользователя или группы в сети.

Если впоследствии вам придется удалять оператора, перейдите на вкладку **Operators** (Операторы), выделите нужного пользователя или группу и нажмите кнопку **Remove** (Удалить).

Управление приложениями IIS

С помощью Web-сервера (типа IIS) приложения можно выполнять непосредственно на Web-сайте. Приложение IIS — это любой файл, выполнение которого происходит в рамках предопределенного множества каталогов Web-сайта. При создании приложения на Web-сайте для него выделяется начальный каталог (он также называется корневым каталогом приложения). Это делается с помощью оснастки IIS. Каждый файл и каталог, находящийся внутри начального каталога Web-сайта, считается компонентом данного приложения (вплоть до обнаружения другого начального каталога). IIS поддерживает приложения ASP, ISAPI (Internet Server API — интерфейс прикладного программирования интернет-сервера), CGI, IDC ((Internet Database Connector — коннектор баз данных Интернета) и SSI (Server Side Includes — вставки на стороне сервера). Мощность приложений обуславливается тем, что между составляющими их файлами возможна организация совместного использования данных. К примеру, для страниц приложения ASP совместными являются контекстный поток, состояние сеанса и настройки переменных.

Термин *защита приложений* обозначает способ запуска приложений; IIS 5.0 предусматривает три уровня защиты приложений. В IIS 4.0 приложения можно было настроить таким образом, чтобы они выполнялись в том же процессе, что и Web-служба (inetinfo.exe), или в изолированном процессе, независимо от Web-служб (dllhost.exe). В дополнение к этому в IIS 5.0 приложения могут работать все вместе в объединенном процессе (т. е. в отдельном экземпляре dllhost.exe). Эти варианты предусматривают различные уровни защиты от ситуации, когда некорректно работающее приложение выходит из строя, и процесс, в рамках которого оно выполняется, перестает отвечать. По умолчанию Web-службы выполняются в отдельном процессе, а все прочие приложения в едином, объединенном процессе. Впоследствии вы можете определять для отдельных приложений высокий приоритет и настраивать их на работу в рамках обособленных процессов. По причинам, связанным с производительностью, исполнять более десяти изолированных приложений неразумно.

Наконец, существует компромисс между производительностью и уровнем защиты приложений. Приложения, исполняемые в рамках процесса Web-служб, работают с большей степенью эффективности, но при этом сохраняется значительный риск, связанный с тем, что некорректно работающее приложение сделает Web-службы недоступными. Рекомендуется запускать inetinfo.exe (Web-службы) в одном процессе, ответственные приложения в другом, а все прочие приложения запускать в совместном, объединенном процессе.

Создание приложений

Чтобы создать приложение, в первую очередь для него нужно выделить начальный (корневой) каталог. После этого можно приступать к заданию свойств приложения. У каждого приложения может быть имя, удобное для пользователя. Под этим именем оно обозначается в оснастке IIS и служит для различения приложений (нигде более такое имя не используется). Чтобы создать приложение, сделайте следующее.

1. Открыв оснастку IIS, выберите начальный каталог нового приложения, например домашний каталог Web-сайта.
2. Откройте страницу свойств каталога и перейдите на вкладку **Home Directory** (Домашний каталог), **Virtual Directory** (Виртуальный каталог) или **Directory** (Каталог).

3. Нажмите кнопку **Create** (Создать) (рис. 23.10). Если на месте кнопки **Create** расположена кнопка **Remove** (Удалить), значит, приложение уже создано.
4. В текстовом поле **Application name** (Имя приложения) введите имя приложения.

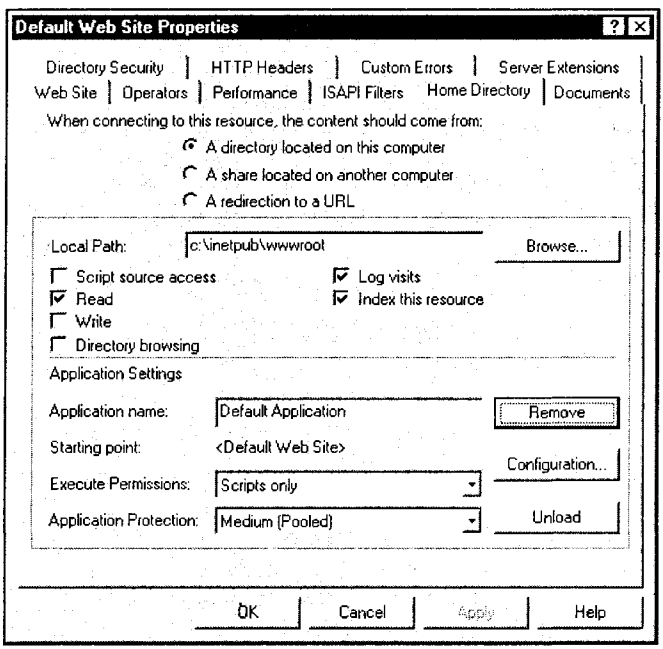


Рис. 23.10. Вы можете создать приложения в рамках Web-сайта и удалять их

Вы также должны установить для нового приложения полномочия.

- Чтобы предотвратить запуск любых программ или сценариев, установите полномочия **None**.
- Чтобы приложения, связанные с обработчиком сценариев, могли запускаться в данном каталоге без полномочий **Execute** (Исполняемые файлы), установите полномочия **Scripts only** (Только сценарии). Полномочия **Script** (Сценарии) следует устанавливать для каталогов, содержащих сценарии ASP, IDC, а также другие сценарии. Полномочия **Script** безопаснее **Execute**, т. к. у вас есть возможность ограничить приложения, запускаемые в данном каталоге.
- Чтобы разрешить в данном каталоге запуск любых приложений, включая связанные с обработчиком сценариев и с бинарными файлами Windows (например, с файлами DLL и EXE), установите полномочия **Scripts and Executables** (Сценарии и исполняемые файлы).

Кроме того, вы можете удалить каталог из приложения. В результате запросы на файлы в данном каталоге и его подкаталогах не будут приводить к запуску приложения. Удаление каталога из приложения не предполагает удаления каталога с Web-сайта и с жесткого диска вашего сервера. Чтобы удалить каталог из приложения, повторите процесс, рассмотренный выше, но нажмите кнопку **Remove** (Удалить)

(вместо **Create**). Чтобы остановить приложение и выгрузить его из памяти, нажмите кнопку **Unload** (Выгрузить). Если кнопка **Unload** затенена, значит, вы находитесь вне начального каталога приложения.

Примечание

Чтобы запустить приложение в отдельном от Web-сервера процессе, установите флажок **Run in Separate Memory Space (Isolated Process)**. В результате все другие приложения (включая Web-сервер) будут защищены от аварийных отказов в случае некорректного функционирования данного приложения.

Сопоставление приложений

IIS позволяет разрабатывать Web-приложения на различных языках программирования и составления сценариев. Чтобы определить, какую программу ISAPI или CGI нужно запустить для обработки запроса, IIS проверяет расширение файла, в котором находится запрошенный ресурс Web-сайта. К примеру, получение запроса на файл с расширением asp заставляет Web-сервер вызвать программу ASP (asp.dll). Именно с ее помощью происходит обработка таких запросов. Такое ассоциирование расширения файла с программой ISAPI или CGI называется *сопоставлением* приложений. IIS предварительно настроен на поддержку наиболее распространенных сопоставлений. Впрочем, вы можете добавлять или удалять их для всех приложений Web-сайта или только для некоторых из них. Чтобы связать расширения и приложения, выполните следующие действия.

1. Откройте оснастку IIS и выберите Web-сайт или начальный каталог приложения.
2. Откройте страницу свойств каталога и перейдите на вкладку **Home Directory** (Домашний каталог), **Virtual Directory** (Виртуальный каталог) или **Directory** (Каталог).
3. Нажмите кнопку **Configuration** (Настройка) и перейдите на вкладку **App Mappings** (Отображение приложений) (рис. 23.11).
4. Нажмите кнопку **Add** (Добавить), а затем в поле **Executable** (Исполняемый файл) введите путь к программе ISAPI или CGI, которая будет обрабатывать указанный файл. Необходимо указать программу, расположенную в локальном каталоге Web-сервера.
5. В поле **Extension** (Расширение) введите расширение файла, которое предполагается ассоциировать с указанной программой ISAPI или CGI. Теперь, если Web-сервер получит URL файла с таким расширением, для обработки запроса он вызовет связанную с ним программу.
6. Чтобы разрешить обработку файлов указанного типа в каталоге с полномочиями Script, установите флажок **Script Engine** (Обработчик сценариев). Когда для каталога установлены полномочия **Script** (вместо **Execute**), в нем могут обрабатываться только те файлы, которые связаны с назначенными обработчиками сценариев.

Чтобы удалить сопоставление приложений, откройте страницу свойств **App Mappings**, выберите расширение файла и нажмите кнопку **Remove** (Удалить). После этого запросы на файлы с таким расширением, расположенные в указанном каталоге или на данном Web-сайте, обрабатываться не будут.

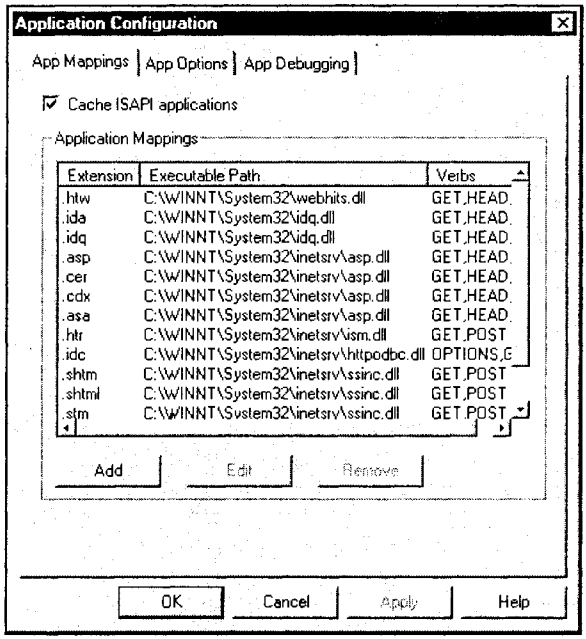


Рис. 23.11. Вы можете настроить сопоставление приложений по отношению к каждому Web-сайту

Настройка приложений ASP

Свойства могут быть заданы для каждого приложения ASP, установленного на Web-сервере. К примеру, вы можете задействовать в приложении состояние сеанса или определить язык сценариев по умолчанию. Не забывайте, что свойства приложения распространяются на все страницы ASP, расположенные в рамках этого приложения, если только вы не замените их непосредственно в свойствах отдельной страницы. Чтобы настроить приложение ASP, сделайте следующее.

1. Откройте оснастку IIS и укажите нужный Web-сайт или начальный каталог приложения.
2. Откройте страницу свойств каталога и перейдите на вкладку **Home Directory** (Домашний каталог), **Virtual Directory** (Виртуальный каталог) или **Directory** (Каталог).
3. Нажмите кнопку **Configuration** (Настройка), а затем перейдите на вкладку **App Options** (Параметры приложений).
4. Задайте свойства приложения.

Для поиска ошибок в сценариях ASP вы можете воспользоваться программой Microsoft Script Debugger. Перед тем как задействовать отладчик на Web-сервере, вы должны настроить этот сервер на выполнение отладки описанным далее образом.

Примечание

Чтобы получить дополнительную информацию о применении этой программы отладки для анализа ваших сценариев, зайдите на домашнюю страницу сайта

Microsoft Scripting Technology, расположенную по адресу: **msdn.microsoft.com/isapi/redir.dll?prd=scripting&ar=home&pver=4.0**.

1. Откройте оснастку IIS и выберите нужный Web-сайт или начальный каталог приложения.
2. Отройте список свойств этого каталога, а затем перейдите на вкладку **Home Directory** (Домашний каталог), **Virtual Directory** (Виртуальный каталог) или **Directory** (Каталог).
3. Нажмите кнопку **Configuration** (Настройка) и перейдите на вкладку **App Debugging** (Отладка приложений).
4. Чтобы включить отладку, выберите **Enable ASP Server-Side Script Debugging** (Включить серверную отладку сценариев). Впоследствии программа отладки будет запускаться в случае генерации ошибки в рамках сценария, а также в случае, если ASP столкнется с контрольной точкой в сценарии.

Настройка приложений CGI

IIS поддерживает приложения CGI. Программы CGI выполняются тогда, когда Web-сервер получает адрес URL, содержащий имя программы CGI и любые параметры, необходимые для ее работы. Если программа CGI скомпилирована в исполняемый файл (EXE), вы должны предоставить каталогу, в котором она содержится, полномочия **Execute** (Исполняемые файлы), иначе ее нельзя будет выполнить. Если программа CGI существует в виде сценария (к примеру, на языке Perl), то каталогу, в котором она содержится, можно присвоить полномочия **Execute** (Исполняемые файлы) или **Script** (Сценарии). В случае назначения полномочий **Script** интерпретатор сценариев необходимо обозначить как обработчик сценариев. Чтобы установить и настроить приложения CGI, сделайте следующее.

Примечание

Общую информацию о программировании приложений CGI можно получить на сайте MSDN Online Library: **msdn.microsoft.com/isapi/redir.dll?prd=msdn&ar=library&pver=6.0**.

- Определите каталог для программ CGI. Для обеспечения дополнительной защиты программы CGI следует отделить от информационных файлов. Присваивать такому каталогу имя Cgi-bin необязательно, но если хотите, вы можете назвать его именно так.
- Если ваши программы CGI существуют в виде сценариев, установите подходящий интерпретатор сценариев. К примеру, для выполнения сценариев Perl необходимо установить интерпретатор Perl. В операционных системах Windows версии Perl, SED и AWK не предусмотрены, но интерпретаторы можно получить от сторонних разработчиков.
- Если ваши программы CGI существуют в виде файлов EXE, назначьте для каталога полномочия **Execute** (Исполняемые файлы). Если же программы CGI написаны в виде сценариев, то каталогу, в котором они расположены, можно присвоить полномочия **Execute** или **Script** (Сценарии).
- В случае назначения полномочий **Script** вы должны обозначить интерпретатор сценариев как обработчик сценариев. Такая маркировка выполняется в свойствах

каталога. В каталоге с такими полномочиями выполнение файлов может производиться только интерпретаторами, помеченными как обработчики сценариев. Прямой запуск исполняемых файлов (DLL и EXE) не допускается, т. к. запрос браузера с указанием имени нужной программы в адресе URL не может инициировать запуск исполняемого файла на Web-сервере. Полномочия **Script** в сочетании с опцией **Script Engine** позволяют вам, ничем не рискуя, помещать информационные файлы (например, документы htm или изображения gif) в один каталог со сценариями CGI. В браузере будут выводиться информационные файлы и выполняться сценарии, но при этом никто не имеет права запустить несанкционированную программу. Кроме того, в браузере не будут отображаться команды сценариев.

Примечание

Если вы назначите каталогам, содержащим исполняемые файлы, полномочия **Read** (Чтение), то посетители вашего сайта получат возможность загружать и запускать эти файлы. По соображениям безопасности исполняемые файлы следует помещать в отдельный каталог, полномочий **Read** для которого не установлено.

- В отношении сценариев CGI вам следует создать сопоставление между расширением файлов, в которых они содержатся, и интерпретатором сценариев.
- IIS устанавливает соответствие между расширениями файлов и интерпретатором. К примеру, если вы пользуетесь сценариями Perl и храните их в файлах с расширением pl, необходимо ассоциировать расширение pl с программой, которая будет выполнять эти сценарии. Свяжите файлы BAT и CMD с интерпретатором команд (Cmd.exe).
- Если вы пользуетесь правами доступа NTFS, убедитесь в том, что полномочиями **Execute** (Исполняемые файлы) по отношению к каталогу, в котором содержится нужная программа, располагают все пользователи, которые должны будут ее запускать. Если посещение вашего Web-сайта анонимными пользователями допускается, убедитесь в том, что полномочия **Execute** есть и у них (за анонимных пользователей отвечает учетная запись `IUSR_имякомпьютера`).
- Если ваш сценарий обращается к другому сценарию, ассоциированному с cmd.exe и исполняемому на удаленном сервере, то по умолчанию на локальном компьютере задается рабочий каталог %SYSTEM32%. Значением по умолчанию для %SYSTEM32% является \Winnt\System32 (в системе Windows 2000) или \Win95\System (в Windows 95 и последующих версиях этой системы).

Примечание

Если вы хотите добиться увеличения скорости выполнения, то имеет смысл разработать расширение ISAPI. Чтобы упростить разработку, попробуйте создать приложение ASP. Технология ASP особенно привлекательна для неопытных программистов и составителей сценариев, поскольку она обеспечивает выполнение многих рутинных операций, традиционно ассоциировавшихся с написанием приложений CGI, например, она проводит анализ заголовков HTTP.

Применение фильтров ISAPI

Подобно расширениям ISAPI, фильтры ISAPI представляют собой программы, реагирующие на получение сервером HTTP-запроса. Их отличие от приложений за-

ключается в том, что они управляются событиями на Web-сервере, а не запросами клиента. Вы можете ассоциировать фильтр ISAPI с определенным событием Web-сервера. Впоследствии фильтр будет получать извещение о каждом таком событии. Например, оповещение фильтра может происходить при событии Read или Write; после этого он выполняет шифрование необработанных данных, которые должны быть возвращены клиенту. Фильтры ISAPI можно установить для всех сайтов на сервере (в таком случае эти фильтры называются *глобальными*) или только для некоторых из них. Если установить глобальные фильтры в сочетании с фильтрами сайта, то для отдельного сайта эти два фильтра будут объединены.

Если для одного и того же события зарегистрировано несколько фильтров, они вызываются последовательно. Фильтры с более высоким приоритетом исполняются раньше, чем фильтры с более низким приоритетом. Если нескольким фильтрам присвоен одинаковый уровень приоритета, то глобальные фильтры, установленные в основных свойствах, запускаются до фильтров, заданных на уровне сайта. Фильтры, имеющие один уровень приоритета и находящиеся на одном уровне наследования, запускаются в порядке их загрузки. Изменения в порядке загрузки фильтров производятся с помощью свойств Web-сервера или Web-сайта. Чтобы добавить фильтр на Web-сервер или на Web-сайт, выполните следующие действия.

1. Откройте оснастку IIS, выберите нужный Web-сервер или Web-сайт и зайдите на страницу его свойств.
2. Перейдите на вкладку **ISAPI Filters** (Фильтры ISAPI) (рис. 23.12).
3. Нажмите кнопку **Add** (Добавить).

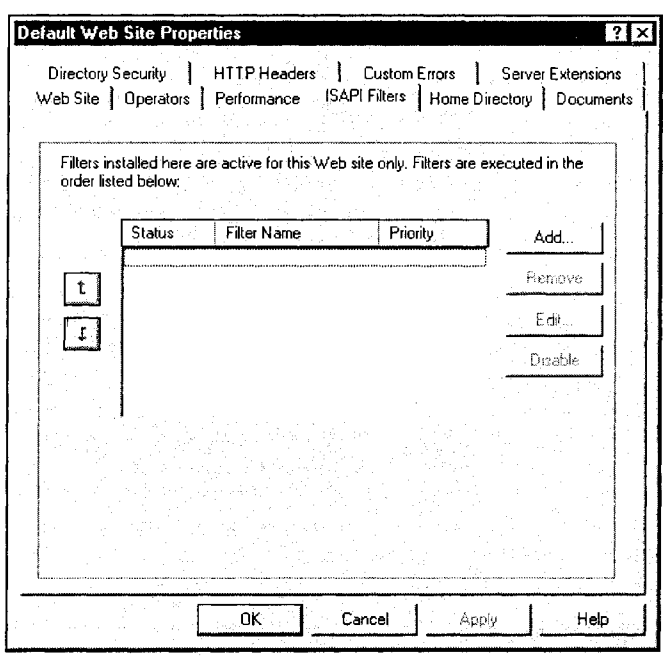


Рис. 23.12. Настройка фильтров ISAPI для Web-сайта

4. Введите имя фильтра в поле **Filter Name** (Имя фильтра), а затем укажите (введите или найдите) файл DLL в поле **Executable** (Исполняемый файл).
5. Нажмите кнопку **OK**.

Примечание

После добавления или изменения глобального фильтра необходимо остановить и перезагрузить Web-сервер. Только таким образом новые фильтры загружаются в память. Фильтр, добавляемый на уровне Web-сайта, загружается сразу и автоматически.

Основы обеспечения безопасности сайтов

Независимо от того, отвечаете ли вы за отдельные Web-серверы или за всю сеть, обеспечение безопасности — это вопрос, важность которого постоянно возрастает. Адекватные меры безопасности, предпринятые на вашем Web-сервере, могут ослабить или устранить значимые угрозы безопасности, исходящие как от злонамеренных лиц, так и от пользователей, исполненных благих намерений, но случайно получивших доступ к данным, предназначенным для служебного пользования или случайно изменивших важные файлы. IIS 5.0 поддерживает пять основных элементов системы защиты, о которых вы должны иметь представление: это аутентификация, контроль над доступом, шифрование, аудит и сертификаты. Из этой части главы вы сможете узнать, как нужно настраивать Web-сервер и операционную систему Windows, чтобы надежно обезопасить ваш Web-сайт и реализовать другие важнейшие функции обеспечения защиты.

Стандарты безопасности

IIS 5.0 содержит ряд функций обеспечения безопасности, причем многие из них выполнены в соответствии со стандартами, принятыми в интернет-сообществе. Эти стандарты способствуют соблюдению единообразия и обеспечивают возможность межплатформенного применения приложений и данных. В IIS существует шесть основных функций обеспечения безопасности.

- *Fortezza.* IIS 5.0 поддерживает стандарт обеспечения безопасности, применяемый правительством Соединенных Штатов, который часто фигурирует под именем Fortezza (**developer.netscape.com/tech/security/formsign/fortezza.html**). Этот стандарт соответствует архитектуре безопасности DMS (Defense Message System — система защиты передачи сообщений) с механизмом шифрования, который обеспечивает конфиденциальность, целостность, аутентификацию и подлинность сообщений, и контроль доступа к сообщениям, компонентам и системам. Указанные функции реализуются в серверном программном обеспечении, в браузерах, а также в аппаратной части плат стандарта PCMCIA. Механизм Fortezza широко используется в правительственных структурах США.
- *Протокол безопасности SSL 3.0* (Secure Sockets Layer — протокол защищенных сокетов). Протокол защищенных сокетов (**home.netscape.com/eng/ssl3/index.html**) — это протокол безопасности на основе открытого ключа, реализуемый через поставщика безопасности Secure Channel (Schannel). Протоколы безопасности SSL

широко применяются в интернет-браузерах и серверах для аутентификации, обеспечения целостности сообщений и конфиденциальности.

- *Базовая аутентификация (обычная проверка подлинности).* Базовая аутентификация (**www.w3.org/Protocols/HTTP/1.0/spec.html**) — это часть спецификации HTML 1.0, отвечающая за сетевую передачу паролей, зашифрованных в формате Base64. Эта спецификация поддерживается большинством браузеров.
- *Краткая аутентификация.* Краткая (Digest) аутентификация (**www.ics.udi.edu /pub/ietf/http/rfc2069.txt**) — это новая для IIS 5.0 функция, позволяющая передавать аутентификационную информацию через сеть в виде *хэша* (Hash — мешанина) и совместимая с прокси-серверами.
- *PKCS #7.* Стандарт криптографии с открытым ключом № 7 (Public Key Cryptography Standard #7, опубликован на сайте **www.rsasecurity.com**) описывает формат таких зашифрованных данных, как цифровые подписи или цифровые конверты, обеспечивающие защиту хранящейся в них информации. Оба эти элемента задействованы в функциях сертификации IIS.
- *PKCS #10.* Стандарт криптографии с открытым ключом № 10 (Public Key Cryptography Standard #10, опубликован на сайте **www.rsasecurity.com**) описывает формат запросов, отправляемых в сертификационные центры (Certificate Authority, CA), для получения сертификата.

Примечание

За дополнительной информацией об операционной системе Windows и проблемах, связанных с сетевой защитой, обращайтесь к сайту Microsoft, посвященному безопасности: **www.microsoft.com/security**.

Методы обеспечения защиты

Прежде чем настраивать систему защиты Web-сервера, установите, какой уровень безопасности достаточен для защиты ваших Web- и FTP-сайтов. К примеру, если вы хотите создать Web-сайт, позволяющий отдельным пользователям обращаться к закрытой информации (например, к финансовым или медицинским записям), то вам понадобится конфигурация, обеспечивающая устойчивую защиту. Эта конфигурация должна обеспечивать надежную аутентификацию отдельных пользователей и допускать к определенным данным только их. Значительная часть системы защиты Web-сервера зависит от настроек безопасности операционной системы Windows. В отсутствие должных настроек функций безопасности Windows защита Web-сервера не представляется возможной. Совершенно необходимо сделать следующее:

- настроить учетную запись администратора Windows;
- создать пользовательские учетные записи и управлять ими;
- создать группы и управлять ими;
- определить политики безопасности Windows.

Одним из компонентов безопасной конфигурации должно стать преобразование разделов вашего жесткого диска в раздел NTFS. Разделы NTFS обеспечивают точный контроль доступа к файлам и каталогам, а также более эффективное хранение данных, чем в таблицах размещения файлов (File Allocation Table, FAT). Для преоб-

разования раздела жесткого диска в NTFS вы можете воспользоваться утилитой Windows Convert. Затем нужно определить, к каким файлам и каталогам посетители ваших Web- и FTP-сайтов смогут обращаться без каких-либо ограничений. Общедоступная и закрытая информация должна размещаться в разных каталогах. Ниже перечислены вопросы безопасности, к которым вам, возможно, придется обратиться, а также рекомендации по повышению степени защиты.

- *Пользуйтесь NTFS.* Уровень защиты в системе NTFS превосходит аналогичные показатели системы FAT.
- *Проверьте полномочия NTFS на сетевых дисках.* По умолчанию, когда Windows создает новые совместно используемые ресурсы, полномочия полного управления ими (Full Control) присваиваются группе Everyone (Все).
- *Пересмотрите полномочия для каталогов.* По умолчанию, когда Windows создает новые каталоги, полномочия полного управления ими (Full Control) присваиваются группе Everyone (Все). Возможно, в вашей ситуации этот вариант окажется нежелательным.
- *Настройте управление доступом для учетной записи* `IUSR_имякомпьютера`. Это поможет ограничить доступ анонимных пользователей к вашему Web-серверу.
- *Храните исполняемые файлы в отдельном каталоге.* Это упростит назначение прав доступа и аудит.
- *Регулярно пересматривайте пользовательские учетные записи.* Проверяйте, нет ли новых учетных записей, созданных лицом, не являющимся действительным администратором. Пересматривайте права, присваиваемые учетной записи `IUSR_имякомпьютера`. Эта учетная запись применяется для анонимного доступа к вашему сайту. Чтобы организовать мониторинг времени и авторства изменений в политиках безопасности, вы можете воспользоваться методикой аудита.
- *Выбирайте сложные пароли.* Если пароли состоят из сочетания букв в нижнем и верхнем регистрах, цифр и специальных символов, угадать их становится сложнее.
- *Ведите строгие политики учетных записей.* Следите за тем, какие типы доступа предоставляются важным пользовательским и групповым учетным записям. В числе прочего нужно знать, кто имеет возможность вносить изменения в политики безопасности.
- *Ограничивайте членство в группе администраторов.* Эта группа, как правило, располагает полным доступом к компьютеру, и именно поэтому ограничение количества лиц с такими правами помогает повысить степень защиты.
- *Назначайте пароль для административной учетной записи.* По умолчанию административная учетная запись не предусматривает пароля. Чтобы повысить степень защиты, придумайте для этой учетной записи сложный пароль.
- *Запускайте минимальное количество служб.* Запускайте только те службы, которые в вашей ситуации абсолютно необходимы. Каждая дополнительная служба представляет собой точку проникновения для злонамеренных атак.
- *Не устанавливайте Web-сервер на основном контроллере домена.* Основной контроллер домена (Primary Domain Controller, PDC) постоянно обрабатывает запросы на аутентификацию. Запуск на нем Web-служб приведет к снижению произ-

водительности. Кроме того, это подвергает основной контроллер домена опасности атак, которые могут сделать уязвимой всю вашу сеть.

- *Задействуйте аудит.* Аудит — это очень ценный инструмент отслеживания доступа к защищенным или наиболее значимым файлам. Помимо этого, аудит может применяться для отслеживания серверных событий, таких как изменение политики безопасности. Аудиторские журналы можно архивировать для последующего ознакомления.
- *Пользуйтесь шифрованием при удаленном администрировании.* Удаленное администрирование обычно предполагает обмен уязвимыми данными (к примеру, пересылку пароля административной учетной записи). Чтобы защитить эту информацию в открытых сетях, пользуйтесь шифрованием под управлением протокола защищенных сокетов (SSL).
- *Пользуйтесь учетной записью низкого уровня в Интернете.* Применение учетных записей администратора, продвинутого пользователя и других привилегированных учетных записей при нахождении в Интернете может привести к открытию точек доступа для атак на ваш компьютер. Никогда не заходите в Интернет с основного контроллера домена.
- *Регулярно резервируйте важнейшие файлы и реестр.* Никакие действия по обеспечению безопасности не могут гарантировать сохранность данных, так что нужно всегда соблюдать постоянный режим резервирования и аварийного планирования по отношению к Web-серверу (как и по отношению ко всей сети).
- *Регулярно запускайте операции поиска вирусов.* Любой компьютер, находящийся в открытой сети, подвержен проникновению компьютерных вирусов. Избежать нежелательных потерь данных помогают регулярные проверки на наличие вирусов.
- *Изолируйте излишние службы от плат сетевых адаптеров.* Это упрощает задачу конфигурирования платформы и уменьшает возможные области атак. Впрочем, в этом случае возможно негативное воздействие на других пользователей вашей системы.
- *Пользуйтесь самой безопасной из всех возможных форм аутентификации.* Задействуйте наиболее защищенный вариант аутентификации из всех ее видов, поддерживаемых компьютером клиента. К примеру, интегрированная аутентификация Windows и краткая аутентификация защищены лучше, чем базовая аутентификация. Кроме того, для организации высокозащищенной аутентификации можно использовать клиентские сертификаты.
- *Назначайте наиболее ограничивающие из всех возможных полномочий.* К примеру, если ваш Web-сайт применяется только для просмотра информации, определите полномочия **Read** (Чтение). Если же в каталоге или на сайте размещаются приложения ASP, назначьте полномочия **Scripts Only** (Только сценарии), но не **Scripts and Executables** (Сценарии и исполняемые файлы).
- *Однозначные и многозначные связывания.* Для связывания клиентских сертификатов с учетными записями Windows вы можете пользоваться либо одним из указанных методов, либо обоими. Однозначное связывание предусматривает высокую степень достоверности, но требует хранения на сервере копии клиентского сертификата. Многозначное связывание проще в реализации и не требует хранения на сервере копии клиентского сертификата.

- *Синхронизируйте полномочия NTFS с полномочиями для Web.* Если Web-полномочия и полномочия NTFS не синхронизированы, применяется наиболее ограничивающие из двух. Синхронизацию можно проводить вручную или с помощью мастера IIS Permissions.
- *Будьте осторожны с полномочиями* ***Write*** (Запись) *и* ***Scripts and Executables*** (Сценарии и исполняемые файлы). Пользуйтесь этим сочетанием с большой осторожностью. Оно предусматривает возможность загрузки на сервер потенциально опасных исполняемых файлов и их запуска.
- *Блокируйте рабочий стол.* Отлучаясь от компьютера, блокируйте рабочий стол. Для этого нужно ввести сочетание клавиш <Ctrl>+<Alt>+<Delete> и выбрать **Lock Workstation** (Блокировка).
- *Пользуйтесь заставкой с паролем.* Временная задержка перед запуском заставки должна быть короткой для того, чтобы после вашего ухода никто не мог воспользоваться вашим компьютером. Заставка должна быть пустой (анимированные заставки способны снизить производительность сервера).
- *Физически блокируйте доступ к компьютеру.* Держите компьютер в запертом помещении. Так вы сможете снизить риск доступа к нему злонамеренных лиц.
- *Пользуйтесь разными администраторскими паролями.* Каждый человек, обладающий административными правами, должен пользоваться индивидуальным паролем и пользовательской учетной записью. Это поможет отслеживать все вносимые изменения.
- *Пользуйтесь договорами о неразглашении.* Степень ответственности администраторов можно увеличить за счет заключения договоров о неразглашении (т. е. о сохранении секретности имен пользователей и паролей).
- *Периодически перераспределяйте учетные записи.* Чтобы снизить риск компрометации данных пользовательской учетной записи, периодически назначайте сотрудникам, располагающим административными или другими высокоуровневыми правами, новые учетные записи.
- *Оперативно отключайте или удаляйте неиспользуемые учетные записи.* Это снизит вероятность того, что поставщик или бывший сотрудник сможет получить доступ к вашей сети.
- *Удаляйте образцы файлов, размещенные по умолчанию.* Это не позволит злоумышленникам знакомиться с содержанием обычных файлов по умолчанию. Возможно, вы не хотите, чтобы посетители их просматривали.
- *Устанавливайте IIS на отдельный логический диск.* В таком случае получение доступа к диску с IIS все же не позволяет злоумышленникам обращаться к операционной системе и другим важнейшим административным данным.

Аутентификация

Обеспечение безопасности начинается с *аутентификации* — удостоверения личности пользователя. IIS 5.0 предусматривает поддержку пяти методов аутентификации, с помощью которых вы можете проверить личность каждого, кто подает запрос о доступе к вашим Web-сайтам.

- *Анонимная аутентификация* позволяет каждому посетителю обращаться к вашему сайту, не предъявляя ни имя пользователя, ни пароль.

- *Базовая аутентификация* предлагает пользователю ввести имя и пароль, которые затем передаются по сети в незашифрованном виде.
- *Краткая аутентификация* — это новая функция, действующая во многом подобно базовой аутентификации, за исключением лишь того, что пароли передаются в виде хэш-кода. Хэш-код — это число, полученное из текстового сообщения, такого как пароль; вычислить из него исходный текст невозможно.. Краткая аутентификация работает только в доменах, управляемых контроллером домена Windows 2000.
- *Интегрированная аутентификация Windows* предполагает использование технологии хэширования для идентификации пользователя без фактической отсылки пароля через сеть.
- *Сертификаты* — это цифровые удостоверения, которые можно использовать для установления соединения по протоколу SSL. Кроме того, они подходят для выполнения аутентификации.

Эти методы позволяют обращаться к общедоступным областям вашего сайта, но предотвращают несанкционированный доступ к частным файлам и каталогам.

Управление доступом

Права доступа NTFS — это основа системы защиты вашего Web-сервера; они позволяют определять уровень доступа к файлам и каталогам со стороны пользователей Windows и их групп. К примеру, если какое-то предприятие решило опубликовать на вашем Web-сервере свой каталог, вам придется создать пользовательскую учетную запись Windows для этого предприятия, а затем настроить права доступа к его Web-сайту, каталогу или файлу. Эти полномочия позволят сделать так, чтобы обновление содержимого Web-сайта могло быть выполнено только администратором сервера и владельцем предприятия. Основной части пользователей будет разрешено лишь просматривать данный Web-сайт, но вносить изменения в опубликованную на нем информацию они не смогут.

WebDAV (поддержка которого обеспечивается IIS 5.0) — это расширение протокола HTTP 1.1, которое облегчает манипуляции с файлами и каталогами через соединение HTTP. Посредством команд WebDAV (Web Distributed Authority Versions — распределенные в Интернете авторские версии) свойства файлов и каталогов можно как просматривать, так и добавлять. Также предусматривается возможность удаленного создания, удаления или копирования файлов и каталогов. Дополнительный контроль доступа настраивается как через полномочия Web-сервера, так и посредством NTFS.

Сертификаты

Сертификаты — это документы цифровой идентификации, позволяющие клиентам и серверам проводить взаимную аутентификацию. Они требуются серверу и клиентскому браузеру для установления соединения SSL, через которое можно отсылать зашифрованную информацию. Среди функций SSL на базе сертификатов в IIS 5.0 присутствуют сертификат сервера, сертификат клиента, а также разнообразные цифровые ключи. Эти сертификаты можно создавать с помощью Microsoft Certificate Services или получать их от стороннего учреждения, пользующегося доверием обеих сторон и называемого *сертификационным центром* (CA).

Сертификаты серверов позволяют пользователям устанавливать подлинность Web-сайта. Сертификат сервера содержит подробную идентификационную информацию

(например, название организации, связанной с содержимым сервера), название учреждения, издавшего сертификат, а также открытый ключ, применяемый при установлении шифрованного соединения. Эти данные помогают убедить пользователей в достоверности содержимого Web-сервера, а также в безопасности защищенного соединения HTTP. Посредством SSL аутентификацию может проводить и ваш Web-сервер. Он проверяет содержимое сертификатов клиентов. Типичный сертификат клиента содержит подробную идентификационную информацию о пользователе и об учреждении, издавшем сертификат, а также открытый ключ. Для реализации хорошо защищенного метода удостоверения личности пользователей вы можете задействовать аутентификацию клиентских сертификатов в сочетании с шифрованием SSL.

Шифрование

Процесс обмена закрытыми данными (к примеру, номерами кредитных карточек или телефонными номерами) между пользователями и сервером можно обезопасить посредством *шифрования*. Шифрование засекречивает данные перед их отправкой, а расшифровка рассекречивает их после получения. Основой шифрования, применяемого в IIS, является протокол SSL 3.0, обеспечивающий надежные средства установления зашифрованного канала связи между сервером и пользователем. Протокол SSL подтверждает подлинность вашего Web-сайта, а, кроме того, имеет возможность факультативной идентификации пользователей, обращающихся к Web-сайтам, доступ на которые ограничен.

В сертификатах содержатся ключи, применяемые при установлении безопасного соединения SSL. Открытый и закрытый ключи образуют криптографическую пару. Такая пара применяется Web-сервером для согласования безопасного соединения с Web-браузером пользователя, которое позволяет определить уровень шифрования, необходимый для защиты обмена информации. Чтобы этот тип соединения можно было установить, Web-сервер и браузер пользователя должны быть оснащены совместимыми друг с другом возможностями шифрования и дешифрования. В ходе обмена данными создается ключ шифрования (сеансовый ключ). Этот секретный ключ сеанса отсылается клиентом серверу при помощи схемы открытого ключа (например, RSA).

Как серверу, так и Web-браузеру сеансовый ключ необходим для шифрования и расшифровки передаваемой информации. Степень шифрования (или стойкость) ключа измеряется в битах. Чем больше количество битов в сеансовом ключе, тем выше степень шифрования и защиты. Несмотря на то, что при высоком уровне стойкости ключа обеспечивается более серьезная защита, для реализации такого уровня требуется больший объем ресурсов сервера. Сеансовый ключ Web-сервера обычно имеет длину 40 бит, но в зависимости от необходимого уровня защиты его длина может достигать 128 бит. Чтобы задействовать шифрование, сделайте следующее.

1. Откройте оснастку IIS, выберите Web-сайт, каталог или файл и откройте страницу его свойств.
2. Если вы еще не создали криптографическую пару сервера и не организовали запрос на сертификат, перейдите на вкладку **Directory Security** (Безопасность каталога) или **File Security** (Безопасность файла), а затем нажмите кнопку **Server Certificate** (Сертификат сервера) (рис. 23.13), расположенную в области **Secure**

communications (Безопасные подключения). Выполнить последующие процедуры вам поможет мастер Web Server Certificate Wizard. Если вы уже создали криптографическую пару сервера и сделали запрос на сертификат, перейдите на вкладку **Directory Security** или **File Security**, а затем нажмите кнопку **Edit** (Изменить), расположенную в области **Secure communications**.

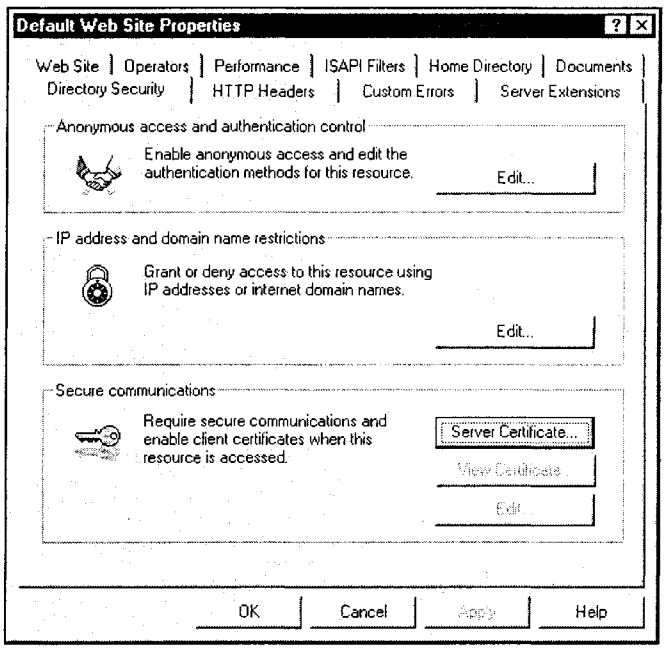


Рис. 23.13. Настройка серверного сертификата для вашего Web-сервера

3. В диалоговом окне **Secure Communications** установите флажок **Require secure channel (SSL)** (Требуется безопасный канал (SSL)).
4. Сообщите пользователям о необходимости установления с вашими Web-публикациями безопасного соединения HTTPS (для этого URL-адрес Web-сайта с ограниченным доступом должен начинаться не с **http://**, а с **https://**).

Примечание

Зашифрованные пересылки могут значительно снизить скорость передачи и производительность сервера, так что шифрованием SSL следует пользоваться исключительно для передачи закрытой информации, например, для проведения финансовых операций.

Вы также можете настроить Web-сервер на применение во всех сеансах безопасных соединений SSL стойкости ключа, как минимум в 128 бит (вместо 40-битовой стойкости, принимаемой по умолчанию). В случае настройки 128 бит как минимальной стойкости пользователям, пытающимся установить безопасный канал связи с вашим сервером, придется пользоваться браузером, способным выполнять обмен информа-

цией с применением 128-битового уровня стойкость сеансового ключа. Чтобы настроить стойкость шифрования, выполните следующие действия.

1. Откройте оснастку IIS, выберите нужный Web-сайт, каталог или файл и откройте страницу его свойств.
2. Если вы еще не создали криптографическую пару сервера и не организовали запрос на сертификат, перейдите на вкладку **Directory Security** (Безопасность каталога) или **File Security** (Безопасность файла), а затем нажмите кнопку **Server Certificate** (Сертификат сервера), расположенную в области **Secure communications** (Безопасные подключения). Выполнить последующие процедуры вам поможет мастер Web Server Certificate Wizard. Если вы уже создали криптографическую пару сервера и сделали запрос на сертификат, перейдите на вкладку **Directory Security** или **File Security**, а затем нажмите кнопку **Edit** (Изменить), расположенную в области **Secure communications**.
3. В диалоговом окне **Secure Communications** установите флажок **Require secure channel (SSL)** (Требуется безопасный канал (SSL)).
4. Установите флажок **Require 128-bit Encryption** (Требуется 128-битовое шифрование), если необходим такой уровень шифрования.
5. Нажмите кнопку **OK**.

Примечание

Криптография с серверным пропусканием (Server-Gated Cryptography, SGC) — это расширение SSL, которое позволяет финансовым организациям, владеющим экспортными версиями IIS, пользоваться стойким (128-битовым) шифрованием. Несмотря на то, что возможности SGC встроены в IIS 5.0, для применения этой технологии требуется специальный сертификат SGC.

Аудит

Для наблюдения за активностью разнообразных видов защиты пользователей и Web-серверов администраторы могут пользоваться методиками аудита безопасности. Аудит конфигурации сервера рекомендуется проводить регулярно, т. к. подобные операции позволяют выявить те области, в которых содержатся ресурсы, допускающие несанкционированный доступ и фальсификацию. Для регистрации аудита можно использовать встроенные утилиты Windows, средства IIS 5.0, а также ваши собственные приложения Active Server Pages (ASP).

Регистрация активности на сайтах

Web- и FTP-сайты можно настроить таким образом, чтобы осуществлялась регистрация пользовательской и серверной активности. Регистрационные данные IIS помогают регулировать доступ к публикациям, определять степень их популярности, производить оценку требований, связанных с безопасностью, а также выполнять локализацию возможных проблем, связанных с Web- или FTP-сайтами. В этой части главы рассматриваются принципы и процедуры, необходимые для управления регистрацией на вашем Web-сайте. Регистрацию активности на сайтах IIS не следует путать с регистрацией событий, которая осуществляется операционной системой

Windows 2000 и просматривается при помощи Event Viewer, поскольку регистрация в IIS является более сложной.

Регистрация типов файлов

Регистрация на Web- или FTP-сайте производится с помощью модулей, которые работают независимо от всех прочих процессов сервера. Для каждого отдельного Web- или FTP-сайта вы можете выбирать формат журналов регистрации. Если регистрация на сайте включена, ее можно отключить или распространить только на отдельные каталоги сайта. Регистрационные файлы, которые создает IIS, можно читать и в текстовом редакторе, но обычно они загружаются в служебную программу формирования отчетов. При регистрации ODBC (Open DataBase Connectivity — открытый интерфейс доступа к базам данных) записи вносятся в базу данных, которая в свою очередь активируется при создании отчетов.

Примечание

Значения времени, приводимые в регистрационных файлах, отражают время обработки сервером запросов и ответов. Они не указывают время прохождения запросов и ответов по сети к клиенту, а также время их обработки на компьютере клиента.

Формат расширенной регистрации W3C

Расширенный формат журналов, разработанный консорциумом W3C, представляет собой настраиваемый формат ASCII с множеством разнообразных полей. В нем предусмотрена возможность включения тех полей, которые важны именно для вас, и при этом размер регистрационных файлов остается вполне умеренным, т. к. в них не включаются ненужные поля. Поля разделяются пробелами. Время фиксируется в формате UTC (Universal Time Coordinated — универсальное синхронизированное время, среднее время по Гринвичу). В нижеследующих примерах приводятся строки файла W3C с полями `Time`, `Client IP Address`, `Method`, `URI Stem`, `HTTP Status` и `HTTP Version`.

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2002-05-02 17:42:15
#Fields: time c-ip cs-method cs-uri-stem sc-status cs-version
17:42:15 172.16.255.255 GET /default.htm 200 HTTP/1.0
```

В этой записи указывается, что `2.05.02` в `17:42` (UTC) пользователь, применявший версию `1.0 HTTP` и IP-адрес `172.16.255.255`, выдал команду HTTP `GET` по отношению к файлу `default.htm`. Запрос был возвращен без каких-либо ошибок. В поле `#Date:` указывается дата создания первой записи журнала, т. е. создания самого журнала. В поле `#Version:` обозначается применявшийся формат регистрирования W3C. Чтобы настроить расширенную регистрацию W3C, сделайте следующее.

1. Выберите нужный Web- или FTP-сайт и откройте страницу его свойств.
2. Активируйте ведение журналов (флажок **Enablet Logging** (Вести журнал), если эта функция отключена), и выберите из списка **W3C Extended log file format** (Расширенный формат файла журнала W3C).
3. Нажмите кнопку **Properties** (Свойства).

4. На вкладке **Extended Properties** (Расширенные свойства) выберите поля, в которые предполагается заносить регистрационные данные. По умолчанию задействованы поля **Time** (Время), **Client IP Address** (IP-адрес клиента), **Method** (Метод), **URI Stem** (Ресурс URI) и **HTTP Status** (Состояние протокола).
5. Нажмите кнопку **Apply** (Применить).

Примечание

Дополнительную информацию о спецификации расширенного формата W3C можно получить на Web-сайте консорциума W3C. **www.w3.org**.

Формат регистрации Microsoft IIS

Формат файла журнала Microsoft IIS — это жесткий (ненастраиваемый) формат ASCII, который обеспечивает регистрацию большего (по сравнению с Общим форматом файлов журнала NSCA Common) количества элементов. Формат Microsoft IIS содержит базовые элементы типа IP-адреса, имени пользователя, даты и времени запроса, кода состояния HTTP и количества полученных байт. Он также включает подробные элементы, например, истекшее время, количество отправленных байтов, действие (например, загрузка, выполненная при помощи команды `GET`), а также целевой файл. Элементы разделяются запятыми, так что читать такие журналы легче, чем данные в других форматах ASCII, в которых в качестве разделителей применяются пробелы. Предполагается фиксация местного времени. Если вы откроете файл формата Microsoft IIS в текстовом редакторе, то его записи будут выглядеть примерно так, как в следующем примере:

```
192.168.114.201, -, 03/20/2001, 7:55:20, W3SVC2, SALES1, 192.168.114.201,
172.21.13.45, 4502, 163, 3223, 200, GET, DeptLogo.gif
172.16.255.255, anonymous, 03/20/98, 23:58:11, MSFTPSVC, SALES1,
192.168.114.201, 60, 275, 0, 0, 0, PASS, intro.htm
```

В этом примере первая запись указывает на то, что анонимный пользователь (на самом деле, гостевой пользователь под учетной записью `IUSER_имякомпьютера`) с IP-адресом `192.168.114.201` выдал команду HTTP `GET` в отношении файла изображения `DeptLogo.gif`. Команда поступила от сервера `SALES1` с IP-адресом `172.21.13.45` в `7:55` `20.03.01`. Для обработки этого 163-битового HTTP-запроса потребовалось `4502` мс (4,5 с). В результате анонимному пользователю было безошибочно (код ответа `200`) возвращено `3223` байта данных. В показанном регистрационном файле все поля отделяются друг от друга запятыми. Дефис (-) ставится в поле, действительное значение которого отсутствует.

Формат файлов регистрации NCSA Common

Формат регистрации NCSA (National Center for Supercomputing Applications — Национальный центр по применению суперкомпьютеров, создавший интернет-браузер NCSA Mosaic) — это жесткий (ненастраиваемый) формат ASCII, применяемый на Web-сайтах (но не на FTP-сайтах). В нем фиксируется основная информация о пользовательских запросах, например, имя удаленного хоста, имя пользователя, дата, время, тип запроса, код состояния HTTP и количество байт, полученных сер-

вером. Элементы разделяются пробелами, фиксируется местное время. Если вы откроете файл формата NCSA Common в текстовом редакторе, то его записи будут выглядеть примерно так, как в следующем примере:

```
172.21.13.45 - REDMOND\fred [08/Apr/2002:17:39:04 -0800] "GET
/scripts/iisadmin/ism.dll?http/serv HTTP/1.0" 200 3401
```

Эта запись обозначает, что `8.04.02` в `17:39` пользователь под именем `Fred` с IP-адресом `172.21.13.45`, расположенный в домене `REDMOND`, выдал команду HTTP `GET` (т. е. загрузил файл). Пользователю `Fred` было безошибочно возвращено `3401` байта данных.

Регистрация ODBC

Формат регистрации ODBC предполагает запись фиксированного набора полей данных в совместимую с ODBC базу данных (например, в Microsoft Access или Microsoft SQL Server). Среди прочих регистрируются такие элементы, как IP-адрес и имя пользователя, дата и время запроса, код состояния HTTP, полученные и отправленные байты, выполненное действие (например, загрузка объекта при помощи команды `GET`), а также цель (например, загруженный файл). Предусматривается фиксация местного времени. В случае применения журнала этого типа вы должны указать базу данных, к которой будет производиться подключение, и настроить ее на прием данных.

Учет процессов

Учет процессов — это новая функция IIS. Ее можно задействовать в рамках отдельно взятого сайта. Она помещает в файл расширенного формата регистрации W3C дополнительные поля, в которых фиксируются данные о том, как Web-сайты потребляют ресурсы процессора на сервере. Эта информация необходима для выявления сайтов, на функционирование которых уходит слишком большой объем ресурсов процесса, а также для определения неисправных сценариев или процессов CGI. Учет процессов не предусматривает детализацию использования ресурсов процессора отдельными приложениями. Регистрируются лишь данные о внепроцессных приложениях. Эта функция применима только к Web-сайтам (в отношении FTP-сайтов она не используется), и запись таких данных производится только в случае использования файлов формата расширенной регистрации W3C. Как правило, данные, получаемые при помощи учета процессов, применяются для определения необходимости в регулировке процессов на Web-сайте. Регулировка процессов ограничивает процессорное время, доступное Web-сайту. Чтобы задействовать учет процессов и, таким образом, приступить к отслеживанию уровня использования процессора, выполните следующие действия.

1. Выберите Web-сайт и откройте страницу его свойств.
2. На вкладке **Web Site** (Web-узел) нажмите кнопку **Properties** (Свойства).
3. Установите флажок **Process Accounting** (Учет процессов), расположенный на вкладке **Extended Properties** (Расширенные свойства) (рис. 23.14).
4. Нажмите кнопку **OK**.

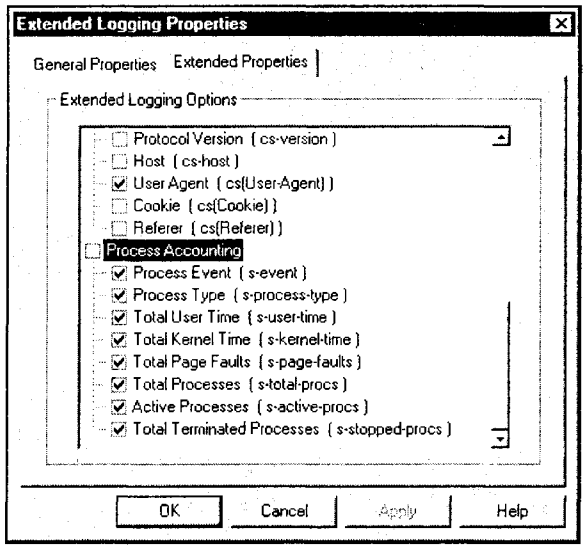


Рис. 23.14. Включение учета процессов в отношении отдельного Web-сайта

Управление журналами регистрации

Активировать регистрацию можно в отношении каждого отдельного Web- или FTP-сайта. При этом нужно выбрать подходящий формат регистрации. При активировании регистрации она распространяется на все каталоги сайта, но вы можете отменить ее по отношению к некоторым из них. Чтобы включить регистрацию на Web- или FTP-сайте, сделайте следующее.

1. Выберите Web- или FTP-сайт и откройте страницу его свойств.
2. На странице свойств **Web Site** (Web-узел) или **FTP Site** установите флажок **Enable Logging** (Вести журнал).
3. Выберите формат из списка **Active log format** (Формат текущего журнала) (рис. 23.15). По умолчанию устанавливаются флажки **Enable Logging** и **W3C Extended Log File Format** (Расширенный формат файла журнала W3C), причем задействуются следующие поля: `Time` (Время), `Client IP Address` (IP-адрес клиента), `Method` (Метод), `URI Stem` (Ресурс URI) и `HTTP Status` (Состояние протокола).
4. Нажмите кнопку **Apply** (Применить).
5. Нажмите кнопку **OK**.

Примечание

Если вы решите задействовать регистрацию ODBC, нажмите кнопку **Properties** (Свойства), а затем введите в соответствующие поля имя источника данных (**Data Source Name**) и имя таблицы в рамках указанной базы данных. Если для обращения к базе данных требуется имя пользователя и пароль, введите их и нажмите кнопку **OK**.

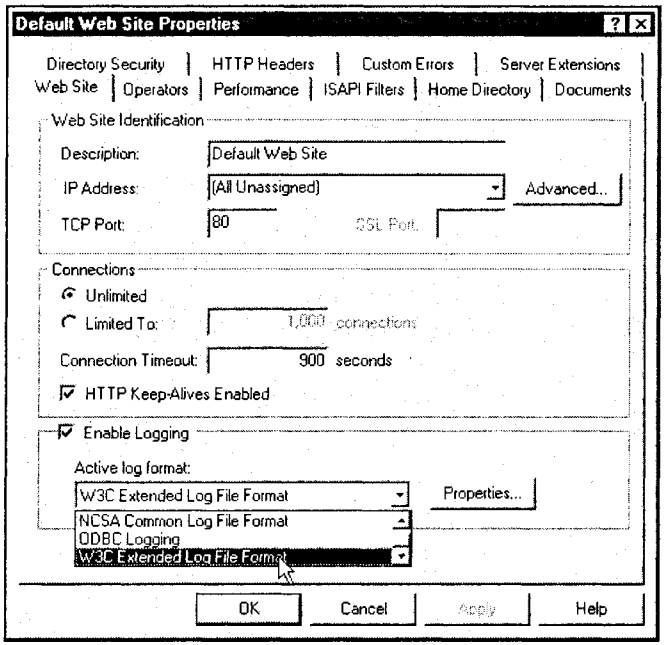


Рис. 23.15. Выбор формата файла регистрации сайта

Чтобы отключить или включить регистрацию каталога в рамках сайта, выполните следующие действия.

1. Выберите нужный каталог и откройте страницу его свойств.
2. На вкладке **Home Directory** (Домашний каталог) или **Directory** (Каталог) взгляните на флажок **Log visits** (Запись в журнал). По умолчанию этот флажок установлен.
3. Чтобы отменить регистрацию в данном каталоге, снимите этот флажок. Чтобы повторно включить регистрацию, установите его. Настоящие настройки не оказывают воздействия на учет процессов.

Сохранение файлов регистрации

Вы можете указать каталог, в котором будет производиться сохранение файлов регистрации, и определить условия создания новых файлов регистрации. Ниже представлена процедура сохранения файлов регистрации.

1. Выберите нужный Web- или FTP-сайт и откройте страницу его свойств.
2. На вкладке **Web Site** (Web-узел) или **FTP Site** нажмите кнопку **Properties** (Свойства).
3. На вкладке **General Properties** (Общие свойства) выберите вариант графика создания новых файлов регистрации. Эти варианты приводятся ниже.
   - *Ежечасно* (**Hourly**). Новые файлы регистрации создаются ежечасно, начиная с первой записи. Эта функция обычно применяется на крупных Web-сайтах.

- *Ежедневно* (**Daily**). Новые файлы регистрации создаются каждый день, начиная с первой записи после полуночи.
- *Еженедельно* (**Weekly**). Новые файлы регистрации создаются каждую неделю, начиная с первой записи после полуночи в субботу.
- *Ежемесячно* (**Monthly**). Новые файлы регистрации создаются каждый месяц, начиная с первой записи после полуночи последнего дня месяца.
- *Неограниченный размер файла* (**Unlimited file size**). Данные всегда сохраняются в один и тот же файл регистрации. Обращение к такому файлу производится только после остановки сайта.
- *При превышении размера...* (**When file size reaches**). Новый файл регистрации создается тогда, когда размер текущего файла достигает установленного порога (нужно указать желаемый размер).

4. В области **Log file** (Каталог файла журнала) введите путь к каталогу, в котором предполагается хранить файлы регистрации. Он должен находиться на локальном диске, причем путь к нему не может быть относительным. Кроме того, при определении каталога файлов регистрации нельзя указывать подключенные диски и пути UNC наподобие \\server1\share1\.
5. Нажмите кнопку **Apply** (Применить).

Настройка производительности

Требования к аппаратному обеспечению зависят от предоставляемых услуг. К примеру, FTP-служба потребляет меньше памяти, чем Web-служба. Кроме того, приложения ASP, сценарии CGI, запросы баз данных и файлы видеоизображений загружают процессор в большей степени, чем статические страницы HTML. Следовательно, чтобы обеспечить для пользователей удовлетворительный уровень обслуживания, вы должны гарантировать оптимальную производительность сервера. Уровень производительности изменяется со временем вслед за изменениями трафика и информации, содержащейся на сайте. Для того чтобы разумно отрегулировать производительность, администратор сервера должен продумать стратегию мониторинга, который может производиться с помощью самых разнообразных инструментальных средств. Эта часть главы посвящена анализу принципов и приемов регулировки производительности сайта.

Основы регулирования

Тестирование производительности и регулирование являются рутинными процессами. Чтобы работа была эффективной, вы должны тщательно спланировать стратегию оценивания своего Web-сервера. Первый этап состоит в измерении текущего уровня производительности. Так как производительность сервера с течением времени может значительно изменяться, мониторинг должен быть достаточно продолжительным, чтобы вы смогли получить реальную картину активности сервера. Вы также должны проанализировать все компоненты системы с целью обнаружения узких мест. Появление узких мест может быть вызвано наличием неподходящего или неверно настроенного аппаратного обеспечения, а также программными настройками IIS или Windows 2000. При проведении мониторинга должна быть предусмотрена проверка производительности во всех областях.

Получив данные о том, как работает ваш сервер, вы должны приступить к планированию изменений, нацеленных на повышение его производительности. Любые изменения должны производиться поочередно, по одному за раз. В противном случае оценка влияния каждого из них в отдельности оказывается невозможной. После внесения изменения мониторинг необходимо продолжить. Так вы сможете выяснить, добились ли вы желаемого результата (и нет ли при этом нежелательных побочных эффектов). Так как изменения, внесенные в один ресурс, могут приводить к возникновению узких мест в других областях, после любого изменения важно проверять производительность всех ресурсов. Оценив влияние отдельного изменения, вы можете определиться с тем, необходима ли последующая корректировка.

Инструментальные средства мониторинга

Мониторинг сервера — это наиболее значительный компонент его администрирования. Подобрав подходящие средства мониторинга, вы получаете возможность выявлять неисправности сервера, оценивать результаты внесения изменений в публикации, размещенные на Web-сайте, и планировать обновления, направленные на расширение доступности ваших сайтов. Оптимальный вариант средств (и методов) резервирования зависит от того, какая информация вам нужна. К примеру, если вы пытаетесь измерить общую нагрузку на Web-сервер, то для выполнения недельного графика вам пригодится System Monitor. С его помощью можно будет организовать вывод таких данных, как количество соединений с компьютером и передач файлов. Если вы замечаете замедление производительности сервера, можно проверить наличие ошибок с помощью Event Viewer (инструментального средства для просмотра журналов регистрации, генерируемых операционной системой Windows 2000). Кроме того, мониторинг сервера можно реализовать в виде анализа журналов регистрации, которые генерируются IIS *(см. ранее разд. "Регистрация активности на сайтах")*. В Windows 2000 поддерживается большое количество инструментальных средств мониторинга.

System Monitor

Утилита System Monitor — это мощный инструмент, применяемый для текущего контроля активности сервера и подведения итогов о его производительности через определенные периоды времени (как в краткосрочной, так и в долгосрочной перспективе). При помощи этого инструмента вы можете выводить данные о производительности в виде графиков или отчетов реального времени, собирать данные в файлы и генерировать предупреждения на случай критических событий. Утилита System Monitor анализирует выходные данные счетчиков, которые осуществляют текущий контроль активности определенных объектов (отдельных служб или механизмов, управляющих ресурсами сервера). К примеру, если вы захотите просмотреть объект под названием Web Service, то увидите счетчики, которые отслеживают количество полученных за одну секунду байт и количество предпринятых за тот же период времени попыток соединения.

Windows 2000 содержит несколько счетчиков, а при помощи утилит, входящих в комплекты ресурсов (Resource Kits) Windows 2000, их можно дополнить счетчиками уровня использования дисков и активности TCP. Помимо этого, IIS предусматривает установку для IIS специальных счетчиков, включая счетчики Web- и FTP-служб, счетчики приложений Active Server Pages и глобальные счетчики. Счетчики Web,

FTP и Active Server Pages отслеживают активность соединений, а глобальные счетчики IIS осуществляют текущий контроль таких параметров, как уровень использования пропускной способности и активность кэширования в отношении всех служб IIS.

Event Viewer

Windows 2000 содержит службу регистрации событий, которая фиксирует, например, ошибки при запуске службы или ее успешный старт. Такие журналы регистрации событий просматриваются с помощью Event Viewer. Эта утилита применяется для мониторинга журналов регистрации событий системы (System), безопасности (Security) и приложений (Application). Располагая этими данными, вы можете лучше понять последовательность и типы событий, которые становятся причиной появления конкретной проблемы производительности.

Task Manager

Утилита Task Manager может применяться для просмотра текущих заданий и потоков. Через нее также производятся изменения назначенного приоритета процессов. Впрочем, после завершения процесса новая настройка приоритета теряется. Уровни использования процессора и памяти можно просматривать в режиме реального времени, но эти данные не сохраняются.

Network Monitor

Утилита Network Monitor отвечает за сбор данных об исходящем и входящем трафике компьютера и предоставляет подробную информацию об отправляемых и получаемых кадрах. Этот инструмент помогает анализировать сложные модели сетевого трафика. С помощью Network Monitor можно просматривать данные заголовков, включаемые в HTTP- и FTP-запросы, поступающие на сервер. В большинстве случаев перед вами стоит задача разработки фильтра захвата, который работает как запрос базы данных, выделяя подмножество передаваемых кадров. Также существует возможность применения триггера захвата, который реагирует на события, происходящие в сети, инициированием операции (подобной запуску исполняемого файла).

Оптимизация диска

Узкие места, связанные с жесткими дисками, наиболее часто фиксируются на сайтах с очень большими наборами файлов, обращения к которым случаются нерегулярно. То, насколько часто IIS приходится обращаться к жесткому диску, напрямую зависит от объема оперативной памяти, а также от количества и размеров запрашиваемых файлов. Если объем оперативной памяти мал, а запросы подаются на большое количество различных файлов (или размеры запрашиваемых файлов значительны), IIS теряет возможность сохранения копий этих файлов в оперативной памяти, и, следовательно, не может обеспечить более быстрый доступ к ним. В таком случае IIS оказывается вынужденным получать файлы с жесткого диска (посредством файла подкачки). Оперативность, с которой IIS может обнаружить запрашиваемый файл, обуславливается скоростью доступа и размером жесткого диска.

Для проведения мониторинга жестких дисков следует задействовать утилиту System Monitor, которая будет регистрировать уровень использования процессора в процентном отношении, уровень использования сетевого адаптера и счетчик %Disk

Time объекта Physical Disk (рис. 23.16). Если показания счетчика %Disk Time высоки (но процессор и сетевой адаптер не достигли предела насыщения), значит, узкое место создает диск.

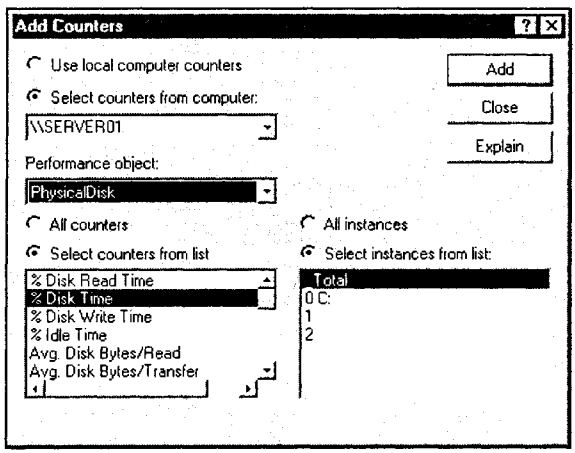


Рис. 23.16. Добавление счетчиков в System Monitor

Чтобы повысить эффективность обращения к диску, сформируйте массив RAID с наборами расслоенных дисков. Если сервер активно применяется для работы с базой данных, то, возможно, вам понадобится увеличить объем оперативной памяти (довести его до 1 Гбайт или более), поскольку таким способом можно свести к минимуму задержки при доступе к диску, или установить RAID-контроллер с объемным кэшем оперативной памяти. Кроме того, следует вести резервирование. В этом случае вам не придется проводить восстановление с резервных копий, если из строя выйдет один из дисков. Многие современные контроллеры поддерживают возможность горячей замены, так что при сбое диска его замена может производиться без вынужденного простоя сервера. В любом случае, нужно создавать качественные резервные копии и хранить одну из них вне рабочего места.

Оптимизация памяти

Любому компьютерному специалисту известно, что ОЗУ — это пространство памяти, используемое программами во время их работы. Как правило, при запуске приложения компьютер копирует необходимые программные файлы с жесткого диска в оперативную память, и приложение работает именно в ней. Время доступа к оперативной памяти значительно меньше аналогичного показателя для жесткого диска, так что чем меньше компьютер обращается к жесткому диску, тем быстрее могут работать приложения. При работе IIS он тоже занимает некоторую часть оперативной памяти. То, какова эта часть, зависит от ряда факторов, включая следующие:

- объем оперативной памяти, применяемой для кэширования;
- размер файла подкачки;
- объем свободного дискового пространства;

- количество запущенных служб;
- тип процессора(ов);
- количество и размер информационных файлов (например, файлов HTML);
- количество соединений, открытых в данный момент времени;
- другие активные приложения, требующие пространства в оперативной памяти.

Кэш-память

Когда IIS получает запрос на статический файл, индекс этого файла кэшируется Web-сервером в оперативной памяти, а сам файл кэширует операционная система Windows 2000. При последующих запросах на тот же файл IIS пользуется его копией, кэшированной в оперативной памяти (вместо того, чтобы возвращаться к жесткому диску для очередного извлечения файла). В результате период времени, необходимый IIS для выполнения запроса, уменьшается, а в глазах посетителей скорость доступа увеличивается. Впрочем, время, в течение которого файл хранится в кэше, зависит от ряда других факторов. По мере того как в IIS поступают запросы на другие объекты, файлы, кэшированные ранее, удаляются из кэша, освобождая пространство для нового содержимого. Это означает, что, если через IIS возможно обращение к большому числу файлов, но объем ОЗУ незначителен, доступ может быть замедлен. При этом IIS вынужден извлекать многие файлы с жесткого диска. Если на том же компьютере работают другие приложения, также потребляющие ресурсы оперативной памяти, то кэшированные копии файлов вытесняются из памяти, освобождая пространство для новых файлов. Вполне возможно, что IIS не сможет содержать кэшированные файлы в оперативной памяти. Результатом является замедление доступа через IIS, т. к. файлы извлекаются с жесткого диска.

Поскольку крупные файлы занимают в оперативной памяти больше пространства, чем файлы небольших размеров, запросы на крупные файлы (например, файлы со звуком или видеоизображениям) могут привести к значительной реорганизации кэшированных файлов. Так происходит в том случае, если объем оперативной памяти невелик. Если ваши документы значительны по размеру, если вы публикуете большое количество документов или если на компьютере с IIS вы пользуетесь другими приложениями, активно потребляющими ресурсы ОЗУ, повышение производительности системы можно осуществить путем добавления памяти. Впрочем, если вы публикуете очень небольшое количество файлов (или их размеры относительно малы), приращение оперативной памяти не приведет к повышению производительности Web-сервера. Повлиять на производительность может настройка объема памяти, который Windows 2000 выделяет под файловый кэш. Если важнейшей функцией вашего сервера является размещение Web-сервера, настройте его как сервер приложений (заменив этой установкой принимаемую по умолчанию настройку функции файлового сервера).

1. На рабочем столе откройте **My Computer** (Мой компьютер), а затем выберите **Network and Dial-up Connections** (Сеть и удаленный доступ к сети).
2. Щелкните на **Local Area Connection** (Подключение по локальной сети) правой кнопкой мыши и откройте соответствующий список свойств.
3. Выберите **File and Printer Sharing for Microsoft Networks** (Служба доступа к файлам и принтерам сетей Microsoft) и нажмите **Properties** (Свойства).

4. В свойствах **Server Optimization** (Оптимизация сервера) установите переключатель в положение **Maximize data throughput for network applications** (Максимум производительности для сетевых приложений) (рис. 23.17).

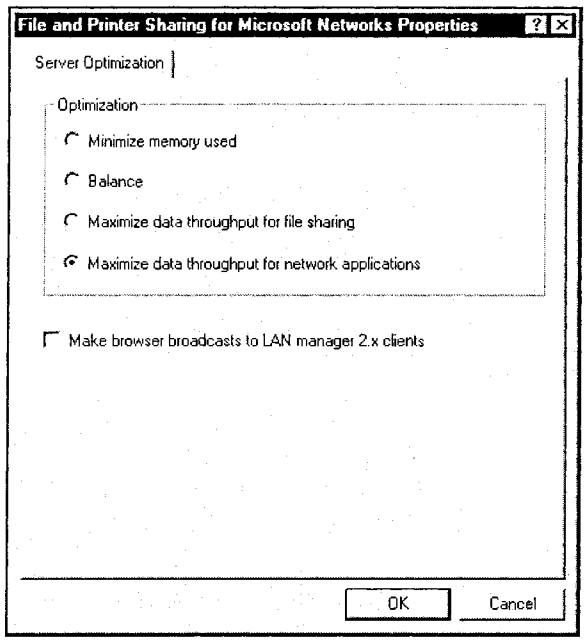


Рис. 23.17. Оптимизация сервера в расчете на сетевые приложения

Провести оценку производительности кэша сервера помогает утилита System Monitor. Выбирая объект производительности, выберите **Internet Information Services Global** и для ознакомления с активностью кэша воспользуйтесь следующими счетчиками:

- очистки кэша (Cache Flushes);
- результативные обращения в кэш (Cache Hits);
- результативные обращения в кэш в процентном отношении (Cache Hits %);
- нерезультативные обращения в кэш (Cache Misses);
- индексы кэшированных файлов (Cached File Handles);
- перечни файлов каталогов (Directory Listings);
- объекты (Objects).

Значение счетчика Cache Hits % должно быть как можно выше. Низкое значение (в особенности если оно сопровождается высоким значением счетчиками % Disk Time объекта Disk) указывает на то, что ваш сервер не может извлечь достаточное количество своих файлов из кэша. Это может обуславливаться либо большим количеством различных запрашиваемых файлов, либо незначительным объемом и необходимостью увеличения кэша.

Память и скорость отклика

Чтобы повысить скорость отклика на запросы, обычно требуется специально выделить память и ресурсы процессора отдельным соединениям. Таким образом, ресурсы, доступные для других приложений, продолжают быть ограниченными даже тогда, когда запросы не поступают. Максимальное увеличение производительности памяти в отношении всех приложений, работающих на вашем сервере, может привести к незначительному снижению оперативности откликов на запросы, исходящие от пользователей, которые приходят на ваш сайт (дело в том, что ресурсы памяти и процессора выделяются запросам не сразу).

Как правило, для оптимального использования памяти и времени отклика IIS должен автоматически настроиться. Для этого достаточно рассчитать количество запросов, поступающих за 24-часовой период. При изменении этой расчетной оценки IIS устанавливает новое число сокетов, выделяемых для прослушивания новых запросов. Если указанное число немного превосходит фактическое количество соединений, то попытки соединений проходят быстрее. Если это число значительно превосходит фактическое количество попыток соединения, происходит растрата памяти. Чтобы определить число соединений с сервером за один день, воспользуйтесь журналом регистрации System Monitor. Он может регистрировать значения счетчиков **Total Connection Requests** (Общее количество запросов на соединение) и **Current Connections** (Текущие соединения). Оба они находятся в рамках объекта Web Service. Чтобы добиться реалистичной фиксации условий, возникающих на вашем сервере, проводите сбор данных в файлах регистрации в течение нескольких дней (если это

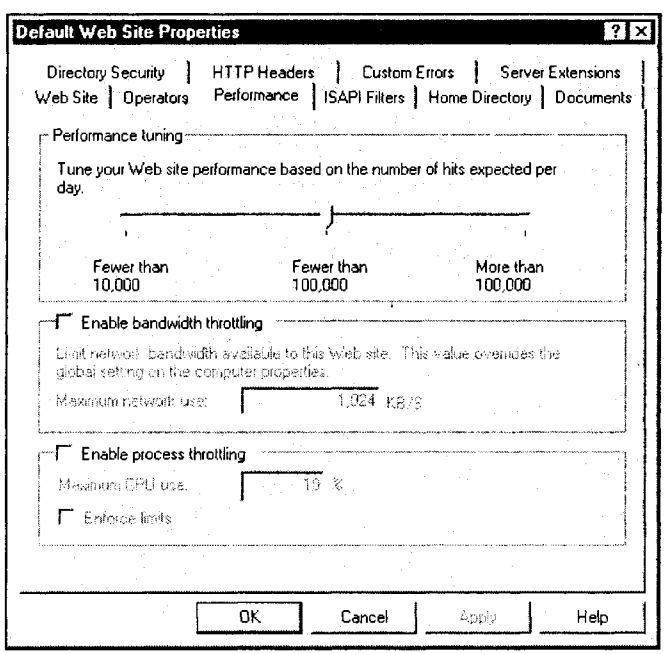


Рис. 23.18. Регулировка производительности Web-сервера исходя из рассчитанного количества соединений

возможно). После этого, исходя из своих расчетов, укажите число ежедневных соединений. Откройте оснастку IIS, выберите нужный Web-сайт и, чтобы вывести страницу его свойств, нажмите кнопку **Properties** (Свойства). На вкладке **Performance** (Быстродействие) укажите значение, незначительно превосходящее исчисленное количество соединений, прием которых ожидается в течение 24-часового периода (рис. 23.18).

В IIS 5.0 сайты с разными IP-адресами (но с одинаковым номером порта) пользуются одним и тем же набором сокетов. Таким образом, создание нескольких сайтов с разными IP-адресами (но с единым для всех портом 80) не приводит к значительному увеличению потребления неперемещаемой области памяти со стороны IIS. IIS гибко распределяет сокеты между всеми сайтами, таким образом добиваясь снижения потребления ее ресурсов. Такое объединение сокетов позволяет IIS 5.0 размещать на одном оборудовании намного больше сайтов, чем было возможно в IIS 4.0. Впрочем, объединение сокетов вынуждает IIS проводить прослушивание всех IP-адресов, что приводит к появлению риска компрометации системы безопасности защищенных доменов в рамках нескольких сетей. Кроме того, действия по сужению пропускной способности и регулировке производительности распространяются на все Web-сайты, настроенные на применение единого номера порта. Если вы прибегаете к сужению пропускной способности (или выполняете другие действия, связанные с регулировкой производительности) по отношению к отдельным сайтам, то объединение сокетов для этих сайтов необходимо запретить.

Оптимизация процессора

По мере развития Web-серверов производительность становится все более значимым фактором. На сегодняшний день, с увеличением количества Web-приложений, предназначенных для публикаций баз данных, индексирования информации и совместной работы, максимизация аппаратной и программной производительности стала важнейшей задачей. В этой части главы мы обратимся к тем аспектам производительности, которые определяются процессором, и приведем рекомендации по модернизации, исходя из результатов тестов контроля производительности.

Узкие места из-за процессоров

Процессор выполняет текущую обработку инструкций, получаемых компьютером. Скорость передачи информации между различными компонентами компьютера (такими как сам процессор, жесткий диск и оперативная память) обуславливается тактовой частотой процессора и размером шины данных, применяемой им для этих целей. Тактовая частота обычно измеряется в мегагерцах (МГц) или гигагерцах (ГГц). Типичная шина данных способна передавать 16, 32 или 64 бита данных за один такт. Измерение производительности процессора производится с помощью утилиты System Monitor. Узкие места системы, обусловленные процессором, характеризуются очень высокими процентными показателями уровня использования процессора (CPU % Utilization) в условиях, когда мощности сетевого адаптера потребляются далеко не в полном объеме. Если показатель CPU % Utilization высок, вы можете:

- модернизировать процессор;
- установить на тот же компьютер дополнительные процессоры;

- скопировать сайт на другой компьютер и распределить трафик между этими двумя компьютерами;
- переместить приложения, потребляющие значительные ресурсы процессора (например, программы для работы с базами данных), на другой компьютер.

Регулировка использования процессора

Вы можете ограничить процент времени, которое будет затрачиваться процессором на обработку внепроцессных приложений WAM, ISAPI и CGI применительно к отдельным Web-сайтам, разрешив регулировку процессов. Ограничение обращений к процессору оказывается полезным, если на одном компьютере размещается большое количество сайтов, и при этом выясняется, что внепроцессные приложения одного из этих сайтов потребляют все ресурсы процессора (не допуская к нему другие сайты). Если для обработки приложений сайта, для которого введены подобные ограничения, в течение заданного периода требуется больше времени, чем назначенный процент, то исходя из масштаба перерасхода такое событие регистрируется.

- *Уровень 1.* Событие фиксируется в журнале регистрации событий Windows 2000, когда суммарный уровень использования процессора превышает предельный за определенный период времени.
- *Уровень 2.* Событие фиксируется в журнале регистрации событий, когда уровень использования процессора превышает 150% от предустановленного; для всех внепроцессных приложений на данном Web-сайте приоритет обращения к процессору приравнивается к Idle (обращение возможно только в случае простоя процессора).
- *Уровень 3.* Событие фиксируется в журнале регистрации событий, когда уровень использования процессора превышает 200% от предустановленного; все внепроцессные приложения данного Web-сайта останавливаются.

После того как сайт достиг уровня 2 или 3, соответствующее событие остается в силе вплоть до наступления следующего временного интервала. К примеру, если в течение 24-часового интервала внепроцессным приложениям сайта разрешается занимать 10% времени обработки процессора, то приложения этого сайта должны обращаться к процессору в течение 2,4 часов из 24. Если сайт занимает процессор более 2,4 часов, но менее 3,6 часов, то единственным последствием окажется фиксация этого события в журнале регистрации событий. После того как время обращения сайта к процессору превысило 3,6 часов, всем внепроцессным приложениям этого сайта присваивается приоритет Idle. Если сервер не очень загружен, и приложения продолжают потреблять время процессора, то в конечном итоге при достижении уровня 4,8 часов из 24-часового интервала все внепроцессные приложения Web-сайта останавливаются. Чтобы отрегулировать использование процессора Web-сайтом, выполните следующие действия.

1. Откройте интегрируемое приложение IIS и выберите Web-сайт, в отношении которого планируете ограничить уровень использования процессора.
2. Откройте страницу свойств этого Web-сайта и перейдите на вкладку **Performance** (Быстродействие).
3. Установите флажок **Enable process throttling** (Разрешить регулировку процесса) (см. рис. 23.18) и введите процент от общего времени процессора, которым предполагаете ограничить сайт.

4. Если вы хотите разрешить, чтобы вступали в силу последствия переиспользования процессорного времени уровней 2 и 3, установите флажок **Enforce limits** (Наложить ограничения).

В случае разрешения регулировки процессов следует снизить значение интервала блокировки по превышению лимита времени для CGI. По умолчанию этот интервал приравнивается к 5 минутам. Если приложение CGI выходит из строя, поток не снимается вплоть до достижения значения лимита времени. Период времени между сбоем и окончательным отпусканием потока учитывается при расчете времени процессора, потребляемого данным приложением. Временной лимит CGI в IIS 5.0 — это общее количество времени, в течение которого приложение CGI должно быть выполнено (т. е. это не просто период времени до обмена данными).

Сужение пропускной способности

Каждое соединение предполагает выделение значительной пропускной способности. Сужая пропускную способность, потребляемую IIS, вы обеспечиваете наличие свободной пропускной способности для других приложений (например, для почтовых и новостных серверов). Если на основе IIS работает несколько Web-сайтов, можно сузить пропускную способность для каждого из них в отдельности. Это позволит гарантировать наличие пропускной способности для всех сайтов, применяющих один сетевой адаптер. Сужение пропускной способности распространяется только на пропускную способность, потребляемую файлами HTML.

Хотя данные об общем количестве попыток соединения за день и могут дать представление об общей активности на отдельном сайте, необходимо учитывать изменения частоты соединений (параметра, отражающего количество соединений в секунду). Лишь в этом случае вы сможете определить наличие/отсутствие перегрузок в пиковые промежутки времени. Если более 50% общей пропускной способности канала используется регулярно, нужно рассмотреть возможность его модернизации. Если вы только приступаете к настройке Web-сайта и не располагаете данными, пригодными для анализа, но при этом планируете запустить несколько служб (например, Web-, почтовый и новостной серверы), лучше начать с установки 50% ограничения для Web-сервера по применению им полезной пропускной способности. По прошествии некоторого рабочего времени вы сможете проанализировать производительность сайта и соответствующим образом скорректировать пропускную способность.

Чтобы организовать сужение пропускной способности, в первую очередь определите, какая ее часть потребляется сервером. Чтобы ознакомиться с показаниями счетчика **Bytes Total/sec** (Всего байт/с) или **Current Bandwidth** (Текущая пропускная способность) объекта **Network Interface** (Сетевой интерфейс), воспользуйтесь утилитой System Monitor. Если вы предпочитаете сравнить входящий и исходящий трафик, можете ознакомиться с показаниями обоих соответствующих счетчиков: **Bytes Sent/sec** (Отправлено, байт/с) и **Bytes Received/sec** (Получено, байт/с). Сравните эти значения с суммарной пропускной способностью вашего сетевого канала. При нормальной нагрузке ваш сервер не должен использовать более 50% общей полезной пропускной способности. Оставшаяся пропускная способность задействуется в пиковые периоды. Чтобы сузить пропускную способность, потребляемую IIS, выполните описанные далее действия.

1. Откройте оснастку IIS и выберите компьютер, на котором установлен сервер IIS.
2. Открыв страницу свойств IIS, установите флажок **Enable Bandwidth Throttling** (Регулировка полосы пропускания).
3. В поле **Maximum Network Use** (Предельная нагрузка на сеть) введите максимальное количество килобайт в секунду (Кбайт/с), которое должно быть доступно IIS.

Чтобы сузить пропускную способность для отдельного Web-сайта, сделайте следующее.

1. Откройте оснастку IIS, выберите нужный Web-сайт, а затем, чтобы вывести страницу его свойств, нажмите кнопку **Properties** (Свойства).
2. На вкладке **Performance** (Быстродействие) установите флажок **Enable bandwidth throttling** (Регулировка полосы пропускания) (см. рис. 23.18).
3. В поле **Maximum network use** (Предельная нагрузка на сеть) введите максимальное количество килобайт в секунду, которое должно быть доступно данному Web-сайту.

Производительность соединения локальной сети

Помимо аппаратного обеспечения сервера на его производительность напрямую влияет тип сетевого соединения. Если ваш сетевой канал не справляется с объемом данных, который по нему передается, производительность сервера значительно снижается. Пропускная способность, доступная IIS, также зависит от других приложений, выполняемых на том же компьютере и требующих предоставления пропускной способности (в качестве примера можно привести программы электронной почты). В условиях работы довольно загруженного сайта сервер IIS способен полностью использовать ресурсы платы Ethernet со скоростью передачи данных 10 Мбит/с. Чтобы предотвратить ограничение сервера сетью, нужно активировать либо несколько плат Ethernet на 10 Мбит/с, либо установить одну плату Ethernet со скоростью передачи данных 100 Мбит/с.

Для проверки насыщения сети нужно проверить показатели счетчика **CPU % Utilization** (% использования процессора) утилиты System Monitor на компьютере клиента и на сервере. Если производительность процессора не ограничивает ни клиента, ни сервер, значит, в качестве источника проблемы выступает что-то другое. Чтобы проверить уровень использования сети, можно также воспользоваться утилитой Network Monitor операционной системы Windows 2000. Если этот показатель близок к 100% (в отношении клиента или сервера), значит, вероятнее всего, узким местом является сама сеть. Имейте в виду, что различные модели сетевых адаптеров работают по-разному. Производительность сетевого адаптера определяется драйверами и их настройками, устанавливаемыми во время конфигурации этого устройства. Попробуйте связаться с производителем вашего сетевого адаптера и проверить наличие обновленных версий драйверов.

Производительность интернет-соединения

Пропускная способность Интернета обуславливает скорость доставки данных на ваш компьютер, а также количество запросов, обслуживание которых может проводиться

одновременно. Если для того количества запросов, которое поступает на ваш сайт, производительности не хватает, возможны задержки и сбои. Подключение компьютера к Интернету производится через плату сетевого адаптера или другое сетевое устройство (например, через модем или плату ISDN). Объем полезной пропускной способности является функцией выбранного вами типа соединения.

Кроме определения количества одновременных пользовательских запросов, на обслуживание которых вы рассчитываете, следует учесть скорость, на которой ваши файлы (Web-страницы) отсылаются пользователям. Скорость передачи данных обуславливается скоростью соединения и размером файла. Обычно считается, что на отправку страницы (без внешней графики, аудио- и видеоматериалов) должно уходить не более пяти секунд. Загрузка внешних файлов, как правило, происходит после окончания загрузки текста. Общее правило, касающееся внешних файлов, заключается в том, что время их загрузки не должно превышать 30 секунд. Определившись с величиной пропускной способности, необходимой для работы вашего Web- или FTP-сервера, нужно решить, предполагается ли предоставление других служб, требующих пропускной способности. В число таких служб входят электронная почта, новости, потоковая трансляция аудио- или видеоданных.

Как правило, интернет-соединение направлено к маршрутизатору, а за подключение вашего компьютера к маршрутизатору отвечает плата сетевого адаптера. Чтобы предотвратить возникновение узкого места между интернет-соединением и вашим компьютером, необходим высокопроизводительный сетевой адаптер. К примеру, если подключение к Интернету производится по каналу T1 с пропускной способностью 1,54 Мбит/с, то вариант размещения ваших серверов в локальной сети Ethernet со скоростью передачи 10 Мбит/с должен оказаться вполне достаточным. В то же время, если к Интернету вы подключены посредством канала T3, то серверы имеет смысл расположить в локальной сети на основе распределенного интерфейса передачи данных по оптическим каналам (Fiber Distributed Data Interface, FDI), т. к. пропускная способность T3, приравниваемая к 45 Мбит/с, значительно выше скорости передачи 10 Мбит/с, характерной для сетей Ethernet; в последнем случае даже возможен вариант локальной сети на 100 Мбит/с.

Сжатие страниц

Производительность страниц можно повысить при помощи сжатия. Сжатие HTTP предусматривает снижение времени передачи между браузерами, допускающими сжатие, и IIS. Сжатые файлы быстрее загружаются и повышают производительность любого браузера, работающего в условиях сетевого соединения с ограниченной пропускной способностью (например, модемного соединения). Возможно сжатие только статических файлов, а также статических файлов в сочетании с приложениями. Сжатие HTTP (по крайней мере, в отношении статических файлов) оказывается удобным в том случае, если пропускная способность вашего сервера ограничена. Впрочем, если уровень использования процессора и так чрезмерно высок, дополнительные накладные расходы, связанные с выполнением сжатия (в особенности при сжатии динамических данных), в действительности могут повлиять на производительность сервера неблагоприятным образом.

Когда IIS получает запрос, он проверяет, допускает ли соответствующий браузер сжатие. Затем IIS проверяет расширение запрошенного файла, чтобы определить,

является ли он статическим, или динамическим. Если файл статичен, IIS узнает, поступали ли запросы на него ранее (возможно, он уже хранится в сжатом формате во временном каталоге сжатия). Если нужного файла в сжатом формате не существует, IIS отправляет его браузеру в несжатом варианте, а затем сохраняет его сжатую копию во временном каталоге сжатия. Если версия файла в сжатом формате уже создана, IIS отправляет браузеру именно ее. Сжатие файлов производится после первого запроса, поступившего на них со стороны браузера. Если файл содержит динамические данные, IIS сжимает его сразу после генерации и отправляет браузеру его сжатый вариант, при этом его копии не сохраняется.

Простого способа проверки эффективности сжатия HTTP не существует. Прежде чем задействовать сжатие, воспользуйтесь утилитой System Monitor. Чтобы собрать исходные данные, организуйте регистрацию показаний счетчика **% Processor Time** (% процессорного времени) объекта Processor в течение нескольких дней. Этот счетчик фиксирует общее значение Total, а также значение для каждого процессора в системе. Если на вашем сервере установлено несколько процессоров, то, помимо общих данных, следует ознакомиться с показателями отдельных процессоров. Так вы сможете выявить неравномерное распределение рабочей нагрузки. Ниже приводится процедура включения сжатия HTTP.

1. Откройте оснастку IIS, выберите пиктограмму компьютера, а затем, чтобы вывести страницу его свойств, нажмите кнопку **Properties** (Свойства).
2. Выберите **Master Properties** (Мастер свойств), **WWW Service** (WWW-служба).
3. Нажмите кнопку **Edit** (Изменить).
4. На вкладке **Service** (Служба) установите флажок **Compress static files** (Сжимать статические файлы) (рис. 23.19). Так вы включите сжатие статических файлов для их передачи клиентам, поддерживающим сжатие.
5. Чтобы разрешить сжатие прикладных файлов, установите два флажка: **Compress static files** (Сжимать статические файлы) и **Compress application files** (Сжимать файлы приложений).
6. Чтобы определить каталог, в котором будут храниться сжатые файлы, введите путь к локальному каталогу в поле **Temporary folder** (Временный каталог) или с помощью кнопки **Browse** (Просмотр) найдите его. Этот каталог должен располагаться на локальном диске в разделе NTFS. Каталог не может быть коллективным и сжатым.
7. Установите неограниченный (**Unlimited**) максимальный размер этого каталога или ограничьте его, введя значение размера в текстовом поле **Limited**.

Разрешив сжатие, продолжайте в течение некоторого времени (желательно в течение нескольких дней) регистрировать показатели указанных счетчиков. Так вы получите достаточные данные для сравнения. Сопоставьте показатели, полученные в отсутствие сжатия и при его наличии. Если в ходе проверки вы замечаете признаки возникновения узких мест, имеет смысл остановиться. Серьезное ухудшение показателей означает, что производительность сервера при наличии сжатия оказалась ниже, чем в его отсутствие.

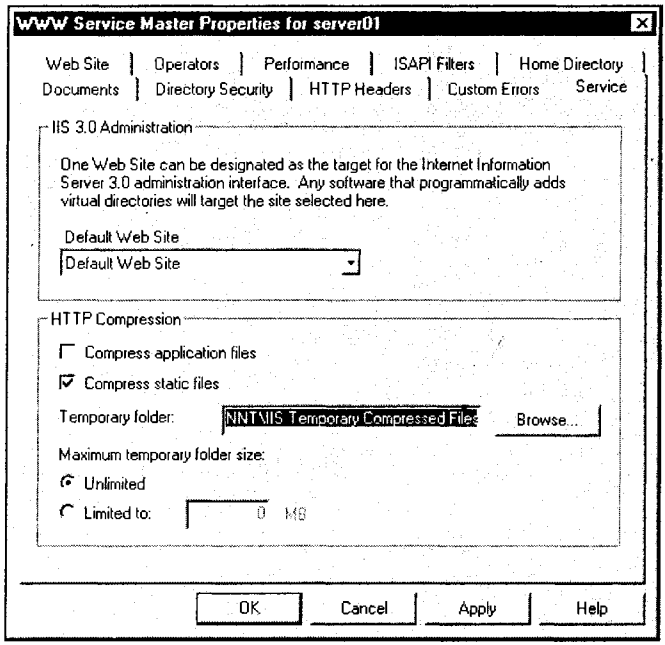


Рис. 23.19. Настройка сжатия HTTP с целью ускорения загрузки Web-страниц

Ограничения на количество соединений

Ограничение соединений — это еще один способ сбережения пропускной способности для других приложений (например, для почтового или новостного сервера, или для другого Web-сайта, работающего на том же Web-сервере). Все попытки установления соединений сверх ограничения отклоняются. Чтобы установить ограничение на количество соединений, воспользуйтесь утилитой System Monitor. Организуйте регистрацию показаний счетчиков **Current Connections** (Текущие соединения), **Maximum Connections** (Максимальное количество соединений) и **Total Connection Attempts** (Общее количество попыток соединения), относящихся, по меньшей мере, к двум объектам Web Service (Web-служба) и FTP Service (FTP-служба). Продолжайте практику регистрации (в течение нескольких дней или недели) до того момента, пока вам не удастся выявить норму. Для ограничения количества соединений необходимо сделать следующее.

1. Откройте оснастку IIS, выберите нужный Web-сайт, а затем, чтобы вывести страницу его свойств, нажмите кнопку **Properties** (Свойства).
2. На вкладке **Web Site** (Веб-узел) установите переключатель в положение **Limited to** (Предельное число).
3. В поле **Connections** (рис. 23.20) введите максимальное количество допустимых одновременных соединений. Положение переключателя **Unlimited** (Неограниченное число) предусматривает возможность установления такого количества одновременных соединений, которое может обеспечить пропускная способность и процессор.

4. В поле **Connection Timeout** (Время ожидания) введите время простоя соединения в секундах.

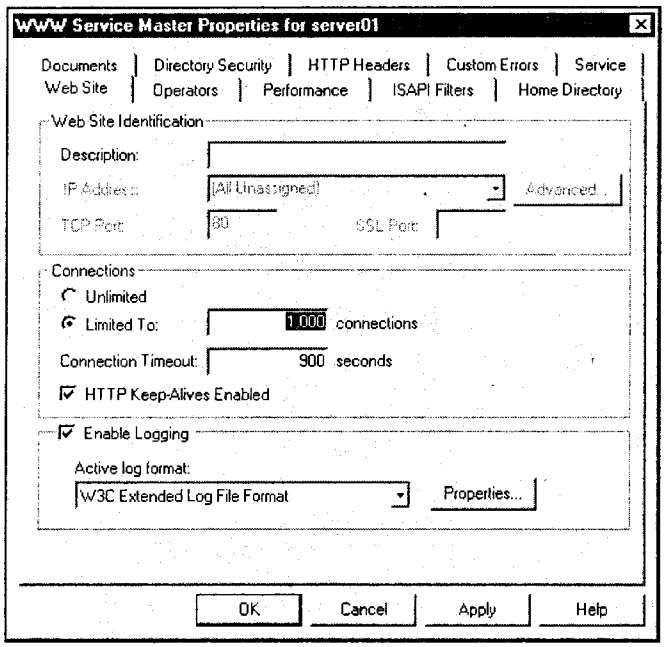


Рис. 23.20. Сужение пропускной способности путем ручного ограничения количества активных соединений с Web-сервером

Дополнительные ресурсы

Apache: **www.apache.org**.

FrontPage: **www.microsoft.com/isapi/redir.dll?prd=frontpage express&ar=home**.

Организация по присвоению имен и номеров в Интернете (Internet Corporation for Assigned Names and Numbers, ICANN): **www.icann.org**.

IIS: **www.microsoft.com/isapi/redir.dll?prd=ieak&ar=isn**.

Learn ASP: **www.learnasp.com/aspng/index.aspx**.

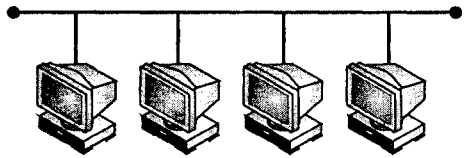
Универсальная сеть доступа к данным Microsoft: **www.microsoft.com/isapi/redir.dll?prd=mdac**.

Microsoft: **www.microsoft.com**.

Институт SANS: **www.sans.org**.

Обновление Windows: **windowsupdate.microsoft.com/isapi/redir.dll?prd=windowsupdate**.

Консорциум Интернета (W3C): **www.w3.org**.



ГЛАВА 24

Администрирование и безопасность Windows 2000

Windows 2000 — это универсальная операционная система (ОС), подходящая для сетей разных масштабов, а такие версии Windows, как NT/2000, обычно признаются самыми востребованными из всех доступных сетевых ОС (на некоторых платформах, кроме того, устанавливается Windows XP). Она содержит ряд мощных и прогрессивных функций, включая IIS (Web- и FTP-службы), сервер Telnet, кластеризацию, поддержку DNS и DHCP и т. д. Помимо прочего, хорошо известный графический интерфейс делает Windows 2000 комфортной средой как для администраторов, так и для пользователей, каким бы опытом они ни обладали. Впрочем, многообразие функций, содержащихся в Windows, предполагает крутую кривую обучения, что делает овладение предметом довольно сложной задачей. В этой главе администраторам будет представлен обзор функций Windows 2000, рассмотрены процессы инсталляции и базового тестирования, изложены основные принципы администрирования пользователей и выстраивания защиты.

Примечание

Подробная информация об операционной системе Windows 2000 и администрировании содержится в комплекте ресурсов (Resource Kit) Windows 2000; кроме того, существует огромное количество книг, в которых эти темы рассмотрены детальнейшим образом.

Основы инсталляции

Если на вашем сервере не была предустановлена Windows 2000, вам придется пройти через процесс ее инсталляции. По сути, он предельно автоматизирован, но по ходу его выполнения вам придется принимать те или иные решения. Существует множество способов установки Windows 2000 Server, однако, что касается запуска процесса инсталляции, у вас есть лишь два варианта: либо загрузиться с компакт-диска Windows 2000 Server, либо приготовить загрузочные дискеты. Большинство серверов, собранных менее пяти лет назад, способны загружаться со своих приводов CD-ROM (а это, несомненно, лучшее решение для выполнения инсталляции). Впрочем, если необходимость в приготовлении загрузочных дискет все же возникнет (например,

если на сервере нет привода CD-ROM), то вам придется это сделать, запустив программу makeboot.exe, расположенную в каталоге \Bootdisk компакт-диска Windows 2000 Server. При составлении обзора инсталляции для этой главы допускалось, что вы загружаетесь с компакт-диска Windows 2000 Server.

Запуск программы установки

Если раньше вы уже устанавливали какую-либо версию Windows, то знаете, что нужно для запуска стандартной программы установки (Setup). Процесс инсталляции Windows 2000 в этом смысле ничем не отличается. При загрузке с компакт-диска Windows 2000 Server сначала появляется экран реального режима (DOS), который помогает принять первые решения, связанные с установкой. Чтобы подтвердить свое намерение установить Windows 2000 Server, нажмите клавишу <Enter> (или, чтобы выйти из программы установки, нажмите <F3>). После этого решите, что вам нужно: установить Windows 2000 Server или восстановить существующую инсталляцию этой операционной системы. Для установки Windows 2000 Server следует нажать клавишу <Enter>. В результате на экране появится многословное лицензионное соглашение Windows 2000 Server. Прочтите его, проникнитесь, а затем, чтобы выразить свое согласие и продолжить инсталляцию, нажмите клавишу <F8>.

Управление разделами

Когда начнется процесс инсталляции, перед вами появится перечисление всех имеющихся разделов диска, на которые можно установить Windows 2000 Server. Чтобы выбрать существующий раздел диска, воспользуйтесь стрелками и клавишей <Enter>. Чтобы создать новый раздел диска (обычно это нужно делать при установке системы на новый сервер), нажмите клавишу <C>. С другой стороны, намереваясь удалить существующий раздел (как правило, это делается для удаления всех следов старой операционной системы перед созданием нового раздела для новой инсталляции), нажмите клавишу <D>. В случае создания нового раздела вы должны будете указать его размер. По умолчанию будет предложен максимальный размер раздела. Если вы согласны с этим вариантом, нажмите клавишу <Enter> — в результате новый раздел будет создан. Затем появится экран с перечислением всех разделов, включая тот, который вы только что создали — он обозначается как **New (Unformatted)** (Новый (Неформатированный)). Для продолжения процесса инсталляции выберите этот новый раздел и нажмите клавишу <Enter>.

Выбрав новый раздел, необходимо определиться с форматом диска — это может быть FAT (File Allocation Table — таблица размещения файлов) или NTFS (New Technology File System — файловая система новой технологии). На большинстве серверов применяются только разделы NTFS, так что вам следует выбрать вариант **NTFS**, и для продолжения процесса нажать клавишу <Enter>. После этого программа установки проведет форматирование раздела вместо вас. По завершении процесса форматирования программа установки автоматически скопирует файлы, необходимые для продолжения инсталляции Windows 2000 Server, в новый раздел. Во многих случаях администраторы предпочитают создавать по меньшей мере два раздела: один для операционной системы, другой — для приложений. По завершении копирования файлов происходит автоматическая перезагрузка системы, после чего самостоятельно запускается часть программы инсталляции, оснащенная графическим пользовательским интерфейсом (Graphical User Interface, GUI).

Идентификация устройств

Программа установки на базе GUI помогает вам принимать разнообразные решения, необходимые для выполнения процесса инсталляции, и задает базовую конфигурацию сервера. Во-первых, программа установки пытается обнаружить и настроить все устройства, установленные на компьютере — для завершения этого процесса требуется от пяти до десяти минут (в зависимости от количества установленных на сервере устройств). После установки и настройки аппаратных устройств следует выбрать географическое местоположение системы и нужные настройки клавиатуры. В данном случае значениями по умолчанию являются **English (United States)** и **U.S. Keyboard Layout** (если вы работаете с копией Windows 2000 Server, приобретенной для применения в Соединенных Штатах); чтобы продолжить процесс инсталляции, нажмите кнопку **Next** (Далее).

Лицензирование

Теперь следует ввести ваше имя и название организации, в которой вы работаете. В большинстве компаний принято не привязывать операционную систему к тому или иному сотруднику. Вместо личных данных введите что-нибудь вроде "Отдел продаж", а потом в соответствующем поле обозначьте название вашей компании. Чтобы продолжить, нажмите кнопку **Next** (Далее). Затем вам предложат выбрать способ лицензирования клиентских обращений (Client Access License, CAL). Windows 2000 Server поддерживает схемы лицензирования Per Server (на сервер) и Per Seat (на место). *Лицензирование на сервер* предполагает присвоение лицензий CAL серверу, который впоследствии будет принимать от компьютеров столько соединений, сколько лицензий на нем установлено. *Лицензирование на место* означает, что для каждого из ваших клиентских компьютеров приобретается отдельная лицензия CAL, которая дает им право обращаться к произвольному количеству серверов Windows 2000 (причем серверы не ограничивают это количество). Компания Microsoft рекомендует покупать лицензии Per Server при наличии одного сервера, и Per Seat — при наличии нескольких серверов. Если вы не уверены, какой из этих вариантов лучше, выберите Per Server, поскольку в таком случае у вас появляется возможность однократного бесплатного перехода на лицензирование Per Seat. Установите переключатель в соответствующее вашим предпочтениям положение. В случае выбора лицензирования Per Server укажите количество имеющихся у вас лицензий. Чтобы продолжить, нажмите кнопку **Next** (Далее).

Теперь введите имя сервера, на котором выполняется установка Windows 2000 Server, а также первоначальный административный пароль. Эти данные чрезвычайно важны. Имя компьютера, которое вы укажете, станет именем сервера, т. е. тем самым именем, под которым серверы предстают перед пользователями, когда те перемещаются по сети. Если возможно, выберите имя, которое впоследствии не придется менять. Без административного пароля невозможно выполнять на сервере важнейшие операции — по этой причине следует выбрать надежный пароль, разгадать который будет непросто. Обычно административный пароль состоит из восьми или более символов, среди которых есть и буквы, и цифры. С другой стороны, этот пароль вам придется запомнить. Заполнив указанные поля, нажмите кнопку **Next** (Далее) для продолжения процесса инсталляции.

Факультативные компоненты

Затем вы увидите диалоговое окно, в котором будут перечислены разнообразные компоненты, установка которых в составе Windows 2000 Server не является обязательной. Для целей, которые мы ставим в этой главе, следует выбрать лишь важнейшие варианты, а именно — файловый сервер и сервер печати. Тем не менее ниже перечислены все компоненты, которые вы можете установить (хотя это можно сделать и впоследствии).

- *Службы сертификации.* Службы сертификации необходимы для того, чтобы обеспечить возможность выполнения задач с открытым ключом (например, при настройке защищенного Web-сервера). Эта опция подлежит установке лишь в том случае, если вы знаете, к чему ее необходимо применить.
- *Службы кластеризации.* Службы кластеризации Windows 2000 позволяют двум или нескольким серверам разделять общую рабочую нагрузку и обеспечивать функции файловера на случай аппаратного отказа одного из них. К примеру, при помощи служб кластеризации несколько серверов файлов и печати можно представить сети как один сервер. Устанавливать эту опцию нужно лишь в том случае, если в целях обеспечения высокой работоспособности вы формируете серверный кластер.
- *Информационный сервер Интернета (IIS).* IIS позволяет операционной системе Windows 2000 Server действовать как Web- и FTP-сервер. При выборе этой опции IIS устанавливается совместно с некоторыми вспомогательными функциями. Для работы обычного сервера файлов и печати IIS не требуется.
- *Средства управления и наблюдения.* Эта опция предусматривает установку дополнительных инструментальных средств управления сервером. Утилита Connection Manager позволяет координировать коммутируемые соединения и службы удаленного доступа. Directory Service Migration Tool помогает выполнить переход от службы каталогов NetWare (NetWare Directory Services, NDS) к службе Active Directory, существующей в рамках Windows 2000. Утилиты Network Monitor Tools выполняют элементарные функции анализа и декодирования сетевых пакетов. Простой протокол сетевого управления (Simple Network Management Protocol, SNMP) позволяет Windows 2000 Server отправлять управляющую информацию другому сетевому компьютеру, выполняющему функции управления SNMP. Намереваясь организовать простой сервер файлов и печати, вы можете установить один компонент этого набора — Network Monitor Tools; для этого нажмите кнопку **Details** (Состав), и выберите только его.
- *Службы очереди сообщений.* Эти службы отвечают за формирование очередей из сетевых сообщений, применяемых в некоторых клиент-серверных приложениях. Устанавливать эту опцию нужно лишь в том случае, если она необходима для работы определенного приложения.
- *Отладчик сценариев.* Эта опция предполагает установку инструментальных средств, позволяющих проверять и отлаживать сценарии, написанные на языках VBScript и JScript. Возможно, вам придется подключаться к Интернету с сервера, пользуясь для этого Web-браузером (например, для загрузки обновлений драйверов), или разрабатывать серверные сценарии на VBScript или JScript, поэтому опцию следует установить.

- *Сетевые службы.* Этот вариант выбора подразумевает установку на вашем сервере самых разнообразных сетевых служб. Некоторые из них идеальны для сервера файлов и печати. Имеет смысл установить протокол динамической конфигурации хоста (DHCP). Он позволяет серверу управлять диапазоном IP-адресов, автоматически распределяя их между клиентскими компьютерами. Кроме того, разумно установить службу имен Интернета для Windows (WINS), способную обеспечить разрешение имен и поддержку просмотра сети для клиентских компьютеров, на которых установлены операционные системы Windows с TCP/IP до версии 2000 (например, Windows NT и Windows 9x). Впрочем, если вы намереваетесь организовать простейший сервер файлов и печати, ни первую, ни вторую опцию устанавливать не требуется.
- *Другие службы доступа к файлам и принтерам сети.* Эта опция предполагает установку дополнительного обеспечения, необходимого для организации коллективного доступа к файлам сервера и принтерам с компьютеров Macintosh и машин на базе UNIX. Если на всех клиентских компьютерах в вашей сети установлена одна и та же версия Windows, установки этой опции не требуется.
- *Удаленные службы инсталляции* (Remote Installation Services, RIS). RIS позволяет проводить удаленную установку Windows 2000 Professional на сетевые компьютеры, поддерживающие функцию удаленной загрузки (Remote Boot). Эта функция оказывается удобной, если вы устанавливаете много новых рабочих станций, но не хотите перетаскивать установочный компакт-диск Windows 2000 Professional с одного компьютера на другой. Для размещения образов дисков Windows 2000 Professional на сервере нужно сформировать специальный раздел, но, если вы намереваетесь организовать простой файловый сервер и сервер печати, установка этой опции не требуется.
- *Удаленное хранение.* Эта функция позволяет настроить диск Windows 2000 Server таким образом, чтобы редко используемые файлы автоматически перемещались на свободную магнитную ленту или на перезаписываемый компакт-диск (типа CD-R или CD-RW). Операционная система способна автоматически вызывать эти файлы, как только в них возникает необходимость. Для большинства серверов, на которых свободного места вполне достаточно, эта функция не нужна.
- *Терминальные службы и лицензирование терминальных служб.* Службы Windows Terminal Services работают так же, как и на мэйнфреймах, где все операции выполняются на универсальной машине, а клиенты действуют как терминалы этой машины. Эти две опции позволяют Windows 2000 Server вести многочисленные сеансы Windows для удаленных компьютеров. Приложения исполняются на сервере, а клиентский компьютер отвечает только за вывод информации приложения на дисплей, а также за ввод данных с клавиатуры/мыши. В случае организации сервера файлов и печати необходимость в установке этих опций отсутствует.

Завершающие настройки

Выбрав все необходимые опции и приготовившись к продолжению инсталляции, нажмите кнопку **Next** (Далее). После этого на экране появится приглашение на ввод данных о модеме, подключенном к серверу (если таковой существует). Вы можете ввести свой междугородный код и номер, необходимый для выхода на внешнюю телефонную линию, и указать, какой вид набора поддерживается в вашей телефонной линии: тоновый или импульсный. Заполните обязательные поля и, для продол-

жения, нажмите кнопку **Next** (Далее). Затем нужно будет ввести точную дату и время, а также часовой пояс, в котором расположен сервер. При необходимости обновите эти поля и нажмите кнопку **Next**. Определите настройки своей сети. Есть два варианта настроек: **Typical** (Типовая) и **Custom** (Выборочная). Для небольших сетей обычно подходят типовые настройки. Выборочная настройка позволяют указать детали (например, сетевые компоненты, которые планируется установить, и их предполагаемые настройки).

Домен или рабочая группа

Теперь на экране появляется приглашение на идентификацию системы Windows 2000 Server как участника рабочей группы или домена. Домен представляет собой сложное административное объединение компьютеров в сети Windows 2000, которое предусматривает администрирование сетевых ресурсов из единого центра и обеспечивает возможность организации надежной системы защиты. Домены упрощают задачу администрирования множества серверов Windows 2000 и Windows NT. Для сравнения, рабочая группа представляет собой простую совокупность компьютеров в сети, приспособленную для применения в одноранговых сетях. Существует три режима настройки систем Windows 2000 Server, которые обеспечивают поддержку доменов либо рабочих групп. На контроллере домена (Domain Controller) хранятся данные службы Active Directory, относящиеся к определенному домену; кроме того, контроллер домена отвечает за аутентификацию пользователей и предоставление доступа к ресурсам. Большинство сетей Windows 2000 содержат, по крайней мере, один домен, для сопровождения которого нужен хотя бы один контроллер домена. Серверы-участники домена (Member Servers) являются частью домена, но не содержат копии данных службы Active Directory. Рядовые (Stand-Alone) серверы не принимают участия в организации домена, но зато входят в рабочую группу.

Имейте в виду, что интегрировать в домен новый сервер можно лишь в том случае, если уже существует как сам домен, так и контроллер домена, способный утвердить новый сервер в роли участника домена. Для вновь создаваемого сервера (даже если он будет контроллером домена) выберите рабочую группу и нажмите кнопку **Next** (Далее) для продолжения. После этого программа установки, пользуясь предоставленной вами информацией, завершит свою часть процесса инсталляции Windows 2000 Server.

Настройка сервера

После инсталляции Windows 2000 система перезагрузится, и вы должны будете настроить сервер. При появлении строки регистрации Windows 2000 Server введите комбинацию клавиш <Ctrl>+<Alt>+<Delete>, и зарегистрируйтесь на сервере — вам необходимо зарегистрироваться в роли администратора, пользуясь паролем, введенным в ходе установки. После регистрации появится рабочий стол Windows 2000 Server, а также мастер настройки Windows 2000 Configuration Wizard (рис. 24.1), который поможет вам пройти оставшиеся этапы, необходимые для приведения сервера в рабочее состояние. В случае настройки единственного сервера для небольшой сети вы можете установить переключатель (показанный на рис. 24.1) в положение **This is the only server in my network** (Это единственный сервер в моей сети). Для более сложных вариантов инсталляции Windows 2000 установите переключатель в положение **One or more servers are already running in my network** (Один или более серверов

уже работают в моей сети), хотя в этом случае от вас потребуются более глубокие познания в области настроек. После этого появится экран подтверждения, на котором вы должны согласиться с настройкой на сервере служб наподобие Active Directory, DHCP и DNS (это стандартный набор при наличии в сети единственного сервера). Чтобы продолжить, нажмите кнопку **Next** (Далее); при желании можно получить дополнительные сведения об этих службах, перейдя по ссылкам, приведенным в Server Configuration Wizard.

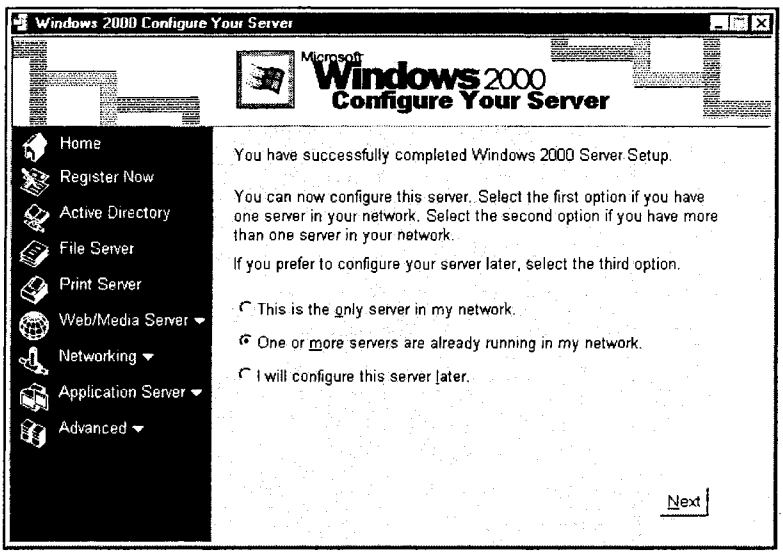


Рис. 24.1. После установки Windows 2000 мастер Configuration Wizard проведет вас через оставшиеся действия по настройке сервера

Теперь вы должны ввести имя домена, который предполагаете создать. Имейте в виду, что имя домена не может содержать пробелы и должно быть простым — зачастую в качестве имени домена употребляется название компании или его сокращение. Кроме того, вы должны ввести все доменные имена Интернета, выделенные для вашей сети. Доменное имя Интернета приобретается и управляется самой компанией. К примеру, если вы работаете в компании под названием Widget Corporation, то домен Windows 2000 разумно назвать widget, а доменным именем Интернета, принадлежащим вашей компанией, может быть **widget.com**. Если никакого доменного имени Интернета у компании нет, сделайте в соответствующем поле запись **local**. К примеру, если имя домена Windows 2000 — **administration.dls**, то доменным именем Интернета будет **administration.dls.com**. Введите нужные данные и нажмите кнопку **Next** (Далее) для продолжения.

После некоторой паузы вы увидите, что выбранные вами настройки установлены, а затем произойдет перезагрузка системы. Для продолжения нажмите кнопку **Next** еще раз (возможно, в ходе этого процесса вам понадобится поместить в привод CD-ROM компакт-диск Windows 2000 Server). После установки всех необходимых компонентов и перезагрузки системы вы должны будете выполнить некоторые завершающие действия при помощи мастера Server Configuration Wizard.

1. Щелкните на пиктограмме **My Network Places** (Мое сетевое окружение) правой кнопкой мыши и выберите **Properties** (Свойства).
2. Выберите **Local Area Connection** (Подключение по локальной сети) правой кнопкой мыши и щелкните на пункте **Properties** (Свойства). В результате откроется диалоговое окно **Local Area Connection Properties** (Подключение по локальной сети — свойства) (рис. 24.2).

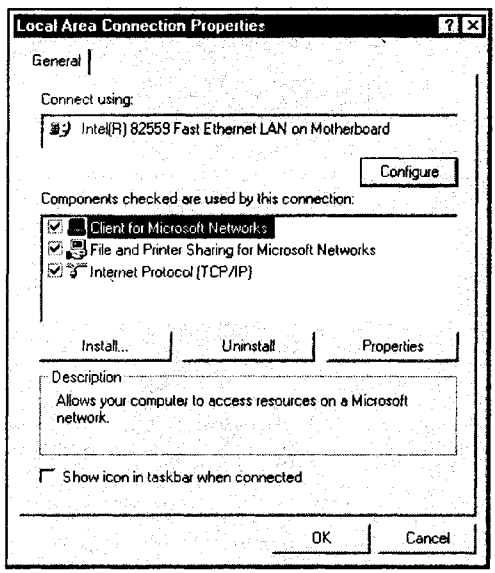


Рис. 24.2. Диалоговое окно **Local Area Connection Properties** позволяет настроить сетевые взаимодействия сервера

3. Выделите запись **Internet Protocol (TCP/IP)** (Протокол Интернета) и нажмите кнопку **Properties** (Свойства).
4. Находясь на вкладке **General** (Общие), установите переключатель в положение **Use the following IP address** (Использовать следующий IP-адрес), и введите IP-номер данного сервера, который будет использоваться в качестве его IP-адреса. Если диапазон номеров еще не существует (и ваша сеть не подключена к сети Интернет напрямую), укажите IP-адрес 192.168.1.1.
5. Введите надлежащую маску подсети. Если раньше маски подсети в вашей сети не использовались, укажите 255.255.255.0.
6. В поле **Preferred DNS Server** (Предпочитаемый DNS-сервер) повторно введите IP-адрес, назначенный серверу (т. е., например, 192.168.1.1). Чтобы закрыть многочисленные диалоговые окна **Properties** (Свойства), нажмите кнопку **OK**.
7. Теперь выполните авторизацию служб DHCP. Выберите последовательно команды **Start, Programs, Administrative Tools, DHCP** (Пуск, Программы, Администрирование). В результате на экране должна появиться оснастка диспетчера DHCP Manager (рис. 24.3).

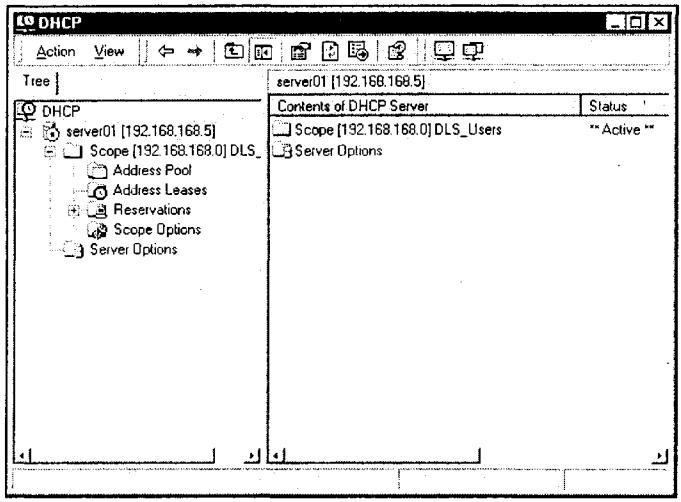


Рис. 24.3. Для того чтобы разрешить серверу выполнение клиентских DHCP-запросов, воспользуйтесь DHCP Manager

8. Разверните дерево, расположенное на левой панели, а затем щелкните на записи нового сервера правой кнопкой мыши. Выберите команды **All Tasks, Authorize** (Все задачи, Авторизовать). Это позволит выполнять запросы DHCP и распределять IP-адреса между клиентскими компьютерами сети.
9. Чтобы внесенные изменения вступили в силу, выключите и перезагрузите сервер. На этом процесс базовой инсталляции и настройки сервера Windows 2000 завершается.

Настройка клиента

После установки Windows 2000 Server и приведения сервера в рабочее состояние имеет смысл провести самое элементарное тестирование, чтобы убедиться в том, что этот сервер доступен для всех клиентских систем, расположенных в данной сети. Таким образом, вам нужно будет создать на сервере пользовательскую учетную запись, совместно используемый ресурс, к которому будет обращаться клиентский компьютер, настроить последний на подключение к серверу, а затем войти на сервер с клиентского компьютера и удостовериться в доступности общего ресурса. Опытные администраторы могут пропустить этот этап, но для остальных он, надо полагать, окажется хорошим упражнением по работе с учетными записями и совместно используемыми ресурсами.

Создание тестовой учетной записи

Хотя и можно зарегистрироваться на сервере в роли администратора, для целей тестирования лучше создать обычную пользовательскую учетную запись.

1. Выберите последовательно команды **Start, Programs, Administrative Tools, Active Directory Users and Computers** (Пуск, Программы, Администрирование, Active Directory — пользователи и компьютеры). В результате откроется консоль управ-

ления Windows с настройками пользователей и компьютеров Active Directory (рис. 24.4).

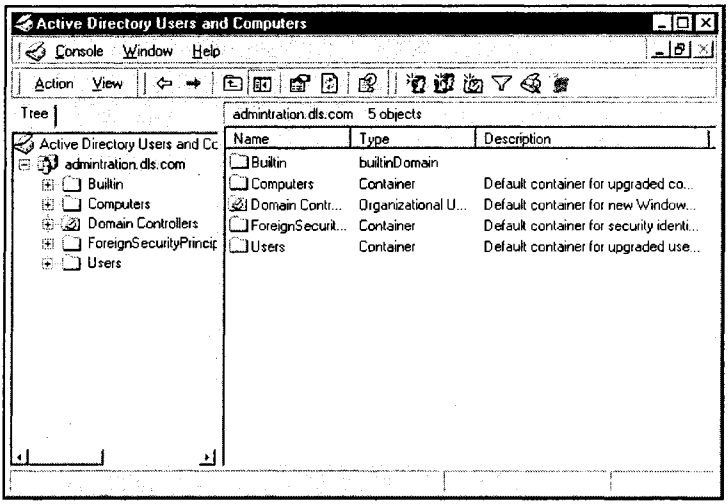


Рис. 24.4. Для управления пользователями и группами сервера используйте Active Directory

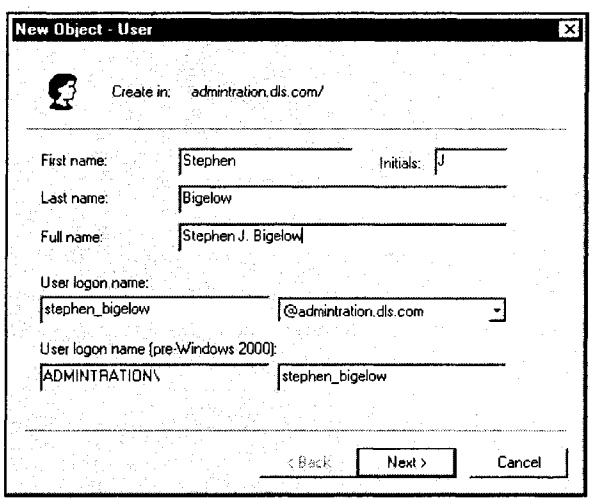


Рис. 24.5. Создание временной пользовательской учетной записи с целью проверки соединения с новым сервером

2. Щелкните на записи сервера (например, **administration.dls.com**) в левой панели правой кнопкой мыши и выберите команды **New, User** (Новый, Пользователь). В результате появится диалоговое окно **Create New Object — User** (Новый объект — Пользователь) (рис. 24.5). Введите имя и фамилию владельца новой, тестовой пользовательской учетной записи. Оставшиеся поля генерируются авто-

матически, исходя из конфигурации сервера, хотя при желании вы можете изменить их содержание. На рис. 24.5 показано, что пользователь stephen_bigelow сможет регистрироваться в Active Directory при помощи учетной записи **stephen_bigelow@administration.dls.com**. Чтобы продолжить, нажмите кнопку **Next** (Далее).

3. Теперь введите пароль для созданной учетной записи (если тестирование будет непродолжительным, допускается использование пароля password). Нажмите кнопку **Next** (Далее), чтобы продолжить, а затем **Finish** (Готово) — чтобы завершить создание новой пользовательской учетной записи.

Создание совместно используемого ресурса

Теперь у вас есть действительная пользовательская учетная запись, но на сервере должен существовать некий объект, к которому ее владелец сможет обращаться. В Windows 2000 Server коллективный доступ к каталогам организуется при помощи механизма под названием *доступ* (share). Совместно используемый ресурс — это видимый в сети ресурс, к которому могут обращаться удаленные пользователи (в случае, если у них есть достаточные полномочия). Давайте создадим на сервере каталог, к которому пользователи смогут обращаться через сеть. В первую очередь нужно создать обычный каталог, поместив его на один из дисководов сервера. Затем щелкните на этом каталоге правой кнопкой мыши и выберите пункт меню **Sharing** (Доступ). В результате на экране появится вкладка **Sharing** (Доступ) диалогового окна свойств этого каталога (рис. 24.6). Установите переключатель в положение **Share this folder** (Открыть общий доступ к этой папке), и взгляните на имя нового совместно используемого ресурса. Это имя, исходя из имени каталога, задается

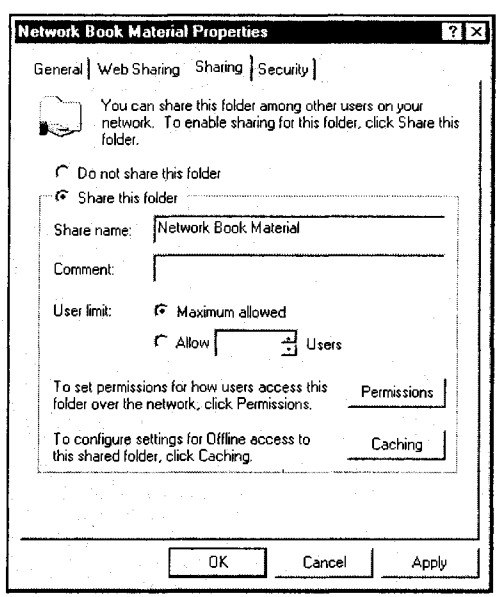


Рис. 24.6. С помощью вкладки **Sharing** из созданного на сервере объекта формируется совместно используемый ресурс

автоматически, но при желании его можно изменить. Чтобы разрешить коллективный доступ к каталогу, нажмите кнопку **OK**.

Настройка клиента

Выберите один из сетевых компьютеров на базе Windows и настройте его на взаимодействие с новым сервером. Если выбранный компьютер уже работает в сети, вполне возможно, что многие из нижеприведенных этапов уже выполнены, однако проверка каждой настройки и указание имени домена нового сервера, вероятно, окажется хорошим упражнением. Чтобы настроить клиентскую машину, выполните следующие действия[1].

1. Выберите **Control Panel** (Панель управления) и щелкните на пиктограмме **Network** (Сеть).
2. Нажмите кнопку **Add** (Добавить), затем в диалоговом окне **Select Network Component Type** (Выбор типа сетевого компонента) выберите **Client** (Клиент), и вновь нажмите **Add** (Добавить).
3. В списке производителей (**Manufacturers**) выберите **Microsoft**, а затем в области **Network Clients** (Сетевые клиенты) выберите **Microsoft Networks**. Чтобы продолжить, нажмите кнопку **OK**.
4. В диалоговом окне **Network** (Сеть) как установленные будут обозначены протоколы **TCP/IP** и **Client for Microsoft Networks** (Клиент для сетей Microsoft) (рис. 24.7).

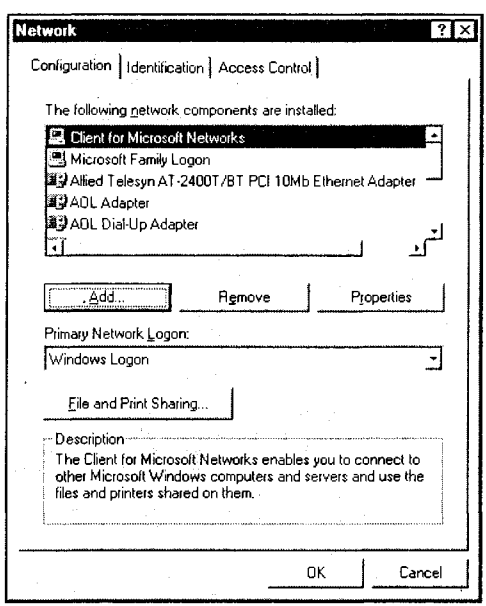


Рис. 24.7. Обязательно настройте клиентский компьютер на полноценный обмен информацией в сети

[1] Здесь рассматривается клиентская ОС Windows 98. — *Ред.*

5. Выделите строку **Client for Microsoft Networks** (Клиент для сетей Microsoft) и нажмите кнопку **Properties** (Свойства).
6. В диалоговом окне **Client for Microsoft Networks Properties** (Клиент для сетей Microsoft: свойства) установите флажок **Log onto Windows NT domain** (Зарегистрироваться на сервере Windows NT) и введите имя нужного домена. В нашем примере именем домена является admintration. Чтобы закрыть диалоговое окно, нажмите кнопку **OK**.
7. Возможно (если необходимые файлы отсутствуют на жестком диске), вам предложат поместить в привод CD-ROM компакт-диск Windows; после этого необходимо перезагрузить клиентский компьютер.

Тестирование соединения

Выполнив все настройки, вы можете зарегистрироваться в домене, управляемом новой системой Windows 2000 Server, и обратиться к файлам, расположенным в совместно используемом каталоге. Когда клиентский компьютер перезагрузится, для регистрации в нужном домене нужно будет задействовать тестовую пользовательскую учетную запись (например, stephen_bigelow), имя домена (admintration) и выбранный пароль (к примеру, password). Если все данные будут введены правильно, произойдет регистрация в домене. В случае возникновения каких-либо затруднений — например, непризнания имени пользователя, пароля или имени домена — вы узнаете о произошедшей ошибке и сможете ее исправить.

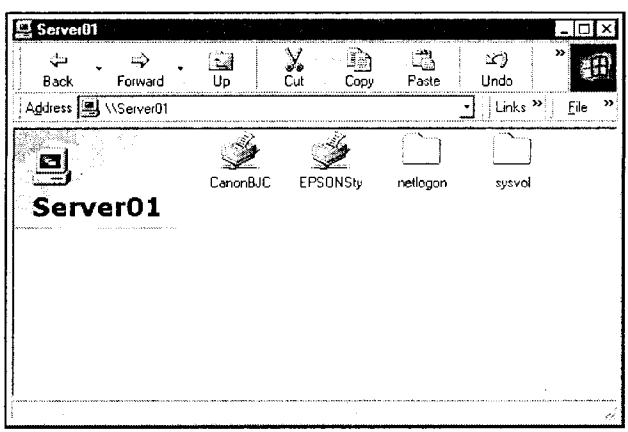


Рис. 24.8. Зарегистрировавшись на сервере, зайдите в Network Neighborhood, чтобы просмотреть все расположенные на нем общие ресурсы

Откройте **Network Neighborhood** (Сетевое окружение) — пиктограмму, расположенную на рабочем столе клиентского компьютера. В списке должен фигурировать новый сервер. В результате перехода на сервер вы увидите перечень всех доступных общих ресурсов. Помимо прочего, вы обнаружите ресурсы netlogon и sysvol, а также созданный вами каталог, для которого установлены права совместного доступа (рис. 24.8). У вас должна быть возможность открытия тестового каталога и просмотра расположенных в нем файлов — их вы можете беспрепятственно удалять, пере-

именовывать, открывать, выполнять в их отношении другие действия (так, как будто вы работаете с файлами, расположенными на локальном жестком диске).

Основы администрирования

Теперь, когда вы успешно установили, настроили и протестировали Windows 2000 Server на новой серверной платформе, самое время сосредоточиться на более сложных задачах, связанных с администрированием сервера. Качественное администрирование помогает обеспечить продуктивность и защиту ваших серверов, так что в круг ваших обязанностей входит разработка и ввод в действие политик безопасности, подходящих для существующей сетевой среды. К примеру, принуждение к частой замене 20-символьных паролей в сущности лишь гарантирует, что пользователи будут их где-то записывать, таким образом, разумеется, подрывая те жесткие меры безопасности, которые вы пытаетесь внедрить. Кроме того, чрезвычайные меры безопасности приводят к тому, что пользователи испытывают трудности при регистрации в сети, а значит, им требуется дополнительная помощь со стороны администратора. В этой части главы рассматриваются основные обязанности администратора — такие как добавление новых пользователей, удаление старых, предоставление пользователям полномочий и т. д.

Пользовательские учетные записи

С тем чтобы получить доступ к серверу Windows 2000, каждый пользователь сети (в том числе администратор) должен иметь учетную запись на данном сервере или в домене (совокупности защитной информации, которой совместно пользуются серверы Windows 2000). Пользовательская учетная запись содержит данные об имени пользователя (том имени, под которым этот пользователь известен системе) и его пароле, а также некоторое количество другой информации, специфичной для каждого отдельного пользователя. Операционная система Windows 2000 Server позволяет создавать, сопровождать и удалять пользовательские учетные записи, затрачивая на это минимум усилий.

Что такое идентификаторы безопасности (SID)

Каждой пользовательской учетной записи, созданной в домене Windows 2000 Server, присваивается специальный номер, называемый идентификатором безопасности (Security ID, SID), причем сервер судит о пользователе именно по его идентификатору. SID состоит из уникального числа, которое назначается домену, и еще одного числа, состоящего в последовательном ряду и присваиваемого каждой новой учетной записи. SID абсолютно уникальны: не существует двух пользователей, у которых были бы одинаковые идентификаторы безопасности, пусть даже у них одинаковые имена и пароли. Если у вас был пользователь "bill", потом вы удалили его учетную запись, а еще позже создали новую учетную запись с тем же именем, у них будут разные идентификаторы защиты — таким образом, ни одна пользовательская учетная запись не может невзначай получить полномочия, первоначально присвоенные другому пользователю с аналогичным именем.

Новые пользовательские учетные записи

Для управления пользовательскими учетными записями существует консоль управления Active Directory Users and Computers (Active Directory — пользователи и компьютеры), открыть которую можно, выбрав последовательно команды **Start, Programs, Administrative Tools** (Пуск, Программы, Администрирование). После запуска этой консоли (см. рис. 24.4) разверните дерево домена, который вы администрируете, и щелкните на каталоге **Users** (Пользователи) в левой панели. На правой панели появится перечень существующих пользователей. Чтобы добавить нового пользователя, щелкните на каталоге **Users** правой кнопкой мыши, выберите пункт меню **New, User**. В результате появится диалоговое окно **New Object — User** (Новый объект — Пользователь) (см. рис. 24.5). Введите данные в поля **First name** (имя), **Last name** (фамилия) и **User logon name** (регистрационное имя пользователя); при необходимости вы также можете внести изменения в другие поля. Чтобы создать профиль пароля нового пользователя, нажмите кнопку **Next** (Далее) (рис. 24.9). Введите пароль, который будет применяться в новой учетной записи, подтвердите его, и пометьте любые подходящие флажки, назначение которых приводится ниже.

- **User must change password at next logon** (Потребовать смену пароля при следующем входе в систему). Установив этот флажок, вы вынуждаете пользователя выбрать собственный пароль при последующей регистрации в системе.

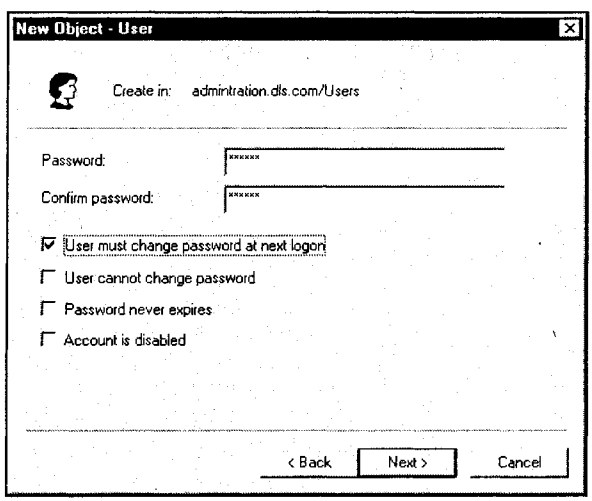


Рис. 24.9. При создании новой пользовательской учетной записи обязательно задайте подходящий пароль

- **User cannot change password** (Пользователь не может изменить пароль). Этот вариант иногда применяется в отношении учетных записей, пароли которых меняются без участия администратора (например, в сетях с более высокой степенью защиты). Впрочем, обычно этот флажок снят.
- **Password never expires** (Срок действия пароля не истекает). Эта опция предусматривает сохранение действительности пароля в течение любого периода времени, на протяжении которого владелец учетной записи желает им пользоваться. Такой

вариант обычно считается неудачным с точки зрения безопасности, так что этот флажок, как правило, снят.

- **Account is disabled** (Учетная запись отключена). Этот флажок в помеченном состоянии приводит к тому, что новая учетная запись блокируется, хотя ее действие можно возобновить при первой же необходимости. Такой вариант удобен, если вы создаете новую учетную запись, но оказывается, что новый пользователь еще не готов к работе в сети.

После ввода пароля и выбора нужных опций нажмите кнопку **Next** (Далее). Появится экран подтверждения, так что для создания учетной записи нужно будет еще раз нажать кнопку **Next** (при необходимости внесения любых изменений в параметры учетной записи нажмите кнопку **Back** (Назад).

Схемы именования

В большинстве небольших организаций регистрационные имена пользователей обычно содержат имена или фамилии владельцев учетных записей. Впрочем, в организации любого размера может быть несколько схожих имен, и поэтому, чтобы избежать необходимости реорганизации схемы именования при возникновении проблем, сразу выберите оптимальный принцип присвоения имен и сделайте так, чтобы им пользовались другие администраторы. При именовании учетных записей необходимо придерживаться непротиворечивой процедуры, которая должна предусматривать возможность расширения пользовательской базы, ограничивать возможность возникновения конфликтов имен, а также обеспечивать безопасность имен учетных записей, максимально усложняя задачу их злонамеренного использования. Ниже приведены некоторые рекомендации, которые могут помочь вам в устранении проблем именования.

- *Имя пользователя и первая буква его фамилии.* Чтобы создать регистрационное имя, возьмите имя владельца учетной записи и соедините его с первой буквой его фамилии. Для имени Stephen Bigelow результатом применения этой схемы будет имя пользователя stephenb или steveb; впрочем, в крупных организациях такая схема непрактична.
- *Первая буква имени пользователя и его фамилия.* Чтобы создать регистрационное имя, возьмите первую букву имени владельца учетной записи и соедините его с его фамилией. Для имени Stephen Bigelow в результате получится sbigelow. В масштабах крупной организации такая схема неосуществима.
- *Первые буквы имени и отчества пользователя плюс его фамилия.* Чтобы создать регистрационное имя, возьмите первые буквы имени и отчества владельца учетной записи, и соедините их с его фамилией. Для имени Stephen J. Bigelow в результате применения этой схемы получится имя пользователя sjbigelow.
- *Первые буквы имени и отчества пользователя плюс первые пять символов его фамилии.* Чтобы создать регистрационное имя, возьмите первые буквы имени и отчества владельца учетной записи и соедините их с первыми пятью символами из его фамилии. Для имени Stephen J. Bigelow получится sjbigel.
- *Имя и фамилия пользователя.* Между именем и фамилией владельца учетной записи ставится символ подчеркивания (_), точки (.) или тире (-). Для имени Stephen Bigelow могут получиться варианты stephen_bigelow, stephen.bigelow или stephen-bigelow.

Безопасные пароли

Пароли представляют собой чувствительные к регистру строки, длина которых в службе каталогов Active Directory может составлять до 104 символов (в Windows NT Security Manager — до 14 символов). Правомерно употребление в рамках паролей букв, чисел и символов. Когда вы определяете для учетной записи пароль, Windows 2000 сохраняет его в зашифрованном виде в базе данных учетных записей. Но просто завести пароль еще недостаточно — основным методом предотвращения несанкционированного доступа к сетевым ресурсам является применение безопасных паролей. Различие между обычным и безопасным паролями заключается в том, что безопасный пароль труднее угадать и взломать. Трудность взлома пароля обуславливается применением сочетаний всех возможных типов символов (включая буквы в нижнем и верхнем регистрах, числа и символы). К примеру, вместо crazydays можно задействовать пароль crAZy2Days&, Cr**y!dayS или даже c*AZY%d*ys.

Изменение пользовательских учетных записей

Создание новой учетной записи — это сравнительно быстрая и простая процедура, в ходе выполнения которой трудности могут возникнуть лишь с несколькими опциями. Однако существует множество других параметров, предназначенных для документирования пользовательских данных и задания разнообразных вариантов безопасности, а это значит, что вам придется обновлять учетные записи. Чтобы обновить существующую пользовательскую учетную запись, откройте в консоли управления список пользователей, щелкните правой кнопкой мыши на записи пользователя, данные которого нужно обновить, и выберите пункт меню **Properties** (Свойства). В результате откроется диалоговое окно личных свойств пользователя (рис. 24.10).

Вкладки **General** (Общая) и **Address** (Адрес) позволяют ввести дополнительную информацию о пользователе (например, вариант обращения к нему, его почтовый адрес, номер телефона, почтовую учетную запись и т. д.). Служба Active Directory интегрируется с новыми версиями Exchange Server, так что эта информация может представлять большое значение для вашей сети. При помощи вкладки **Account** (Учетная запись) (рис. 24.11) вы можете задать некоторые важные параметры пользовательской учетной записи. Именно здесь производятся изменения регистрационного имени пользователя, домена сервера, а также регистрационного имени пользователя для систем старше Windows 2000 — оно применяется для регистрации в домене с компьютера Windows NT или при помощи приложения, которое не поддерживает регистрацию Active Directory.

По умолчанию пользователям разрешается регистрироваться в сети в любое время суток и в любой день недели, и для небольших сетей эта политика обычно подходит. Тем не менее с помощью кнопки **Logon Hours** (Время входа) вы можете ограничить дни и периоды времени, в течение которых пользователи смогут регистрироваться в сети. Ограничение дней/периодов времени регистрации имеет большее значение в крупных сетях, где предпринимаются дополнительные меры по обеспечению безопасности. При задании подобных ограничений обязательно оставляйте в качестве резерва дополнительное время перед началом и после окончания рабочего дня. По умолчанию пользователи могут регистрироваться на всех рабочих станциях в рамках домена, а их аутентификацию проводит сам домен. В некоторых

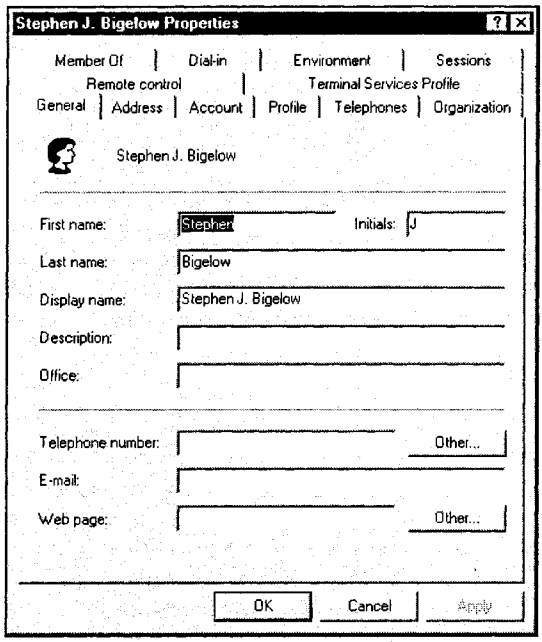


Рис. 24.10. С помощью диалогового окна личных свойств пользователя можно управлять всеми параметрами его учетной записи

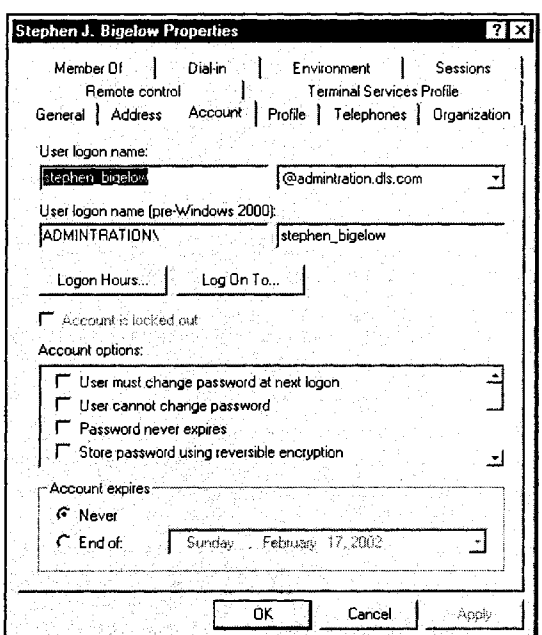


Рис. 24.11. Вкладка учетной записи

случаях, для ужесточения системы безопасности, необходимо ограничить круг компьютеров, на которых можно регистрироваться с данной учетной записью. Чтобы ограничить пункты регистрации пользователя, нажмите кнопку **Logon To**.

Примечание

Функция Logon To работает лишь в том случае, если применяются протоколы NetBIOS или NetBEUI — в сетях, функционирующих исключительно на основе TCP/IP, эта возможность отсутствует.

Область **Account options** (Параметры учетной записи) вкладки **Account** (Учетная запись) позволяет устанавливать дополнительные опции учетных записей, пользуясь соответствующими флажками. Наиболее важны две дополнительные опции: **Account is disabled** (Учетная запись отключена) и **Account is trusted for delegation** (Учетной записи доверены полномочия путем делегирования). Когда учетная запись отключена, владелец не может ею пользоваться, но ее настройки сохраняются в Active Directory. Возможно, вам понадобится запретить доступ к сети временно (например, на время отпуска пользователя), но затем возобновить доступ, не прибегая к удалению учетной записи. Если по отношению к учетной записи выполнено делегирование, вы можете поручить ее владельцу администрирование какой-то части домена (Windows 2000 Server позволяет предоставлять административные полномочия на части дерева Active Directory, не отдавая такие полномочия на весь домен). Последняя опция вкладки **Account**, о которой нужно знать, — это **Account expires** (Срок действия учетной записи). По умолчанию срок действия учетной записи бесконечен (установлен в положение **Never**). Тем не менее вы можете указать срок действия, по истечении которого учетная запись будет автоматически отключена (но не удалена). Эта функция оказывается особенно удобной при необходимости настроить временную пользовательскую учетную запись (например, для временного сотрудника).

Удаление учетных записей

Когда пользователи переходят из отдела в отдел или увольняются из компании, их учетные записи нужно удалять. Эти действия помогают вести "сетевое хозяйство" и обеспечивают безопасность, устраняя возможность несанкционированного (и потенциально опасного) доступа в сеть бывших сотрудников. Чтобы удалить пользовательскую учетную запись, откройте каталог **Users** консоли управления, щелкните на записи пользователя правой кнопкой мыши и выберите пункт меню **Delete** (Удалить). Чтобы удалить несколько учетных записей, выделите их все, щелкните на выделении правой кнопкой мыши и выберите **Delete**.

Примечание

Чем удалять учетную запись, лучше отключите ее — для этого щелкните на записи пользователя(ей) правой кнопкой мыши и выберите пункт меню **Disable Account**.

Группы пользователей

Пользовательские учетные записи обеспечивают абсолютный контроль над действиями участников сети, но координирование одних пользователей быстро превращается в кошмар администратора. К примеру, предположим, что сотрудники отдела

продаж вашей компании имеют доступ к 30 каталогам на сервере. Если бы вы управляли отдельными учетными записями, вам пришлось бы искать все эти 30 каталогов при каждом появлении в отделе нового сотрудника — только так можно было бы узнать, какие полномочия ему нужны. Другой пример: в случае перехода пользователя из одного отдела в другой ему требуется доступ к другому набору каталогов, и вам приходится выяснять все необходимые для него полномочия — для занятого администратора такой объем работы оказывается чрезмерным.

Чтобы упростить рутинную процедуру присвоения сетевых полномочий, сетевые операционные системы допускают создание групп (иногда они называются группами безопасности). Идея заключается в том, чтобы создать группу, назначить ей все необходимые полномочия, а затем подключить к этой группе пользователей. Присваивая полномочия доступа к каталогу на сервере, вы распространяете их на группу, в результате чего все участвующие в этой группе пользователи автоматически наследуют эти полномочия. Групповая схема значительно упрощает нудную деятельность, связанную с координацией сетевых полномочий. Таким образом, права доступа к 20 каталогам, связанным с продажами, можно назначить всей группе отдела продаж (Sales). Создавая учетную запись для нового сотрудника этого отдела, вы просто добавляете его в группу Sales, тем самым автоматически предоставляя ему доступ ко всем необходимым каталогам. Если впоследствии этот сотрудник перейдет в отдел технического обслуживания, вы сможете переопределить его в группу Service, изменив таким образом все необходимые полномочия.

Помимо прочего, при групповом распределении возможно построение иерархии групп, т. е. одни группы могут быть участниками других групп. К примеру, предположим, что в вашей сети существует группа Sales и более широкая группа Administration (участники которой имеют права доступа к другим каталогам). В таком случае можно сначала создать группу Sales, затем — группу Administration, а после этого сделать первую участником второй. Этот подход предполагает логическое распределение ресурсов. Если ресурс имеет отношение к единственному отделу, его следует отнести к группе сотрудников этого отдела. Если ресурс предназначен для группы, занимающей более высокую иерархическую позицию, его нужно назначить именно ей, в результате чего все группы отделов, расположенные ниже по иерархии, унаследуют права доступа к этому ресурсу. Если ресурс должен быть доступным для всех (например, каталог с принципами кадровой политики или справочник по льготам), его нужно отнести к головной группе, находящейся на высшем уровне.

Создание группы

Создание и координация групп производится при помощи консоли управления **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры); для того чтобы открыть ее, выберите последовательно команды **Start, Programs, Administrative Tools** (Пуск, Программы, Администрирование). После запуска консоли (см. рис. 24.4) откройте дерево управляемого вами домена (например, **administration.dls.com**). Группы расположены в каталогах **Built-in** (Встроенные) и **Users** (Пользователи). Встроенные группы являются фиксированными, их нельзя удалить и сделать участниками других групп. Встроенные группы обладают некоторыми предопределенными важными полномочиями; в них могут участвовать все прочие группы, которые вы будете создавать. Чтобы отключить одну из встроенных

групп, нужно просто удалить все группы, которые в ней участвуют. В большинстве случаев вы будете иметь дело с группами, приведенными в каталоге **Users**. Отличить пользовательскую группу от пользовательской учетной записи можно по пиктограмме "с двумя лицами" и обозначению типа (Type). Чтобы создать новую группу, щелкните на каталоге **Users** правой кнопкой мыши, и выберите пункт меню **New Group** (Новая группа). В результате появится новое диалоговое окно **New Object — Group** (Новый объект — группа) (рис. 24.12).

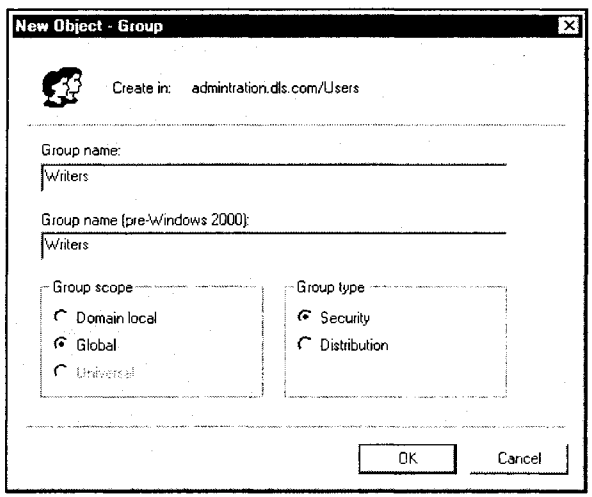


Рис. 24.12. Создание новых групп для систематизации пользователей и предоставления им доступа к ресурсам

Введите имя новой группы в поле **Group name** (Имя группы). Указанное имя будет повторено в поле **Group name (pre-Windows 2000)**. Оно позволяет установить другое имя группы в расчете на компьютеры Windows NT (по возможности их нужно избегать). Установите все необходимые опции, расположенные в нижней части диалогового окна. Область **Group scope** (Область действия группы) обозначает, насколько широко (в рамках домена) используется данная группа. Универсальная (**Universal**) группа распространяется на всю организацию — даже когда в сети существует множество отдельных доменов. Помимо прочего, в универсальные группы могут входить участники, относящиеся к любому домену сети организации. Глобальная (**Global**) группа может содержать исключительно участников, относящихся к тому домену, в котором она существует, однако глобальным группам можно присваивать права, связанные с любым доменом в сети (и даже с несколькими доменами). Локальная группа домена (**Domain local**) существует в рамках отдельного домена и может включать только относящихся к нему участников.

Наконец, необходимо сделать выбор между группой безопасности (**Security**) и группой распространения (**Distribution**). У групп распространения только одно назначение — составление списков получателей почтовых рассылок. Группы распространения задействуются в почтовых программах (подобных Microsoft Exchange) с целью отправки электронной почты ее участникам. Как и в случае с группой безопасности,

в группу распространения можно добавлять контактные данные получателя — для того чтобы он получал электронные почтовые сообщения, отсылаемые группе в целом. Группы распределения не играют никакой роли в плане обеспечения безопасности (в них не определяются полномочия) и не используются для фильтрации настроек групповой политики (Group Policy). Для сравнения, группы безопасности являются неотъемлемым компонентом взаимодействия пользователей и системы безопасности. Группы безопасности выполняют функции координации доступа пользователей и компьютеров к коллективным ресурсам и фильтрации настроек групповой политики. Пользователи, компьютеры и другие группы собираются в группу безопасности, а затем ей присваиваются оптимальные полномочия по отношению к определенным ресурсам (таким как совместно используемые файлы и принтеры). Этот принцип упрощает задачу администрирования, позволяя вам единожды назначать полномочия группе, вместо того чтобы делать это многократно для каждого отдельного пользователя. При добавлении нового пользователя к существующей группе он автоматически получает все права и полномочия, характерные для группы.

Небольшие организации

Некоторые небольшие организации предпочитают формировать группы безопасности с универсальной областью действия, которые отвечают всем потребностям их пользователей. В организациях, планирующих расширение, разумно проводить преобразование изначально сформированных универсальных групп в глобальную/локальную модель, рекомендованную для применения в организациях среднего и крупного масштаба. С другой стороны, некоторые небольшие, но расширяющиеся организации, вероятно, сочтут разумным с самого начала реализовать глобальную/локальную модель. Так как группы с универсальной областью действия (а также их участники) заносятся в базу данных глобального каталога, наличие большого количества универсальных групп — особенно тех, участие в которых часто подвергается изменениям — приводит к появлению значительного репликационного трафика. В такой ситуации имеет смысл следовать рекомендациям для средних и крупных организаций.

Средние и крупные организации

В средних и крупных организациях применяются глобальные группы Account и локальные группы Resource — они позволяют достичь гибкости, масштабируемости и легкости администрирования групп безопасности. Сделайте пользователей участниками групп безопасности с глобальной областью действия. Как правило, глобальную группу можно представить как группу Accounts (т. е. группу, содержащую пользовательские учетные записи). С другой стороны, ресурсы следует поместить в локальные группы безопасности домена (или машины). Локальную группу обычно можно приравнять к группе Resource (группе, в которой назначаются полномочия, связанные с обращением к ресурсу). Кроме того, глобальную группу можно поместить в любую локальную группу домена (или машины) в рамках леса (этот вариант оказывается особенно эффективным в случаях, когда задействовано несколько доменов) или назначить полномочия на обращение к ресурсам локальных групп домена (или машины), в которых они содержатся.

Назначение участников групп

Новые группы не содержат участников, так что пользователей к ним нужно приписывать. Расположите новую группу в каталоге **Users**, щелкните на ней правой кнопкой мыши, и выберите **Properties**. Чтобы вывести список текущих участников (этот список, как показано на рис. 24.13, будет пуст), перейдите на вкладку **Members** (Члены группы). Теперь нажмите кнопку **Add** (Добавить) — в результате откроется диалоговое окно **Select Users, Contacts, or Computers** (Выбор: Пользователи, Контакты и Компьютеры). Прокрутите выведенный список, выберите всех пользователей, которых вы хотите прикрепить к новой группе, и нажмите кнопку **Add**. Если вы хотите, чтобы новая группа стала участником другой группы, перейдите на вкладку **Member Of**, и воспользуйтесь расположенной в ней кнопкой **Add** (как и при добавлении пользователей в группу). Закончив с добавлением участников, нажмите кнопку **OK**. После этого нажатие кнопки **OK** приведет к закрытию диалогового окна **Select Users, Contacts, or Computers**. Теперь новая группа должна быть заполнена.

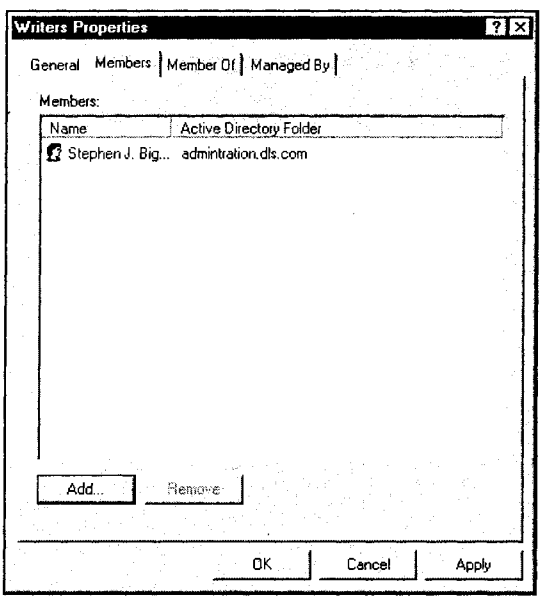


Рис. 24.13. Наполнение группы путем добавления в нее участников (и даже других групп)

Управление дисками и каталогами

Диски и каталоги в системе Windows 2000 Server становятся доступными для сетевых пользователей, когда их превращают в совместно используемые ресурсы (shared resources, или shares). Принцип заключается в следующем: нужно выбрать диск или каталог, разрешить к нему коллективный доступ, а затем установить полномочия доступа. Впрочем, важно понимать, как именно создаются совместно используемые ресурсы, и иметь представление о том, как Windows 2000 Server обеспечивает безопасность таких ресурсов, а также каталогов и файлов на дисках NTFS.

Создание совместно используемых ресурсов

Чтобы создать новый совместно используемый ресурс, нужно открыть на сервере каталог My Computer или программу Windows Explorer. Щелкните на каталоге, который предполагаете сделать совместно используемым, правой кнопкой мыши и выберите пункт меню **Sharing** (Доступ). В результате на экране появится вкладка **Sharing** диалогового окна свойств (см. рис. 24.6). Выберите переключатель **Share this folder** (Открыть общий доступ к этой папке) и укажите имя нового коллективного ресурса (а также комментарий описательного характера — **Comment** — который смогут увидеть пользователи). Далее укажите предельное число пользователей, которые одновременно смогут обращаться к этому общему ресурсу. Как правило, имеет смысл оставить переключатель области **User limit** в исходном положении **Maximum allowed** (Максимально возможное).

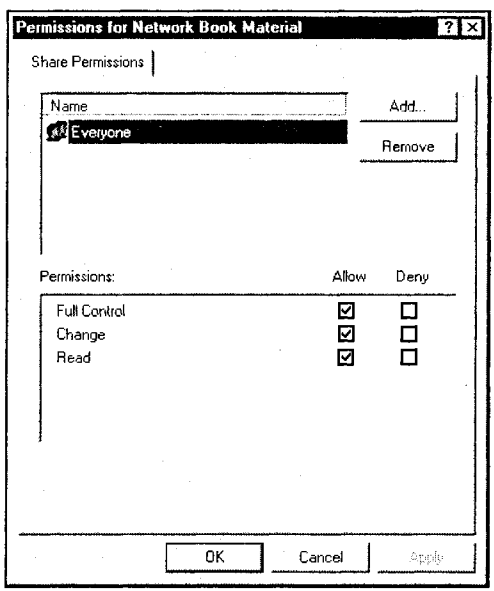


Рис. 24.14. Определение полномочий для общего ресурса в целях защиты информации, хранящейся на сервере

Теперь нужно установить права доступа к этому общему ресурсу. Чтобы открыть диалоговое окно **Permissions** (рис. 24.14), нажмите кнопку **Permissions** (Полномочия). Настройки по умолчанию предоставляют группе Everyone (Все) наиболее полные права по отношению к коллективному ресурсу. Обычно этот вариант оказывается приемлемым. При необходимости ввести какие-либо ограничения на доступ к совместно используемому ресурсу настройки нужно выполнять именно в диалоговом окне **Permissions** (Полномочия). В результате нажатия кнопки **Add** (Добавить) появляется диалоговое окно **Select Users, Contacts, Computers, or Groups** (Выбор: Пользователи, Контакты, Компьютеры или Группы); в нем вы можете указать пользователей и группы, которым требуются права доступа к данному совместно используемому ресурсу. После добавления пользователя или группы при помощи флажков, которые находятся в окне **Permissions** (Полномочия), можно задать точные полномочия: **Full**

Control (Полный доступ), **Change** (Изменение) или **Read** (Чтение). Чтобы сохранить определенные права, нажмите кнопки **Apply** (Применить) и **OK**, а затем сохраните изменения, внесенные в настройки нового ресурса, нажав **Apply** и **OK** еще раз.

После создания совместно используемого ресурса пользователи могут к нему обращаться — это делается через **Network Neighborhood** (Сетевое окружение в системах Windows 9x/NT) или **My Network Places** (Мое сетевое окружение в Windows 2000). Двойной щелчок на совместно используемом ресурсе приводит к его открытию (в зависимости от установленных прав доступа). Кроме того, вы можете сделать ресурс скрытым, но, тем не менее, доступным для тех пользователей, которым известно его имя. Процесс создания скрытого общего ресурса отличается от процесса создания обычного ресурса лишь тем, что в первом случае в конец имени ресурса нужно поставить символ "$". К примеру, myfiles$ — это имя совместно используемого ресурса, который при просмотре доступных сетевых ресурсов не отображается.

Подключение сетевого диска

Возможно, вам понадобится сымитировать подключение к вашему компьютеру жесткого диска с сетевым ресурсом. К примеру, многие приложения, хранящие файлы в сети, требуют, чтобы к сетевым каталогам можно было обращаться при помощи обычного имени дисковода. Процесс имитации диска с сетевым разделяемым ресурсом называется отображением или подключением (mapping) — он подразумевает формирование соответствия (связи) между выбранным именем (буквой) дисковода и собственно сетевым ресурсом (например, каталогом), которому назначено это имя. Чтобы подключить диск, откройте на клиентском компьютере **Network Neighborhood** и найдите общий ресурс, который предполагаете подключить. Щелкните на нем правой кнопкой мыши, и выберите пункт **Map Network Drive** (Подключить сетевой диск). В результате перед вами появится имя домена и ресурса (например, \\author1\my doc c). Выберите имя дисковода для создания соответствия и нажмите кнопку **OK**. С этого момента выбранный ресурс будет отображаться на вашем клиентском компьютере под указанным именем дисковода и, как таковой, будет присутствовать в папке My Computer (Мой компьютер).

Управление принтерами

На приобретение и сопровождение принтеров могут уходить серьезные средства; кроме того, коэффициент их использования редко доходит до максимума (страниц в месяц). Это значит, что значительные мощности принтеров не задействуются. Кроме того, перед администраторами часто ставится задача сопровождения множества принтеров различных производителей и моделей, приписанных многим пользователям. При этом вполне возможно организовать совместное использование принтеров через сеть, в результате чего многие пользователи сети смогут работать с одним и тем же принтером. При наличии общего принтера задания на печать перенаправляются в сетевую очередь (а не в очередь локального принтерного порта). Задание пребывает в очереди (обычно представленной в виде временного файла на сервере печати) вплоть до пересылки на принтер. Очереди заданий на печать способны аккумулировать большое количество заданий, исходящих от любых пользователей сети. После того как задание полностью отсылается принтеру, сервер удаляет его из очереди.

Принцип работы сервера печати реализуется по-разному. Если применяемый принтер подключен к серверу или рабочей станции, расположенной в сети, то задачи сервера печати выполняет именно этот сервер или рабочая станция. Если принтер подключен напрямую к сети (т. е. у принтера есть собственный сетевой порт), то обычно одним из компонентов его сетевого аппаратного обеспечения является встроенный сервер печати. Уровень интеллекта последнего достаточен для того, чтобы войти в сеть и выполнить обслуживание отдельной очереди заданий на печать.

Примечание

Для сетей, численность которых превышает 20 пользователей, лучше всего покупать принтеры с сетевыми интерфейсами и встроенными серверами печати; в противном случае следует задействовать специализированные аппаратные серверы, которые связывают принтеры с сетью.

Задания на печать выдаются программой печати (например, приложением Corel, установленным на рабочей станции). Эта программа отсылает свои печатные выходные данные локальной операционной системе (возможно, это Windows 2000 Professional). Локальная ОС пользуется драйвером принтера, запрошенным программой, для того, чтобы сформировать для принтера фактическое задание на печать. Затем при помощи установленного программного обеспечения сетевого клиента локальная операционная система отправляет форматированное задание на печать в очередь печати — в ней задание пребывает вплоть до освобождения принтера. Сервер печати извлекает задание на печать из очереди и отсылает его на принтер.

Имейте в виду, что несогласованность драйверов может привести к проблемам при печати на совместно используемом принтере. Рабочая станция, отправляющая задание на печать в очередь, форматирует данные, предназначенные для распечатки, при помощи драйвера принтера, составленного для той операционной системы, которая установлена на этой рабочей станции. Когда задание на печать приходит на компьютер, выполняющий функцию сервера печати, задание отправляется на локальный принтер посредством драйвера, установленного на сервере. Таким образом, задание, отформатированное для HP LaserJet 6 на рабочей станции Windows 98, после обработки драйвером LaserJet 6 для Windows 2000 Server (если именно там расположен совместно используемый принтер) может привести к некорректной распечатке. Определенные элементы распечатаются превосходно, однако конечный результат выполнения некоторых необычных или специализированных заданий может содержать ошибки. Решение часто заключается в том, чтобы отправить задание на печать с другой рабочей станции, на которой установлена та операционная система, которая используется на сервере печати (например, если компьютер, выполняющий функцию сервера, работает на базе Windows 2000 Server, попробуйте произвести распечатку с рабочей станции Windows 2000 Professional).

Совместное использование принтера

Теперь мы организуем коллективное использование принтера, подключенного к нашему серверу Windows 2000. Наш аппарат — это обычный принтер, подключенный через параллельный порт к компьютеру, выполняющему функцию сервера, и установленный с применением подходящих для Windows 2000 драйверов. Чтобы открыть на сервере каталог Printers (Принтеры), выберите последовательно команды

Start, Settings, Printers (Пуск, Настройка, Принтеры). В этом каталоге перечислены все установленные на данный момент принтеры. Правой кнопкой мыши щелкните на принтере, который собираетесь сделать общим, и выберите пункт меню **Sharing** (Доступ). На экране появится вкладка **Sharing** диалогового окна свойств этого принтера (рис. 24.15). Установите переключатель в положение **Shared as** (Общий доступ) и присвойте принтеру имя ресурса (например, CanonBJC), под которым он будет представлен на клиентских компьютерах. Если вы согласны с принятыми по умолчанию правами доступа к совместно используемому принтеру (печатать на нем могут участники группы Everyone, т. е. все), нажмите кнопку **OK**.

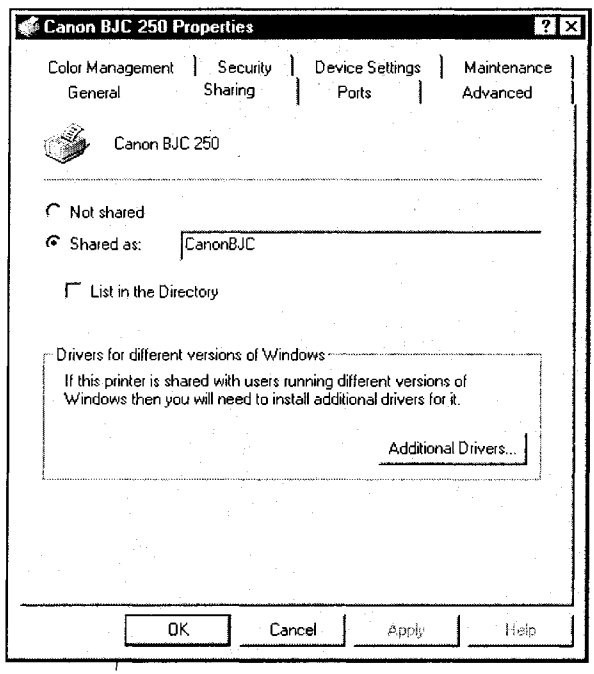


Рис. 24.15. Разделяемые принтеры и пользователи сети

Примечание

Если речь идет о новом принтере, который еще даже не установлен, откройте каталог Printers, а затем при помощи мастера Add Printers Wizard выполните настройку этого принтера на сервере; лишь после этого вы сможете приступить к попыткам сделать его доступным в масштабе сети.

Если к принтеру предъявляются высокие требования по интенсивности печати, можете воспользоваться функцией объединения принтеров. Она предусматривает установку ряда идентичных принтеров, подключенных к единой очереди заданий на печать и предстающих перед сетью как один принтер. При этом пользователи могут отправлять задания на печать "одному" принтеру, и их будет обслуживать первый освободившийся физический принтер. При помощи функции объединения принте-

ров у вас появляется возможность предоставить пользователям сети комплект принтеров как единый принтер, в результате чего объем запросов на печать, который можно будет обработать, очень сильно возрастает. Впрочем, объединенные принтеры действительно должны быть идентичными — дело в том, что они пользуются одним драйвером принтера. Чтобы задействовать функцию объединения принтеров, перейдите на вкладку **Ports** (Порты) совместно используемого принтера, пометьте флажок **Enable printer pooling** (Разрешить группировку принтеров в пул), а затем выберите дополнительные порты, на которых будут установлены принтеры аналогичного типа.

Чтобы установить права доступа к общему принтеру, перейдите на вкладку **Security** (Безопасность) диалогового окна свойств принтера — обратите внимание на исходное распределение полномочий по группам. Каждая группа наделена тремя основными полномочиями: **Print** (Печать), **Manage Printers** (Управление принтерами) и **Manage Documents** (Управление документами). Группа Everyone имеет право на печать (Print), но не может управлять документами в очереди. Полномочиями на управление документами обладает специальная группа под названием Creator Owner. Это означает, что пользователь, отправивший задание на печать, автоматически получает право на его изменение или удаление (но он не может выполнять эти операции по отношению к другим заданиям, находящимся в очереди).

Дополнительные ресурсы

Институт компьютерной безопасности (Computer Security Institute): **www.gosci.com**.

Укрепление Windows 2000: **www.systemexperts.com/win2k.shtml**.

Международная ассоциация по компьютерной безопасности (International Computer Security Association): **www.icsa.net**.

Microsoft: **www.microsoft.com**.

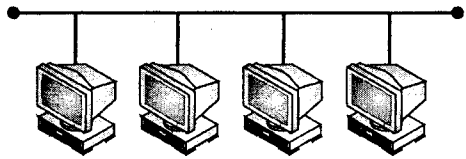
Инструкции по безопасности от NSA (National Security Agency — Управление национальной безопасности): **nsa1.www.conxion.com/win2k/index.html**.

SANS: **www.sans.org**.

Обновления системы безопасности: **www.microsoft.com/windows2000/downloads/security/default.asp**.

Windows 2000: **www.microsoft.com/windows2000/default.asp**.

Техническая поддержка Windows: **www.microsoft.com/windows2000/support/default.asp**.



ГЛАВА 25

Администрирование и безопасность Linux

За последние несколько лет операционная система Linux прошла длинный путь. Когда-то считавшаяся подходящей лишь для ограниченной сферы деятельности, Linux превратилась в прекрасную платформу для клиентских и серверных систем. Помимо прочего, в различных версиях Linux (например, в Red Hat) предусмотрен комплект мощных и прогрессивных серверных функций, включая сервер новостей, Web-сервер, FTP-сервер, файловый сервер, DNS-сервер, серверы баз данных SQL и т. д. Задачи установки и сопровождения также стали значительно проще, чем были несколько лет назад — в основном, благодаря серьезным усовершенствованиям процедуры установки (Setup) и применению удобного графического интерфейса. В этой главе администраторы могут ознакомиться с обзором функций Red Hat Linux 7.2, процессами установки и элементарного тестирования этой ОС; кроме того, здесь представлены общие принципы администрирования пользователей и обеспечения защиты.

Примечание

За подробной информацией об операционной системе Red Hat Linux и методах ее администрирования вы можете обращаться на сайт Red Hat по адресу **www.redhat.com**.

Основы инсталляции

При отсутствии на вашем сервере предустановленной ОС Linux вам придется провести процесс ее инсталляции. По сути, инсталляция Red Hat 7.2 хорошо автоматизирована, но по ходу ее выполнения вам придется принимать те или иные решения. Существует огромное количество способов установки Red Hat Linux, однако, что касается запуска процесса инсталляции, у вас есть лишь два практических варианта: либо загрузиться напрямую с 1-го компакт-диска Linux, либо приготовить загрузочные дискеты. Большинство серверов возрастом менее пяти лет способны загружаться со своих приводов CD-ROM (а это, несомненно, лучшее решение для выполнения инсталляции). Впрочем, если необходимость в создании загрузочных дискет все же возникнет (например, если на сервере нет привода CD-ROM), то при работе в системе на базе Windows вы сможете это сделать, запустив программу rewrite.exe, расположенную в каталоге \dosutils компакт-диска Linux. При этом вы должны буде-

те указать исходный файл (\images\boot.img на компакт-диске Linux) и гибкий диск, на который будет производиться запись. При составлении обзора инсталляции для этой главы допускалось, что вы загружаетесь с компакт-диска Linux.

Проверка аппаратного обеспечения

Несмотря на то, что система Linux сделала большие успехи в части аппаратной совместимости, в ней до сих пор отсутствуют те возможности по совместимости устройств, которыми обладают операционные системы типа Windows XP/2000. Таким образом, прежде чем приступать к инсталляции, нужно найти время на инвентаризацию серверного оборудования. В первую очередь, убедитесь в том, что сервер отвечает минимальным требованиям к аппаратной части (например, к памяти и свободному дисковому пространству), предъявляемым той версией Linux, которую вы намереваетесь устанавливать. Кроме того, все отдельные аппаратные устройства (включая видеоадаптер, звуковое устройство, сетевую плату, хост-адаптер SCSI и пр.) должны присутствовать в списке совместимого оборудования (Hardware Compatibility List, HCL) для данной версии Linux. К примеру, список HCL для Red Hat опубликован по адресу **www.redhat.com/hardware**, а HCL от Caldera есть на сайте **www.caldera.com/products/openlinux/hardware.html**.

Запуск программы установки

Подготовившись к процессу инсталляции, поместите первый установочный компакт-диск Linux в привод CD-ROM, и перезагрузите компьютер. При перезапуске системы она выполнит автоматическое считывание этого компакт-диска и запустит процедуру инсталляции. На дисплее появится текстовый экран, на котором можно будет выбрать текстовый или графический режим инсталляции, а также определить некоторые другие опции. Чтобы запустить графическую процедуру инсталляции, просто нажмите клавишу <Enter> — в результате произойдет загрузка графического пользовательского интерфейса Linux.

Примечание

Если компьютер не загрузится с CD-ROM, то вам, вероятно, придется зайти в CMOS Setup и изменить загрузочную последовательность таким образом, чтобы система сначала проверяла наличие загрузочного носителя в приводе CD-ROM, а уже после этого переходила к проверке жесткого и гибкого дисков.

Основные варианты выбора

Теперь, чтобы подготовить инсталляцию Linux, нужно указать некоторые элементарные данные о вашей системе и ее географическом положении. К счастью, графическая программа установки Linux предусматривает удобный интерфейс типа "укажи и щелкни", сопровождая его контекстно-зависимой справочной системой, так что по мере прохождения инсталляции вы сможете принимать обоснованные решения.

Язык

Выберите язык, которым вы предпочитаете пользоваться в ходе процесса инсталляции и который хотите установить в системе по умолчанию. Впоследствии, при про-

должении установки выбор языка поможет определить настройки вашего часового пояса (программа установки попытается определить подходящий часовой пояс исходя из языка, установленного на данном этапе). Выбрав подходящий язык, нажмите кнопку **Next** (Далее).

Клавиатура

Выберите модель клавиатуры, которая лучше всего подходит к вашей системе. Если вам не удастся найти точное совпадение, укажите общий тип клавиатуры (например, Generic 101-key PC). Теперь укажите подходящий тип раскладки клавиатуры (например, U.S. English). Формирование специальных символов (таких как С, Ф и З) несколькими нажатыми клавишами производится при помощи клавиш диакритических знаков (они также называются сочетанием последовательности клавиш). Такие клавиши задействуются по умолчанию — если они вам не нужны, выберите **Disable dead keys**. При желании протестировать клавиатуру введите текст в пустом текстовом поле, расположенном в нижней части экрана. Чтобы продолжить процесс инсталляции, нажмите кнопку **Next** (Далее).

Мышь

Выберите подходящий тип и интерфейс мыши (например, последовательный или PS/2), установленной в вашей системе. Если найти точное совпадение не удается, выберите одну из общих записей, основываясь при этом на количестве кнопок и типе интерфейса. Если у вас мышь с шинным или PS/2-интерфейсом, определять порт и устройство не придется. При наличии мыши с последовательным интерфейсом выберите порт и устройство, на котором установлена мышь. Флажок **Emulate 3 Buttons** (Имитировать три кнопки) позволяет пользоваться двухкнопочной мышью так, как будто на ней три кнопки. Обычно при наличии трехкнопочной мыши работать в системе X-Window оказывается удобнее — имитация третьей (средней) кнопки производится путем одновременного нажатия обеих имеющихся кнопок мыши.

Тип инсталляции

После появления непродолжительной заставки приходит время выбора типа инсталляции. В Red Hat Linux предусматривается несколько классов установки. Рабочая (workstation) инсталляция обычно оказывается оптимальной для начинающих пользователей Linux. При выборе рабочей инсталляции формируется система для домашнего или настольного применения. Устанавливается графическая, Windows-подобная среда. Серверная (server) инсталляция лучше всего подходит для тех случаев, когда вы хотите задействовать свою систему в роли Linux-сервера, но не намерены специально настраивать конфигурацию системы. Портативная (laptop) инсталляция упрощает процесс установки Red Hat Linux на портативных компьютерах. Как и рабочая инсталляция, она обеспечит наличие подходящих пакетов и предложит вашему вниманию автоматизированную среду установки. Выборочная (custom) инсталляция предусматривает наибольшую гибкость в ходе процесса установки системы. Вы получаете возможность выбрать загрузчик операционной системы, необходимые пакеты и т. д. Выборочный вариант инсталляции лучше всего подходит для тех пользователей, кто уже знаком с процессом установки Red Hat Linux и кому требуется абсолютная гибкость. Если в вашей системе уже есть работающая версия Red Hat Linux (3.0.3 или одна из последующих), и вам нужны новейшие пакеты и последняя версия ядра, оптимальной представляется инсталляция типа модернизации (upgrade).

Управление разделами Linux

На этом этапе процесса инсталляции вам нужно создать разделы Linux — это действие немного отличается от сегментирования в Windows. В среде Linux во время загрузки выполняется монтирование (mounting) разделов. Монтирование делает содержимое раздела доступным — так, как будто он является одним из каталогов системы. К примеру, корневой каталог (/) находится в первом (корневом) разделе. Подкаталог под названием /usr расположен в корневом каталоге, причем в пределах этого подкаталога можно собрать дополнительные разделы. Так как все смонтированные разделы представлены как единое дерево каталогов (а не как автономные диски), программа инсталляции не проводит различия между отдельными разделами. Важно лишь то, к какому каталогу относится каждый отдельно взятый файл. Процесс инсталляции автоматически распределяет свои файлы по всем смонтированным разделам (поскольку смонтированные разделы являют собой различные части дерева каталогов, где обычно и размещаются файлы). Наиболее значимая группа файлов Linux располагается в каталоге /usr, в который записываются все программы. Типичная древовидная структура Linux изображена на рис. 25.1.

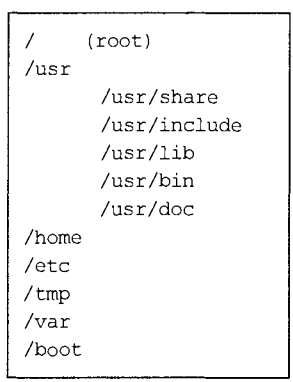


Рис. 25.1. Древовидная структура Linux состоит из смонтированных разделов, представленных в виде подкаталогов корневого системного каталога

Ниже перечислены все важнейшие разделы.

- /usr. Здесь расположены все программные файлы (аналогично каталогу Program Files в системе Windows).
- /home. Здесь находятся домашние каталоги всех пользователей (в случае, если они вообще размещаются на данном сервере). Полезная функция этого раздела заключается в том, что он не позволяет пользователям занять весь диск и оставить другие важные компоненты (такие как журналы регистрации) без свободного пространства.
- /etc. В этом разделе содержится множество конфигурационных файлов и каталогов Linux. Если вы намереваетесь найти файлы, определяющие настройки платформы Linux, искать следует именно здесь.
- /var. Этот раздел предназначен для постоянного хранения регистрационных файлов. Так как файлы регистрации модифицируются сторонними пользователями

(например, посетителями Web-сайта), их архивирование в отдельном разделе может предотвратить атаку типа "отказ от обслуживания" (Denial of Service, DoS), в ходе которой в журнале регистрации создается такое количество записей, что они переполняют весь диск.

- /tmp. Здесь хранятся временные файлы. Так как записывать файлы в этот каталог (аналогичный каталогу C:\TEMP в системах Windows) могут все пользователи, вы должны следить за тем, чтобы он не заполнил все пространство диска — для этого он и размещается в автономном разделе.
- Swap (Подкачка). Здесь хранится виртуальная память. Хотя Linux (и другие версии UNIX) может задействовать для хранения виртуальной памяти обычный дисковый файл (именно так делается в Windows), наличие файла подкачки в автономном разделе повышает производительность.

Linux предусматривает некоторые возможности, связанные с автоматическим сегментированием, и позволяет вам определенным образом контролировать удаление данных из системы (в случае, если они вообще удаляются). У вас есть три варианта.

- *Удалить из системы все разделы Linux* (Remove all Linux partitions on this system). В случае выбора этого варианта из системы будут удалены только разделы Linux (созданные в ходе предыдущей инсталляции Linux). Все прочие разделы, которые, возможно, присутствуют на ваших жестких дисках, будут сохранены.
- *Удалить из системы все разделы* (Remove all partitions on this system). Эта опция позволяет удалить все разделы, существующие на ваших жестких дисках — в том числе те, что были созданы другими операционными системами наподобие Windows 9x/NT/2000.
- *Сохранить все разделы и задействовать свободное пространство* (Keep all partitions and use existing free space). Этот вариант следует выбрать, если вы желаете сохранить все существующие данные и разделы, а свободного пространства на ваших жестких дисках достаточно для проведения инсталляции Linux.

При помощи мыши выберите жесткий диск(и), на который предполагаете установить Red Hat Linux. При наличии двух или нескольких жестких дисков вы можете выбрать один из них — именно на нем будет проводиться инсталляция. Невыбранные жесткие диски (и все содержащиеся на них данные) не будут затронуты. Чтобы пересмотреть разделы, созданные путем автоматического сегментирования, и внести все необходимые изменения, воспользуйтесь опцией **Review**. Выбрав **Review** и нажав кнопку **Next**, чтобы продолжить процесс инсталляции, вы сможете просмотреть созданные разделы в Disk Druid (Жрец дисков). Если эти разделы не отвечают вашим требованиям, в них можно будет внести изменения. Приняв все необходимые решения и подготовившись к продолжению процесса инсталляции, нажмите кнопку **Next**.

Загрузчик операционной системы

Для того чтобы система Red Hat Linux могла загружаться без загрузочного диска, обычно требуется установить загрузчик операционной системы. Есть два варианта: можно установить либо GRUB (выбранный по умолчанию), либо LILO (LInux LOader, загрузчик Linux). GRUB представляет собой программный загрузчик операционной системы, который может применяться для загрузки Red Hat Linux и других

операционных систем — например, Windows 9x. Если вы решите не устанавливать загрузчик операционной системы, не забудьте ближе к завершению процесса инсталляции создать загрузочный диск или предусмотреть другой метод загрузки Linux (например, задействовать загрузчик от стороннего производителя). Если же вы предпочтете выполнить установку загрузчика операционной системы (GRUB или LILO), следует определить, где нужно проводить его установку. Загрузчик операционной системы может быть установлен в одном из двух мест.

- *Главная загрузочная запись* (Master Boot Record, MBR). MBR — это специальная область жесткого диска, которая автоматически загружается системой BIOS вашего компьютера; это самая ранняя временная точка, с которой загрузчик операционной системы может принять на себя управление процессом загрузки. Загрузчик рекомендуется устанавливать именно здесь — за исключением тех случаев, когда запись MBR уже задействована для запуска другого загрузчика операционной системы (например, System Commander или Boot Manager OS/2). Если установить загрузчик в MBR, то GRUB (или LILO) при запуске компьютера будет выводить на экран загрузочную строку. После этого вы сможете инициировать загрузку Red Hat Linux или любой другой операционной системы, на запуск которой настроен загрузчик.
- *Первый сектор корневого раздела.* Этот вариант рекомендуется задействовать в случае, если на вашем компьютере уже используется другой загрузчик операционной системы (например, System Commander). В таком случае первым принимать управление будет ранее установленный загрузчик. Впоследствии вы сможете настроить его на запуск GRUB (или LILO), который, в свою очередь, будет загружать Linux.

Определитесь с тем, куда вы хотите установить GRUB (или LILO). Если на компьютере будет установлена только система Red Hat Linux, имеет смысл указать MBR. На машинах с Windows 9x загрузчик операционной системы также следует поместить в MBR — в этом случае он сможет запускать любую из двух установленных систем. Приводятся все загрузочные разделы — в том числе те, что используются другими операционными системами. Раздел с корневым файлом Linux будет обозначаться "загрузочной меткой" `linux`. Загрузочные метки могут быть присвоены и другим разделам. Чтобы определить загрузочные метки других разделов (или изменить существующую метку), щелкните мышью на нужном разделе, и внесите все необходимые изменения. Наконец, в целях защиты системы следует создать пароль GRUB. В результате пользователи лишатся возможности передавать опции ядру, а следовательно, не смогут подорвать систему защиты компьютера. Введите пароль, затем подтвердите его, и переходите к следующему этапу.

Настройка сети и брандмауэра

Теперь нужно выполнить конфигурацию сетевой платы, установленной на данном компьютере. Если в системе установлено несколько сетевых плат, то для каждой из них будет приведена отдельная вкладка. Вы сможете переключаться между устройствами (например, между eth0 и eth1), причем данные, внесенные в каждую отдельную вкладку, будут распространяться только на соответствующее устройство. Укажите, следует ли настраивать IP-адрес средствами DHCP. В случае выбора опции **Activate on boot** (Активировать при загрузке) сетевой интерфейс будет запускаться каждый раз при включении системы. Затем введите в соответствующие поля IP-

адрес (**IP Address**), сетевую маску (**Netmask**), сетевые (**Network**) и широковещательные адреса (**Broadcast addresses**). При наличии полностью определенного доменного имени, соответствующего данному сетевому устройству, его нужно ввести в поле **Hostname**. Наконец, введите адрес шлюза (**Gateway**) и первичный адрес DNS (**Primary DNS**); при необходимости их можно дополнить вторичным (**Secondary DNS**) и третичным (**Ternary DNS**) адресами DNS. Чтобы продолжить процесс инсталляции, нажмите кнопку **Next**.

В целях повышения безопасности системы в Red Hat Linux интегрирован брандмауэр. Выберите уровень безопасности, который лучше всех годится для вашей системы: высокий (**High**), средний (**Medium**) или нулевой (**No firewall**). В случае выбора уровня **High** ваша система не будет принимать соединения (кроме тех, что определены настройками по умолчанию), которые не были вами ясно установлены. По умолчанию допускаются только соединения DNS и DHCP. Если вы планируете подключить систему к Интернету, безопаснее всего не делать из нее сервер. В случае необходимости применения дополнительных служб воспользуйтесь опцией **Customize** — она позволит разрешить выполнение через брандмауэр отдельных служб.

Если вы выберите средний (**Medium**) уровень безопасности, брандмауэр не позволит удаленным компьютерам обращаться к некоторым ресурсам вашей системы. Намереваясь допустить обращение к некоторым ресурсам (например, к RealAudio), но при этом блокировать доступ к обычным системным службам, выберите средний уровень безопасности, а затем при помощи опции **Customize** выберите службы, выполнение которых через брандмауэр вы хотите разрешить. Вариант **No firewall** предусматривает полный доступ к вашей системе без какой-либо проверки на предмет безопасности. Им следует пользоваться лишь в том случае, если вы работаете в доверенной сети (т. е. не в Интернете), или планируете провести более детальную настройку брандмауэра позднее. Опция **Customize** позволяет добавить доверенные устройства и разрешить выполнение дополнительных входящих служб.

Язык и часовой пояс

Red Hat Linux может установить в системе несколько языков и впоследствии поддерживать их применение. Вы должны выбрать язык, который будет использоваться по умолчанию (в системе Linux после завершения процесса ее инсталляции). В случае установки других языков язык по умолчанию после завершения инсталляции можно будет сменить. В большинстве случаев при работе в системе применяется только один язык, причем, ограничившись им, вы сможете сэкономить значительное дисковое пространство. Чтобы установить в системе несколько языков, отметьте их (или выберите все возможные языки).

Установка часового пояса производится двумя методами: либо вы указываете географическое положение компьютера, либо определяете отклонение нужного часового пояса по отношению к универсальному глобальному времени (coordinated universal time, UTC). Обратите внимание на вкладки **Location** и **UTC Offset**, расположенные в верхней части экрана. Первая позволяет настроить часовой пояс исходя из географического местоположения. Вы можете указывать на карте различные области, которые хотите просмотреть, или щелкнуть на обозначении определенного города — на месте щелчка появится красный символ "X". Кроме того, чтобы найти нужный часовой пояс, вы можете прокрутить список. Вторая вкладка позволяет указать смещение часового пояса по отношению к UTC. На экране присутствует спи-

сок отклонений, из которого вы можете выбрать нужное; кроме того, есть опция, с помощью которой можно установить переход на летнее время. Если вы уверены в том, что система настроена на применение UTC, пометьте флажок **System clock uses UTC**.

Настройка учетных записей

Следующий экран — **Account Configuration** — позволяет определить корневой пароль. Кроме того, здесь можно создавать пользовательские учетные записи, с помощью которых после завершения инсталляции будет выполняться вход в систему. Эти этапы процесса установки Linux особенно важны, а к созданию безопасных паролей придется приложить некоторые умственные усилия.

Корневой пароль

Корневая учетная запись в Linux аналогична административной учетной записи, применяемой на машинах Windows NT/2000. Корневая учетная запись задействуется при установке пакетов, обновлении RPM и выполнении большинства функций, связанных с сопровождением системы (в число которых входит координация пользовательских учетных записей). Регистрация при помощи корневой учетной записи предоставляет вам полный контроль над системой Linux, и именно поэтому к задаче подбора пароля нужно подойти очень серьезно. Разумной практикой является применение корневой учетной записи исключительно для целей администрирования системы и некорневой учетной записи (создание которой рассматривается в *разд. "Корневая учетная запись"*) — для общего пользования. Если вы заведете простую учетную запись для повседневного употребления, а переключаться на корневую учетную запись будете только для выполнения важных управленческих задач, вы сведете к минимуму возможность опечатки или введения неверной команды, которая способна нанести вред вашей системе.

Программа инсталляции выведет на экран приглашение к вводу корневого пароля системы (вы обязаны его указать; в противном случае программа инсталляции не позволит вам перейти к следующим этапам). Минимальная длина корневого пароля составляет шесть символов, причем для подтверждения правильности ввода вы должны указать его дважды. Имейте в виду, что пароль чувствителен к регистру. Если вы решите записать свой пароль, храните эту информацию в безопасном месте. Впрочем, фиксировать создаваемые пароли не рекомендуется.

Примечание

Корневой пароль — это пароль администратора системы Linux. Регистрироваться при помощи корневой учетной записи следует только тогда, когда это необходимо для выполнения задач, связанных с сопровождением системы. Все изменения, произведенные корневым пользователем, могут иметь последствия, распространяющиеся на всю вашу систему.

Пользовательская учетная запись

Будет вполне разумно, если вы создадите для себя по крайней мере одну пользовательскую учетную запись — с ее помощью вы сможете зарегистрироваться в системе Linux сразу после завершения процесса ее инсталляции. Таким образом, впоследст-

вии вы без труда войдете в систему, и вам не придется переключаться на корневую учетную запись лишь для того, чтобы создать пользовательскую учетную запись. Укажите краткое регистрационное имя, соответствующее новой пользовательской учетной записи, а затем введите и подтвердите пароль. Введите полное имя владельца учетной записи и нажмите кнопку **Add**. Данные новой учетной записи будут введены в перечень учетных записей, а содержимое полей, при помощи которых производится формирование учетных записей, будет сброшено — следовательно, вы сможете приступить к созданию новых пользователей (в случае, если вы предпочтете настроить несколько учетных записей заблаговременно). Кроме того, у вас есть возможность редактировать (**Edit**) или удалять (**Delete**) созданные ранее учетные записи.

Выбор пакетов

Операционные системы Linux (в том числе Red Hat) предусматривают установку большого количества дополнительных возможностей (они называются пакетами). В виде пакетов можно установить предпочтительный вариант рабочего стола, Web- и FTP-серверы, серверы новостей, SQL-серверы и т. д. На данном этапе необходимо выбрать те пакеты, которые вам нужны. Если в системе много свободного места (около 1,7 Гбайт), вы, естественно, можете сразу установить дополнительные пакеты, однако их работа может оказать негативное влияние на производительность сервера — не говоря уже о системе защиты. Вы можете выбирать компоненты (совокупности пакетов, сгруппированных в соответствии с их функцией — например, C Development (разработка приложений на C), Networked Workstation (сетевая рабочая станция), или Web Server (Web-сервер)), отдельные пакеты, или и то и другое. Для того чтобы выбрать один из компонентов, нужно пометить флажок, расположенный рядом с его записью. Выберите все компоненты, которые хотите установить — это простейший путь.

Если вам требуется более жесткий контроль над файлами, размещенными в системе Linux, можете выбирать пакеты по отдельности. Для этого пометьте флажок **Select Individual Packages** (Выбор пакетов индивидуально), расположенный в нижней части экрана. Выбрав нужные компоненты, вы сможете добавлять или удалять отдельные пакеты. Просматривать частные пакеты можно в древовидном или одноуровневом представлении. Древовидное представление позволяет просматривать пакеты, сгруппированные по типам приложений, а одноуровневое представление предусматривает вывод названий всех пакетов в алфавитном порядке в правой части экрана. К примеру, в древовидном представлении вы видите перечень групп пакетов. Развернув этот перечень и выделив одну группу, вы увидите справа список входящих в нее пакетов. Чтобы выбрать отдельный пакет, дважды щелкните на флажке, расположенном рядом с его именем. Галочка в этом флажке обозначает, что данный пакет был выбран, и информация о нем выводится в нижней части экрана.

Неразрешимые зависимости

Работа многих программных пакетов зависит от того, установлены ли в вашей системе другие программные пакеты. К примеру, многие графические средства администрирования системы Red Hat требуют наличия пакетов python и pythonlib. Стараясь обеспечить наличие в системе всех пакетов, необходимых для ее полной работоспособности, каждый раз, когда вы устанавливаете или деинсталлируете программные пакеты, Red Hat Linux проводит проверку на предмет таких пакетных зависимостей.

Если для работы одного пакета требуется наличие другого пакета, устанавливать который вы не собираетесь, программа выводит список таких неразрешимых зависимостей и предоставляет вам возможность разрешить их.

Экран **Unresolved Dependencies** появляется только в том случае, если для функционирования выбранных пакетов требуются другие пакеты. В нижней части экрана (под списком недостающих пакетов) расположен флажок **Install packages to satisfy dependencies** (установить пакеты, необходимые для разрешения зависимостей) — по умолчанию он находится в установленном положении. Если вы решите не менять его положение, программа установки автоматически разрешит зависимости пакетов, прибавив все необходимые пакеты к списку выбранных.

Настройка видеотракта

Основой графического пользовательского интерфейса Linux является X-Window. Именно X-Window взаимодействует с видеоаппаратурой системы и передает информацию во внешний интерфейс Gnome или KDE. Последнее, что необходимо сделать до запуска процесса инсталляции Linux, — это провести точную идентификацию видеоадаптера, установленного в вашей системе. На экране X Configuration будет представлен перечень видеоплат, из которого вы сможете выбрать нужную модель. В большинстве случаев программе установки Linux удается корректно идентифицировать видеосистему, однако в любом случае выбранный видеоадаптер нужно сверить со списком установленного в системе аппаратного обеспечения. Если ваша видеоплата в представленном списке отсутствует, значит, возможно, X ее не поддерживает. Впрочем, если вы знаете технические характеристики своей платы, вы можете выбрать опцию **Unlisted Card** и попытаться провести ее настройку путем согласования набора видеомикросхем вашей платы с одним из имеющихся приложений X.

Затем следует ввести объем видеопамяти, установленной на вашей видеоплате (например, 16 или 32 Мбайт). Если вы укажете больший объем памяти, чем есть на самом деле, с видеоплатой ничего не случится, однако запуск приложения X, возможно, будет проходить некорректно. Обнаружив, что выбранные значения неверны, нажмите кнопку **Restore original values** — именно так можно вернуться к предложенным настройкам. Если вы намереваетесь настроить X после завершения процесса инсталляции (или вообще не собираетесь этого делать), выберите **Skip X Configuration**.

Утилита конфигурации X-Window выведет на экран перечень мониторов, из которого вам предстоит выбрать установленную модель. Можете согласиться с моделью, выбранной в результате процедуры автоматического распознавания, или выбрать из списка другую модель. Если ваш монитор в перечне отсутствует, выберите наиболее подходящую из представленных общих моделей. В случае выбора общего монитора программа установки сделает предположение относительно диапазона кадровой и строчной синхронизации (соответствующие значения обычно указываются в документации, сопровождающей каждый монитор). Предполагаемые диапазоны кадровой и строчной синхронизации также будут приведены на экране. Обнаружив, что выбранные вами значения неверны, нажмите кнопку **Restore original values** — именно так можно вернуться к предложенным настройкам. Выполнив все действия, связанные с настройкой монитора, нажмите кнопку **Next**.

Запуск инсталляции

Теперь должен появиться завершающий экран, подготавливающий к началу инсталляции Red Hat Linux. Чтобы прервать процесс инсталляции, нажмите кнопку Reset, расположенную на системном блоке вашего компьютера, или воспользуйтесь сочетанием клавиш <Ctrl>+<Alt>+<Delete>, которое вызывает перезагрузку системы. Если у вас нет подобных намерений, просто запустите процесс инсталляции, и не мешайте его продвижению. В какой-то момент вы должны будете вставить в привод CD-ROM второй установочный компакт-диск Linux. Обязательно воспользуйтесь возможностью создать загрузочную дискету, когда на экране появится соответствующее приглашение. После завершения процесса инсталляции нужно будет перезагрузить систему. Извлеките все диски из флоппи-дисковода и из привода CD-ROM. Если вы не выполнили установку загрузчика операционной системы, теперь придется воспользоваться загрузочным диском. По завершении обычного цикла включения питания на экране появится графическая строка загрузчика операционной системы, с помощью которой вы сможете запустить систему и приступить к работе на платформе Linux.

Примечание

После перезагрузки системы вы сможете ознакомиться с полным протоколом процесса инсталляции — он записан в файле /tmp/install.log.

Настройка сервера

Нет никакой гарантии, что настройки, принимаемые по умолчанию при инсталляции Linux, окажутся оптимальными в условиях вашей сети. После успешной установки Linux и перезагрузки системы нужно выбрать время на пересмотр сетевых настроек Linux и внесение в конфигурацию всех необходимых изменений. К счастью, на рабочих столах KDE и Gnome, применяемых в Red Hat Linux 7.2, предусмотрено графическое диалоговое окно, которое упрощает задачу просмотра и регулирования сетевых настроек. Пользуясь рабочим столом KDE, выполните следующие действия.

1. Щелкните на логотипе **K**, расположенном в нижнем левом углу рабочего стола. В результате откроется список групп приложений.
2. Выберите команды **System, Network Configuration** (Система, Конфигурация сети).
3. Введите корневой пароль (он нужен для внесения изменений в сетевые настройки) и нажмите кнопку **OK**.
4. Откроется диалоговое окно **Network Configuration** (рис. 25.2).

Аппаратное обеспечение

По умолчанию на экране появляется вкладка **Hardware**, в которой приводится физическое описание установленной сетевой платы. При помощи вкладки **Hardware** осуществляется добавление (**Add**), редактирование (**Edit**) и удаление (**Delete**) любых физических элементов сети Ethernet, модема, ISDN и оборудования маркерного кольца, конфигурируемых на сервере Linux. К примеру, чтобы настроить тип адаптера (указать производителя и модель) и имя устройства ядра для устройства

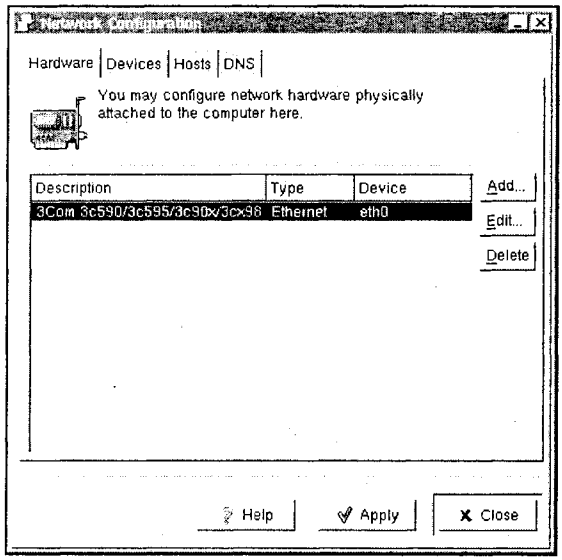


Рис. 25.2. Диалоговое окно **Linux Network Configuration** позволяет настроить физические и логические аспекты сетевого соединения системы

Ethernet, нужно выделить запись сетевой платы и нажать кнопку **Edit**. Выбранный тип адаптера определяет конкретный модуль (драйвер) ядра, который будет загружаться для данной сетевой платы. Указав адаптер, выберите имя устройства ядра сетевой платы (например, /dev/eth0 или /dev/eth1). Кроме того, вы можете выполнить настройки системных ресурсов данного устройства, таких как IRQ (Interrupt Request — запрос прерывания) и DMA (Direct Memory Access — прямой доступ к памяти).

Устройства

Вкладка **Devices** (рис. 25.3) позволяет добавлять (**Add**), редактировать (**Edit**) и удалять (**Delete**) логические сетевые устройства, связанные с физическим сетевым аппаратным обеспечением. К примеру, после установки или замены сетевой интерфейсной платы и ее точной идентификации, проводимой на вкладке **Hardware**, настройка ее сетевых свойств выполняется при помощи вкладки **Device**. Выделите нужное устройство, и нажмите кнопку **Edit**. В результате откроется диалоговое окно **Device** — к примеру, параметры устройства Ethernet будут выведены в диалоговом окне **Ethernet Device**, с помощью которого вы сможете отредактировать его общие настройки (**General**), настройки протокола (**Protocol**) и аппаратного устройства (**Hardware Device**). На вкладке **General** вы можете присвоить устройству мнемоническое имя, настроить включение устройства при загрузке компьютера, разрешить пользователям включать и отключать устройство. Вкладка **Protocols** позволяет редактировать настройки TCP/IP, в том числе IP-адрес (включая DHCP), имя хоста и статические сетевые маршруты. Псевдоним устройства определяется на вкладке **Hardware Device**. Псевдоним устройства дает возможность настраивать несколько виртуальных устройств, соответствующих одному физическому устройству.

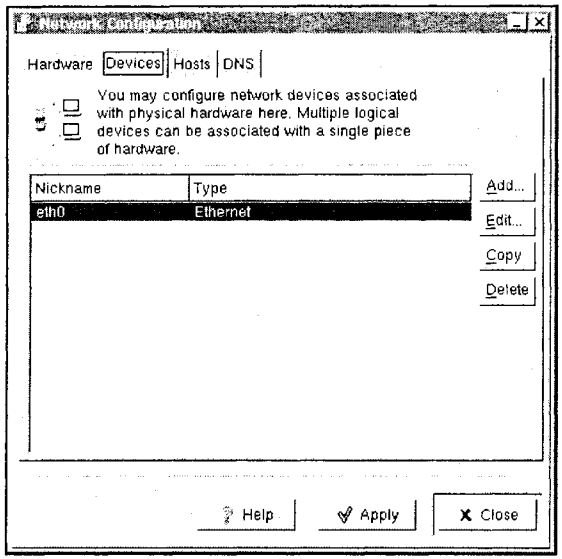


Рис. 25.3. Вкладка **Devices** позволяет настраивать логические элементы идентификации сетевой платы

Хосты

Вкладка **Hosts** (рис. 25.4) позволяет добавлять (**Add**), редактировать (**Edit**) и удалять (**Delete**) статические соответствия IP-адресов, которые хранятся в файле /etc/hosts.

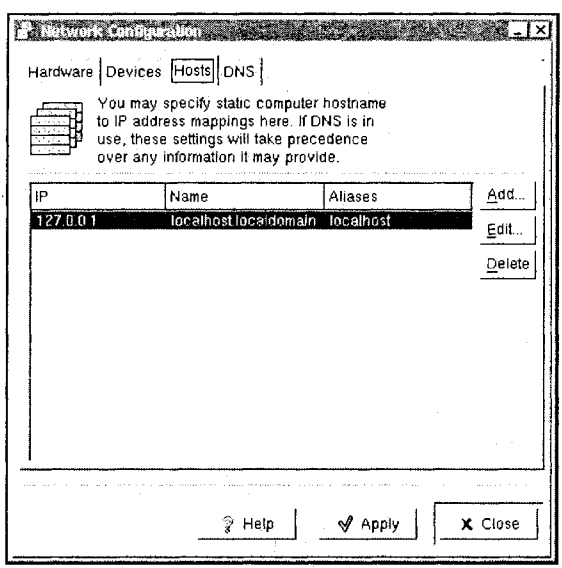


Рис. 25.4. Вкладка **Hosts** позволяет настраивать в системе Linux статическое соответствие IP-адресов

Этот файл содержит IP-адреса и имена хостов, в которые эти IP-адреса должны разрешаться. Когда система пытается разрешить имя хоста в IP-адрес (или определить имя хоста, соответствующее данному IP-адресу), в первую очередь она обращается к файлу /etc/hosts, и только после этого — к серверам имен (так происходит в том случае, если вы пользуетесь конфигурацией Red Hat Linux, принятой по умолчанию). Если нужный IP-адрес присутствует в файле /etc/hosts, обращения к серверам имен не происходит. Чтобы добавить в файл /etc/hosts новую запись, нажмите кнопку **Add**, расположенную во вкладке **Hosts**, введите необходимые данные, и нажмите кнопку **OK**. Чтобы внести выполненную запись в файл, нажмите кнопку **Apply**.

DNS

Если ваша система Linux входит в сеть, имеет смысл задействовать DNS-сервер. Серверы имен применяются для поиска других хостов, присутствующих в сети, а вкладка **DNS** позволяет настроить имя хоста системы, ее домен, серверы имен и домен поиска. На вкладке **DNS** (рис. 25.5) можно выполнить настройку имени хоста и домена системы, а также указать до трех адресов DNS-серверов. Кроме того, в этом диалоговом окне производится редактирование (**Edit**) или удаление (**Delete**) доменных имен в пределах пути поиска DNS, а также вносятся изменения в порядок поиска доменных имен. Имейте в виду, что эти записи сервера имен не превращают в сервер имен данную систему.

Примечание

После обновления конфигурации системы Linux не забудьте ввести все изменения в действие и сохранить их. Как правило, для того чтобы новые настройки вступили в силу, перезагрузки системы Linux не требуется.

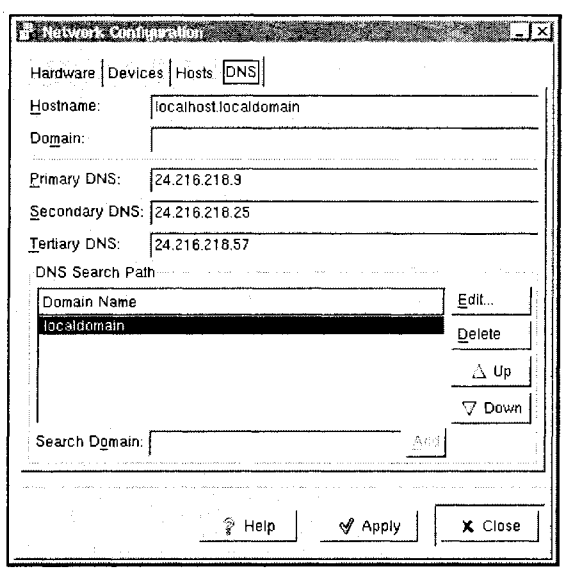


Рис. 25.5. Вкладка **DNS** позволяет идентифицировать в системе Linux серверы доменных имен

Проверка соединения

Настроив систему Linux и убедившись в том, что сетевой DHCP-сервер выделил для нее IP-адрес, проверьте, видят ли новую систему другие рабочие станции, участвующие в сети. К примеру, на станциях Windows 9x/2000 система Linux должна быть обозначена в каталогах Network Neighborhood или My Network Places. В них она представлена как пиктограмма с именем рабочей группы (к примеру, по умолчанию задействуется рабочая группа Mygroup и присваивается имя Localhost). Имейте в виду: пусть даже новая система Linux видна пользователям локальной сети, но для того, чтобы они могли обращаться к ее файлам и другим ресурсам (например, к принтерам), на ней необходимо сформировать совместно используемые ресурсы. Возможно, для того чтобы пользователи Windows получили возможность обращаться к общим ресурсам системы Linux, в последней придется установить пакет Samba.

Основы администрирования

Теперь, когда вы успешно установили, настроили и протестировали систему Red Hat Linux на новой серверной платформе, самое время сосредоточиться на более сложных задачах, связанных с администрированием сервера. Корректное администрирование помогает обеспечить сохранение продуктивности и безопасности ваших серверов — следовательно, ваша задача состоит в разработке и внедрении политик безопасности, наилучшим образом подходящих для конкретной сетевой среды. В системах Linux в качестве пользователей могут выступать как живые люди (учетные записи, привязанные к физическому пользователю), так и логические пользователи (учетные записи, предназначенные для того, чтобы отдельные приложения могли выполнять определенные задачи). Пользователь, независимо от того, к какому из этих типов он принадлежит, располагает идентификатором пользователя (user ID, UID — как правило, он уникален) и идентификатором группы (group ID, GID). Для сравнения, группы представляют собой единицу логической организации в системе — они связывают пользователей друг с другом и предоставляют им права на чтение, запись или исполнение отдельно взятого файла. Каждый создаваемый файл присваивается тому или иному пользователю, той или иной группе. Для этого файла назначается два комплекта полномочий на чтение, запись и исполнение: один — для владельца файла и группы, к которым этот файл привязан, и второй — для всех остальных пользователей данного хоста. Впоследствии администратор (корневой пользователь) имеет право заменять пользователя и группу, связанных с конкретным файлом (а также полномочия, заданные по отношению к нему). В этой части главы рассматриваются основные административные задачи, как-то: создание новых пользователей и удаление старых, замена паролей и т. д.

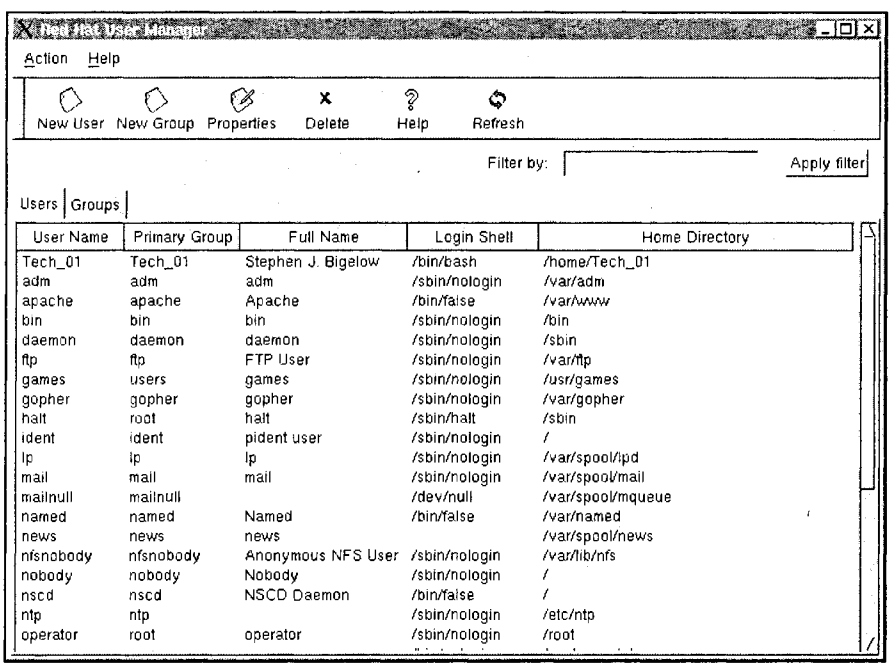
Пользовательские учетные записи

Администратор обязан иметь представление о таком понятии, как пользовательские учетные записи. Для того чтобы любой пользователь сети (в том числе администратор, которого еще называют корневым пользователем) смог получить доступ к серверной системе Linux, в этой системе у него должна быть пользовательская учетная запись. Пользовательская учетная запись определяет имя пользователя (под которым

он известен данной системе), его пароль, а также ряд других данных, характерных для этого пользователя. На сервере Linux предусмотрены графические средства, позволяющие создавать, сопровождать и удалять пользовательские учетные записи, затрачивая на это минимальные усилия.

Новые пользовательские учетные записи

Каждый раз, когда новый пользователь собирается приступить к работе в сети (либо ему нужен доступ к конкретной системе), вы должны создать для него новую пользовательскую учетную запись. Управление учетными записями осуществляется с помощью диспетчера Linux User Manager. Чтобы открыть User Manager, щелкните на логотипе **K**, расположенном в нижнем левом углу рабочего стола, и выберите команды меню **Red Hat, System, User Manager**. В результате откроется диалоговое окно **User Manager** (рис. 25.6). User Manager позволяет просматривать, редактировать, добавлять и удалять локальных пользователей и их группы. Для просмотра всех локальных пользователей, существующих в системе, перейдите на вкладку **Users**, а для получения списка всех локальных групп, созданных в системе, воспользуйтесь вкладкой **Groups**. Если вам требуется найти конкретного пользователя или группу, введите несколько первых букв нужного имени в поле **Filter by**, и нажмите клавишу <Enter> (или кнопку **Apply filter**). В результате будет сформирован отфильтрованный список. В табл. 25.1 представлен перечень стандартных пользователей (людей и процессов), устанавливаемых вместе с самой системой Linux.



User Name	Primary Group	Full Name	Login Shell	Home Directory
Tech_01	Tech_01	Stephen J. Bigelow	/bin/bash	/home/Tech_01
adm	adm	adm	/sbin/nologin	/var/adm
apache	apache	Apache	/bin/false	/var/www
bin	bin	bin	/sbin/nologin	/bin
daemon	daemon	daemon	/sbin/nologin	/sbin
ftp	ftp	FTP User	/sbin/nologin	/var/ftp
games	users	games	/sbin/nologin	/usr/games
gopher	gopher	gopher	/sbin/nologin	/var/gopher
halt	root	halt	/sbin/halt	/sbin
ident	ident	pident user	/sbin/nologin	/
lp	lp	lp	/sbin/nologin	/var/spool/lpd
mail	mail	mail	/sbin/nologin	/var/spool/mail
mailnull	mailnull		/dev/null	/var/spool/mqueue
named	named	Named	/bin/false	/var/named
news	news	news		/var/spool/news
nfsnobody	nfsnobody	Anonymous NFS User	/sbin/nologin	/var/lib/nfs
nobody	nobody	Nobody	/sbin/nologin	/
nscd	nscd	NSCD Daemon	/bin/false	/
ntp	ntp		/sbin/nologin	/etc/ntp
operator	root	operator	/sbin/nologin	/root

Рис. 25.6. Диалоговое окно **User Manager** позволяет вам администрировать пользователей и группы

Таблица 25.1. *Перечень стандартных пользователей Red Hat Linux 7.2*

Пользователь	Идентификатор пользователя	Идентификатор группы	Каталог	Оболочка
Adm	3	4	/var/adm	
Amanda	33	6	/var/lib/amanda/	
Apache	48	48	/var/www	
Bin	1	1	/bin	
Daemon	2	2	/sbin	
Ftp	14	50	/var/ftp	
Games	12	100	/usr/games	
Gdm	42	42	/var/gdm	
Gopher	13	30	/usr/lib/gopher-data	
Halt	7	0	/sbin	/sbin/halt
Ident	98	98	/	/sbin/nologin
Junkbust	73	73	/etc/junkbuster	
Ldap	55	55	/var/lib/ldap	
Lp	4	7	/var/spool/lpd	
Mail	8	12	/var/spool/mail	
Mailman	41	41	/var/mailman	
Mailnull	47	47	/var/spool/mqueue	
Mysql	27	27	/var/lib/mysql	
Named	25	25	/var/named	
News	9	13	/var/spool/news	
Nobody	99	99	/	
Nscd	28	28	/	
Operator	11	0	/root	
Piranha	60	60	/etc/sysconfig/ha	
Postgres	26	26	/var/lib/pgsql	
Pvm	24	24	/usr/share/pvm3	/bin/bash
Radvd	75	75	/	
Root	0	0	/root	/bin/bash
Rpc	32	32	/	
Rpcuser	29	29	/var/lib/nfs	

Таблица 25.1 (окончание)

Пользователь	Идентификатор пользователя	Идентификатор группы	Каталог	Оболочка
Rpm	37	37	/var/lib/rpm	
Shutdown	6	0	/sbin	/sbin/shutdown
Squid	23	23	/var/spool/squid	/dev/null
Sync	5	0	/sbin	/bin/sync
Uucp	10	14	/var/spool/uucp	
Wnn	49	49	/var/lib/wnn	
Xfs	43	43	/etc/X11/fs	

Чтобы добавить в систему нового пользователя, нажмите кнопку **New User**, расположенную в верхней части окна **User Manager**. В результате на экране появится диалоговое окно **Create New User** (рис. 25.7). Введите имя пользователя и полное имя владельца новой учетной записи в соответствующие поля. Пароль нового пользователя нужно ввести в поля **Password** и **Confirm Password** (длина пароля должна составлять по меньшей мере шесть символов — в нем имеет смысл задействовать сочетание букв, цифр и специальных символов). Теперь выберите регистрационную оболочку. Если вы не уверены в том, какую оболочку следует выбрать, согласитесь со значением, принимаемым по умолчанию — /bin/bash. Домашним каталогом, создаваемым по умолчанию, является /home/*<имя_пользователя>*, но вы, естественно, можете изменить его (если же вы решите, что создавать домашний каталог для данного пользователя излишне, снимите флажок **Create home directory**).

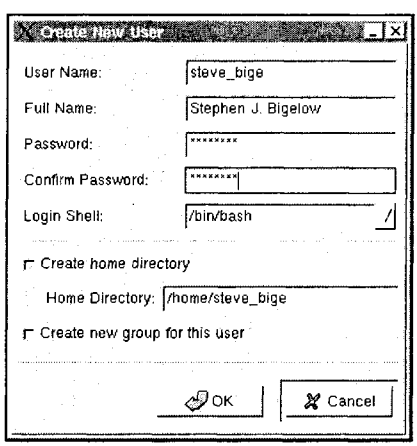


Рис. 25.7. В диалоговом окне **Create New User** вводятся подробные данные о новых пользовательских учетных записях

Кроме того, в Red Hat Linux реализована схема частных пользовательских групп (User Private Group, UPG). Она не вносит изменений в механизм управления груп-

пами, принятый в UNIX, а лишь предлагает новое соглашение. По умолчанию создание каждого нового пользователя сопровождается формированием уникальной группы, носящей его имя. Если вы не хотите создавать эту группу, снимите флажок **Create new group for this user**. Чтобы создать нового пользователя, нажмите кнопку **OK**. Чтобы сделать этого пользователя участником других пользовательских групп, перейдите на вкладку **User**, выберите в ней нужного пользователя, и нажмите кнопку **Properties**. В окне **User Properties** перейдите на вкладку **Groups**. Укажите группы, в которых данный пользователь, по вашему мнению, должен участвовать (более развернутая информация о распределении по группам будет представлена далее в этой главе).

Теневые пароли

Если вы работаете в рамках многопользовательской среды (но не пользуетесь сетевой схемой аутентификации наподобие Kerberos), имеет смысл задействовать теневые средства (их также называют теневыми паролями), которые смогут обеспечить дополнительную защиту аутентификационных файлов в вашей системе. На самом деле, по умолчанию файлы с паролями Linux делаются читаемыми — из-за этого профессиональные администраторы часто требуют применения теневых паролей, которые понижают степень уязвимости паролей. В ходе инсталляции Red Hat Linux защита средствами теневых паролей в вашей системе задействуется по умолчанию — равно как и пароли MD5 (еще один метод шифрования паролей для их хранения в системе). Теневые пароли предусматривают некоторые явные преимущества по сравнению с традиционными методами хранения, применяемыми в Linux/UNIX; они предоставляют, к примеру, следующие возможности:

- улучшенная система безопасности, помещающая зашифрованные пароли (которые обычно хранятся в каталоге /etc/passwd) в каталог /etc/shadow, чтение которого разрешено только корневому пользователю;
- предоставление данных о времени существования паролей (период времени с момента последнего изменения пароля);
- контроль над тем, как долго может существовать пароль, прежде чем пользователь обязан будет его поменять;
- способность задействовать файл /etc/login.defs в целях гарантированного исполнения политики безопасности — особенно в части сроков действия паролей.

Изменение пользовательских учетных записей

Со временем, по мере развития сети, вам придется обновлять различные пользовательские записи. Для этого откройте диалоговое окно **User Manager**, перейдите на вкладку **Users**, выберите нужного пользователя из списка **User**, и нажмите кнопку **Properties** (или выберите пункт **Properties** меню **Action**). В результате на экране появится диалоговое окно **User Properties** (рис. 25.8) — оно делится на четыре вкладки.

- **User Data.** Эта вкладка содержит основную информацию о пользователе, которая была введена еще при создании его учетной записи. При помощи этой вкладки можно менять полное имя пользователя, его пароль, домашний каталог и регистрационную оболочку.

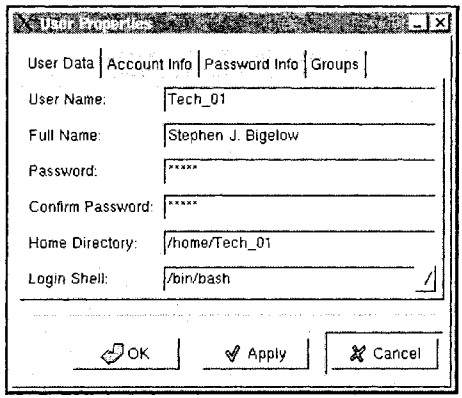


Рис. 25.8. С помощью диалогового окна **User Properties** можно изменить информацию о пользователе, его учетной записи, пароле и участии в группах

- **Account Info.** На этой вкладке содержится опция **Enable account expiration**, с помощью которой устанавливается окончание срока действия учетной записи в определенный день (дата завершения срока действия вводится в соответствующие поля). Для отключения учетной записи пользователя — с тем, чтобы он не имел возможности регистрироваться в системе — пометьте флажок **User account is locked**.
- **Password Info.** На этой вкладке приводится дата последнего изменения пользователем своего пароля. Чтобы заставить пользователя менять свой пароль по истечении заданного количества дней, пометьте флажок **Enable password expiration**. Кроме того, вы можете определить количество дней, на протяжении которых пользователь не будет иметь права менять свой пароль, количество дней до получения пользователем предупреждения о необходимости изменения своего пароля, и количество дней до того момента, когда учетная запись перестанет действовать.
- **Groups.** Эта вкладка позволяет выбрать группы, в которых будет участвовать пользователь. Вы можете сделать пользователя участником нескольких или всех групп, хотя с точки зрения безопасности обычно это не целесообразно.

Удаление учетных записей

Обычно, когда пользователь увольняется из организации или переходит работать за пределы вашего домена, его неиспользуемую учетную запись удаляют. Это уменьшает суету (администратору придется координировать меньше учетных записей), а уровень защиты повышается — лишенные прав бывшие сотрудники теряют возможность последующей регистрации в системе или передачи своей регистрационной информации сторонним, неуполномоченным пользователям. Чтобы удалить пользователя, откройте User Manager, перейдите на вкладку **Users**, выберите пользователя, которого собираетесь удалить, и нажмите кнопку **Delete**. В зависимости от того, какая версия Linux установлена на вашей машине, система, возможно, спросит вас, что делать с данными пользователя (заархивировать их, удалить или оставить нетронутыми). Если вы предполагаете, что рабочие файлы пользователя вам понадобятся,

оставьте их. Если пользователь может вернуться, заархивируйте данные (или просто отключите его учетную запись). В других обстоятельствах следует удалить данные и тем самым увеличить объем свободного дискового пространства.

Группы пользователей

Linux работает не совсем так, как другие операционные системы типа Windows. Там, где Windows проводит явное различие между пользователями и группами, Linux старается несколько размыть эту границу — в основном, потому, что пользовательские учетные записи часто связываются с соответствующей группой. К примеру, в соответствии с настройками по умолчанию, создание пользователя под названием pwruser1 приводит к формированию для него группы pwruser1 (если только в процессе создания учетной записи вы не снимите флажок **Create new group for this user**). В условиях, когда для каждого пользователя автоматически создается новая группа, велика вероятность того, что за очень короткий период времени список сделается слишком громоздким.

Создание группы

Как бы то ни было, Linux предусматривает возможность создания и координации уникальных групп с помощью диалогового окна **User Manager** (как показано на рис. 25.6). Чтобы просмотреть перечень всех существующих групп, перейдите на вкладку **Groups**. Как и в случае с пользователями, существует набор стандартных групп, которые формируются в процессе инсталляции Linux. В табл. 25.2 эти стандартные группы приводятся в том виде, в котором они перечислены в файле /etc/group. Чтобы добавить новую группу, нажмите кнопку **New Group**. В результате появится диалоговое окно **Create New Group** с приглашением на ввод имени группы. Укажите имя новой группы, а затем нажмите кнопку **OK** — в результате созданная группа будет помещена в список групп.

Таблица 25.2. *Перечень стандартных групп Red Hat Linux 7.2*

Группа	Идентификатор группы	Участники
Adm	4	root, adm, daemon
apache	48	apache
bin	1	root, bin, daemon
daemon	2	root, bin, daemon
dip	40	
disk	6	root
floppy	19	
ftp	50	
games	20	
gdm	42	gdm

Таблица 25.2 (продолжение)

Группа	Идентификатор группы	Участники
gopher	30	
ident	98	ident
junkbust	73	junkbust
kmem	9	
ldap	55	ldap
lp	7	daemon, lp
mail	12	mail
mailman	41	mailman
mailnull	47	mailnull
man	15	
mem	8	
mysql	27	mysql
named	25	named
news	13	news
nobody	99	
nscd	28	nscd
piranha	60	piranha
popusers	45	
postgres	26	postgres
pppusers	44	
pvm	24	pvm
root	0	root
rpc	32	rpc
rpcusers	29	
rpm	37	rpm
slipusers	46	
slocate	21	
squid	23	squid
sys	3	root, bin, adm
tty	5	
users	100	

Таблица 25.2 (окончание)

Группа	Идентификатор группы	Участники
utmp	22	
uucp	14	uucp
wheel	10	root
wnn	49	wnn
xfs	43	xfs

Чтобы просмотреть свойства существующей группы, выделите ее запись в списке **Group** и нажмите кнопку **Properties** (или выберите пункт **Properties** меню **Actions**). В результате появится диалоговое окно **Group Properties**. На вкладке **Group Data** лишь приводится имя группы (которое при необходимости можно изменить). На вкладке **Group Users** (рис. 25.9) перечисляются пользователи, являющиеся участниками данной группы. Чтобы добавить в группу новых пользователей, пометьте флажки, расположенные рядом с их именами; напротив, для удаления пользователей снимите соответствующие флажки. Чтобы принять изменения состава пользователей выбранной группы, нажмите кнопку **OK** или **Apply**; затем убедитесь в том, что нужные пользователи действительно присоединены к группе, сверяясь со списком **Group**. Наконец, вы можете удалить группу, в существовании которой более нет необходимости. Перейдя на вкладку **Groups** в User Manager, выберите группу, которую предполагаете удалить, и нажмите кнопку **Delete**.

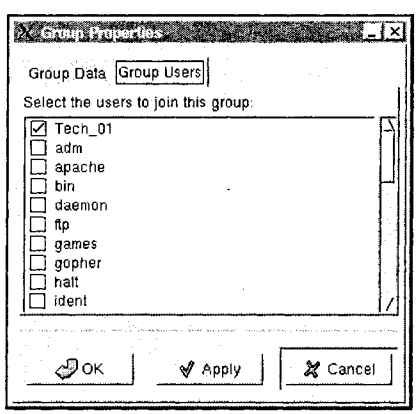


Рис. 25.9. При помощи окна **Group Properties** пользователи делаются участниками одной или нескольких групп

Совместно используемые ресурсы в Linux

После того как сервер Linux заработал в вашей сети, обычно возникает желание настроить другие сетевые компьютеры, чтобы они смогли обращаться к файлам и

принтерам через сеть. В случае применения Linux, для того чтобы организовать совместное использование файлов и принтеров через сетевое соединение, вам придется задействовать утилиту Samba (с помощью протокола SMB). Samba особенно полезна, если в вашей сети сосуществуют машины, на одной части которых установлены операционные системы Windows, а на другой — Linux. Samba позволяет задействовать совместное использование файлов и принтеров всеми системами, присутствующими в сети, хотя процесс, который для этого нужно пройти, оказывается сложнее, чем создание коллективных ресурсов в системах Windows. К примеру, если в вашей системе есть учетная запись Tech_01, расположенная в принятом по умолчанию каталоге /home/Tech_01, то с помощью файла smb.conf вы можете определить этот "каталог" как совместно используемый ресурс.

Примечание

"Коллективные ресурсы" Linux могут приводить в замешательство — особенно в том случае, если вы привыкли к незамысловатости совместного использования файлов и каталогов в системах Windows. Linux не предусматривает тех "совместно используемых ресурсов", которые существуют в Windows. Приведенные здесь данные — это лишь краткий обзор общих ресурсов Linux. В документации по Linux содержится намного больше информации, связанной с применением Samba для подключения машин Linux к сети Windows. Для получения более подробных сведений об утилите Samba посетите сайт **www.redhat.com/support/resources/print_file/samba.html**. Для организации совместного использования ресурсов исключительно между системами Linux применения Samba не требуется.

Обновление файла SMB.CONF

В качестве конфигурационного файла Samba выступает /etc/samba/smb.conf. После внесения изменений в этот конфигурационный файл они не вступят в силу, пока вы не выполните перезапуск демона Samba — это делается при помощи команды `service smb restart`. Конфигурационный файл, принимаемый в Red Hat Linux 7.2 по умолчанию (smb.conf), позволяет пользователям просматривать содержимое своих домашних каталогов Linux в виде коллективного ресурса Samba, работая на машинах Windows и зарегистрировавшись с помощью своего имени пользователя и пароля. Кроме того, он организует совместное использование всех принтеров, настроенных в системе Red Hat Linux как коллективные принтеры Samba; таким образом, вы можете подключить принтер к системе Red Hat Linux, и отправлять на него задания с любой машины Windows, работающей в сети. Чтобы определить рабочую группу Windows и строку описания, введите в файл smb.conf следующие строки:

```
workgroup = ИМЯ_РАБОЧЕЙ_ГРУППЫ
server string = КРАТКОЕ ПРИМЕЧАНИЕ О СЕРВЕРЕ
```

Замените `ИМЯ_РАБОЧЕЙ_ГРУППЫ` именем рабочей группы Windows, к которой должна принадлежать данная машина Linux. Запись `КРАТКОЕ ПРИМЕЧАНИЕ О СЕРВЕРЕ` является факультативной; она определяет комментарий Windows о системе Samba. Чтобы создать коллективный каталог Samba в системе Linux, отредактируйте секцию `Shares` файла smb.conf так, как показано на рис. 25.10. Это позволит сделать коллективный ресурс Tech_01, находящийся в каталоге /home/Tech_01, общедоступным для всех участников сети.

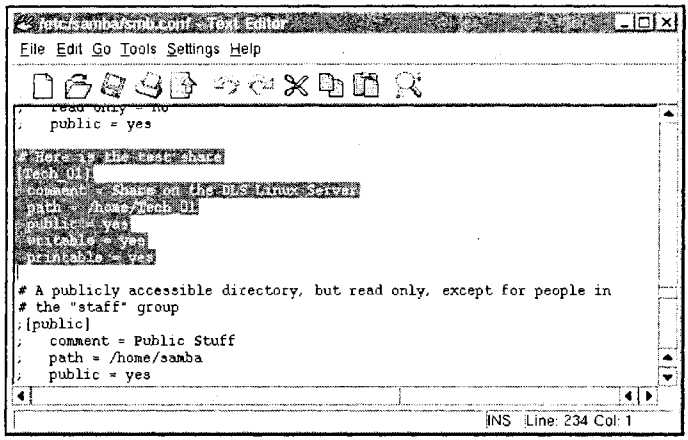


Рис. 25.10. Пример обновления файла smb.conf, направленного на создание коллективного ресурса Linux средствами утилиты Samba

Подключение из Linux

Чтобы подключиться к коллективному ресурсу Samba из системы Linux, введите в строке оболочки следующую команду:

```
smbclient //имя_хоста/имя_коллективного_ресурса -U имя_пользователя
```

Необходимо заменить `имя_хоста` именем хоста или IP-адресом сервера Samba, к которому вы намерены подключиться, `имя_коллективного_ресурса` — именем совместно используемого каталога, к которому вы собираетесь обратиться, а `имя_пользователя` — именем пользователя Samba в этой системе. Введите точный пароль (или, если для данного имени пользователя указания пароля не требуется, нажмите клавишу <Enter>). Появление строки `smb:\>` означает, что ваша регистрация прошла успешно. При желании обратиться к содержимому вашего собственного домашнего каталога, замените `имя_коллективного_ресурса` вашим именем пользователя. Если ключ `-U` не используется, имя текущего пользователя передается серверу Samba. Чтобы выйти из `smbclient`, введите в строке `smb:\>` команду `exit`.

Подключение из Windows 9x

После того как вы сформировали в системе Linux коллективный ресурс, безошибочно отредактировали файл smb.conf и перезапустили службу `smb`, в каталогах **Network Neighborhood** (Сетевое окружение) клиентов Windows 9x должно появиться имя сервера Linux. Чтобы открыть доступные общие ресурсы, просто перейдите на этот сервер. Имейте в виду, что перед обращением к этим ресурсам от вас может потребоваться ввод пароля. Если вы предпочитаете, чтобы общий ресурс обозначался именем дисковода (например, e:, f: и т. д.), щелкните на нем правой кнопкой мыши, и для выбора имени дисковода выберите пункт **Map Network Drive** (Подключить сетевой диск). Кроме того, вы можете определить, нужно ли проводить повторное подключение каждый раз при регистрации в Windows. Если вы не хотите заходить в каталог Network Neighborhood каждый раз, когда необходимо обратиться к этому

общему ресурсу (и не намерены присваивать ему имя дисковода), перетащите его пиктограмму на рабочий стол.

Пароли в Windows NT/2000

Хотя машины Windows NT/2000 допускают простое обращение к коллективным ресурсам Linux через каталог My Network Places, различия в схеме парольной защиты между Linux и Windows NT/2000 заставляют технических специалистов решать проблемы совместимости. Протокол Microsoft SMB первоначально предусматривал передачу паролей в открытом тексте, однако в Windows 2000 и Windows NT 4.0 (начиная с Service Pack 3) требуется применение зашифрованных паролей Samba. Чтобы сделать возможным использование Samba для взаимодействия систем Red Hat Linux и Windows NT/2000, вы можете либо отредактировать реестр Windows и разрешить передачу паролей в открытом тексте, либо настроить Samba в системе Linux на режим зашифрованных паролей. Если вы решите внести изменения в реестр, это нужно будет сделать на всех машинах Windows NT/2000 — таким образом, вы столкнетесь со сложной и трудоемкой проблемой. Чтобы настроить утилиту Samba в системе Red Hat Linux на применение зашифрованных паролей, выполните следующие операции с помощью командной строки.

1. Создайте для Samba отдельный файл хранения паролей. К примеру, чтобы создать его на основе существующего файла /etc/passwd, введите следующую команду:

   ```
   cat /etc/passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
   ```

2. Сценарий mksmbpasswd.sh устанавливается в каталоге /usr/bin вместе с пакетом Samba. Теперь, для изменения прав доступа к файлу с паролями Samba такого, чтобы операции чтения и записи мог проводить только корневой пользователей, введите следующую команду:

   ```
   chmod 600 /etc/samba/smbpasswd
   ```

3. Этот сценарий не выполняет копирования в новый файл пользовательских паролей. Чтобы установить пароли каждого пользователя Samba, введите следующую команду (заменив `username` именем каждого отдельного пользователя):

   ```
   smbpasswd username
   ```

4. Пользовательская учетная запись Samba не вступит в действие, пока вы не определите для нее пароль Samba. Следующим этапом будет разрешение зашифрованных паролей в конфигурационном файле Samba. Для этого нужно снять комментарии со следующих строк файла smb.conf:

   ```
   encrypt password = yes
   smb passwd file = /etc/samba/smbpasswd
   ```

5. Чтобы ввести изменения в действие, перезапустите Samba — для этого наберите в строке оболочки команду `service smb restart`.

Примечание

Для выполнения этих процедур требуется знание интерфейса командной строки Linux. За описанием отдельных команд и подробной информацией обращайтесь к документации по Linux.

Дополнительные ресурсы

Caldera Linux: **www.caldera.com**.

Kerberos: **web.mit.edu/kerberos/www**.

Linux: **www.linux.org**.

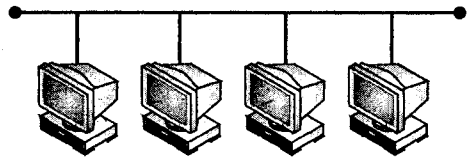
NSA: **www.nsa.gov**.

Red Hat Linux: **www.redhat.com**.

Советы по применению Samba:
www.redhat.com/support/resources/tips/Samba-Tips/Samba-Tips.html.

SANS: **www.sans.org**.

SuSe Linux: **www.suse.com/index_us.html**.



ГЛАВА 26

Поиск и устранение неисправностей при регистрации в сети

Когда пользователь испытывает трудности при попытке регистрации в компьютерной сети, он испытывает особенно неприятные ощущения. Проблема может оказаться совершенно элементарной, например у него нет полномочий на применение цветного принтера, или представлять собой нечто более хитрое — например, отсутствие возможности зарегистрироваться на каком-либо устройстве.

Но проблемы, возникающие при регистрации, приводят не только к потере пользователем времени и хорошего настроения. По данным исследования, проведенного Консорциумом по применению сетей (Network Applications Consortium, NAC), 70 процентов своего времени администратор тратит на восстановление потерянных или забытых паролей.

В этой главе освещены вопросы, связанные с сетевой регистрацией в средах Windows, NetWare и UNIX/Linux. В дополнение к основным проблемам регистрации, здесь рассматриваются принципы управления правами и полномочиями пользователей и методы их администрирования.

Регистрация в Windows

В разнообразных вариантах Windows предусмотрены всевозможные средства регистрации, управления правами пользователей, их полномочиями и учетными записями. Кроме того, для формирования определенных рабочих условий для пользователей и групп, в которые они объединяются, могут использоваться сценарии.

В этом разделе вы ознакомитесь с процессом регистрации в среде Windows и методиками его управления. Помимо этого, здесь освещена тема управления правами и полномочиями пользователей.

Служба NetLogon

В среде Windows клиенты пользуются службой NetLogon для установления соединения с серверами NT, 2000 и .NET. Применение этой службы совершенно необходимо при попытке регистрации в домене. Процесс регистрации здесь рассматривается с точки зрения тех действий, которые производятся на клиентской и серверной машинах Windows.

Клиенты

На клиентских машинах Windows пользовательские запросы на регистрацию обрабатываются локальными средствами защиты (Local Security Authority, LSA); если в локальной базе данных пользовательских учетных записей не удается обнаружить соответствие предоставленной записи, LSA передает запрос службе NetLogon, которая, в свою очередь, перенаправляет запрос контроллеру домена. Служба NetLogon в системах NT Server передает такие запросы в базу данных защищенных доменных каталогов, или, если запрошенные ресурсы расположены в другом домене, пропускает их через находящийся в этом домене контроллер.

Служба NetLogon требует работы служб Workstation и Server. При подключении клиентов NT Workstation, настроенных на автономную или групповую работу, необходимо быть уверенным в том, что конфигурация этих служб предусматривает автоматический запуск. Проверить эти настройки можно при помощи окна **Services** (Службы) Панели управления (Control Panel). Кроме того, эта служба требует наличия права доступа к данному компьютеру из сети (**Access this Computer from Network**), которое устанавливается в User Manager. Имейте в виду, что настройки этого права, принимаемые по умолчанию, предполагают всеобщее разрешение доступа к данному компьютеру. Это означает, что любой пользователь домена, работая за клиентской машиной, может зарегистрироваться в домене.

Прежде чем служба NetLogon сможет проводить эти операции, она должна найти соответствующую машину (или, как в случае со службой NetLogon в NT Server, машины). Этот процесс называется обнаружением (discovery), а запускается он одновременно с включением данной службы при загрузке системы. Клиентская служба NetLogon попытается "обнаружить" службу NetLogon машины NT Server. Если оказывается, что полученное имя пользователя и пароль присутствуют в базе данных безопасности, между машинами устанавливается защищенный канал связи. Если процесс обнаружения оканчивается неудачей, служба NetLogon данного клиента задействует кэшированные данные пользователя, созданные во время предыдущей регистрации. Таким образом, пользователь регистрируется на клиентской машине и получает локальные полномочия, существовавшие на момент последней регистрации.

Если процесс обнаружения прошел успешно, но пользовательской учетной записи на сервере выявлено не было, возможны два варианта.

- Если гостевые (Guest) учетные записи включены, а гостевой пароль не установлен, пользователь будет зарегистрирован как гость (Guest); в противном случае попытка регистрации завершится неудачей.
- Если клиент Windows NT пытается зарегистрироваться на резервном контроллере домена (Backup Domain Controller, BDC), то служба NetLogon BDC проводит процесс аутентификации через основной контроллер домена (Primary Domain Controller, PDC), если последний доступен. Так происходит в тех случаях, когда пароль пользователя был изменен на PDC, но дублирование этого изменения на BDC выполнено не было (подробнее об этом — в *разд. "Контроллеры доменов"*). В такой ситуации PDC разрешает регистрацию.

Примечание

При обращении к сетевым ресурсам клиентов, работающих не на клиентских или серверных машинах Windows, их аутентификация производится службами NetLogon

на соответствующих контроллерах доменов. Тем не менее никаких ограничений по доступу к локальным ресурсам для таких клиентов не существует.

Контроллеры доменов

Служба NetLogon на контроллерах доменов отвечает на запросы аутентификации, исходящие от клиентов этих доменов, а также устанавливает защищенные каналы связи со всеми прочими контроллерами доменов, с которыми у них есть доверительные отношения. При запуске доменная служба NetLogon пытается выполнить процедуру обнаружения всех доверенных доменов. При необходимости во время запуска в течение 5 секунд производится троекратный опрос каждого домена. Если в течение этого временного периода процесс обнаружения не приводит к результату, контроллер домена повторяет попытку каждый раз при получении запроса на аутентификацию от клиента, требующего предоставления доступа к ресурсам, расположенным за пределами данного домена. Если таких запросов не поступает, контроллер повторяет попытку обнаружения каждые 15 минут.

В системе NT Server эта служба принимает от клиентов запросы на аутентификацию и, при необходимости, передает их доверенным серверам, расположенным в других доменах. Это касается как регистрационной аутентификации, так и запросов на обращение к ресурсам (файлам или принтерам). Если зарегистрированный пользователь стремится подключить сетевой диск, находящийся вне данного домена, служба NetLogon PDC передает такой запрос основному контроллеру домена или (при использовании Active Directory) контроллеру доверенного домена. Если имя пользователя и пароля совпадают с записью базы данных безопасности этого домена, запрос выполняется. В случае отказа сервер предлагает пользователю повторно ввести имя и пароль, тем самым предоставляя возможность доступа, если у пользователя есть две учетных записи в разных доменах, или если он знает имя пользователя и пароль действительной учетной записи в данном домене.

Кроме того, служба NetLogon ответственна за синхронизацию базы данных безопасности между отдельными контроллерами доменов. Изменения пользовательских или групповых учетных записей (например, их паролей, членства в группах, полномочий групп или пользователей) заносятся в журнал изменений (он хранится в памяти и на диске *%Systemroot%*\Netlogon.chg). По умолчанию размер файла этого журнала равен 64 Кбайт; и как только он наполняется, новые изменения начинают вытеснять самые старые.

Windows 2000 и Kerberos

В системе Windows 2000 реализован дополнительный уровень защиты, связанный с регистрацией пользователя. Когда пользователь пытается зарегистрироваться на рабочей станции Windows 2000, активизируется протокол системы защиты Kerberos. По существу, процесс регистрации состоит из следующих этапов (проиллюстрированных на рис. 26.1):

1. *Пользователь отправляет запрос на допуск к службе выдачи сертификатов данного домена.* Для выполнения этой задачи между источником обеспечения безопасности (Security Support Provider, SSP) Kerberos на клиентской машине и центром распространения ключей (Key Distribution Center, KDS) Kerberos на контроллере домена происходит обмен данными службы аутентификации (Authentication Service,

AS). Если этот процесс проходит успешно, пользователь получает сертификат для получения сертификата (Ticket-Granting Ticket, TGT), который может задействоваться при последующих процедурах регистрации.

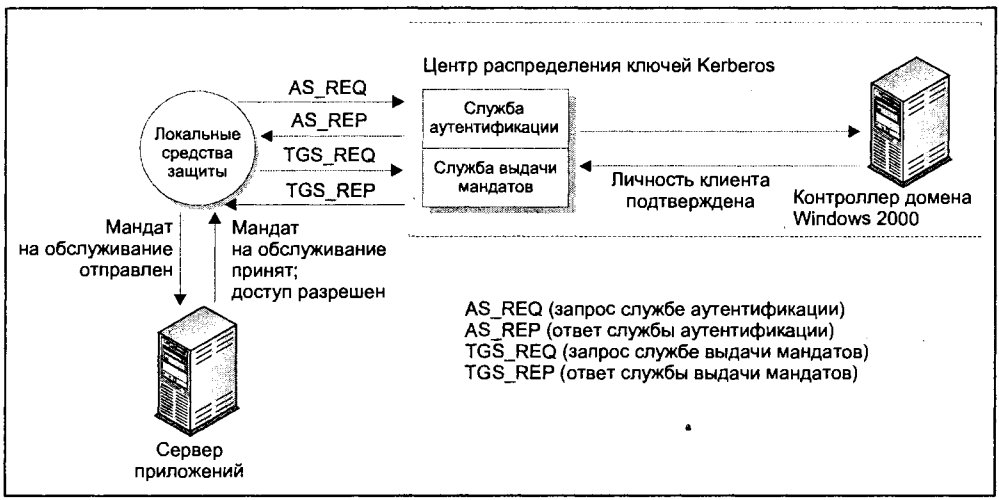


Рис. 26.1. Процесс регистрации в системе Windows 2000 с Kerberos

2. *Пользователь отправляет запрос на получение сертификата на компьютер.* Между Kerberos SSP на клиентской машине и KDC в учетном домене пользователя происходит обмен данными службы выдачи сертификатов (Ticket Granting Service, TGS). Результатом является предоставление пользователю сертификата, который он может предъявить, запрашивая разрешение на доступ в сеть.
3. *Пользователь отправляет запрос локальным системным службам на компьютере.* На завершающем этапе Kerberos SSP предоставляет локальным средствам защиты (Local Security Authority, LSA) клиентского компьютера сеансовый сертификат. Если этот компьютер и пользователь находятся в разных доменах, необходимо выполнение еще одного этапа. Прежде чем запрашивать сертификат на данный компьютер, Kerberos SSP должен сначала запросить у KDC учетного домена пользователя сертификат (TGT), подходящий для предъявления центру KDC учетного домена искомого компьютера. Затем SSP предъявляет TGT центру KDS и получает сеансовый сертификат на обращение к нужному компьютеру.

Вопросы политики учетных записей

В Windows NT для управления конфигурациями пользователей и компьютера, хранящимися в базе данных реестра NT, администраторы пользуются сервисной программой System Policy Editor. При помощи System Policy Editor создаются системные политики, контролирующие рабочую среду пользователя и его действия и реализующие настройки конфигурации на всех компьютерах с системами NT.

В Windows 2000/XP/.NET для аналогичных целей задействуется оснастка Group Policy консоли управления (Microsoft Management Console, MMC); она усовершенст-

вована по сравнению с System Policy Editor и обеспечивает лучшее соответствие определениям пользовательских и компьютерных конфигураций для пользователей и их групп. Групповые политики определяют компоненты пользовательской среды, которыми должны управлять системные администраторы, например, настройки политик, связанные с опциями защиты, размещением программ и сценариями.

Расширения оснастки Group Policy

Оснастка Group Policy содержит несколько встроенных расширений. Они раскрываются в узлах **User Configuration** (Конфигурация пользователя) и **Computer Configuration** (Конфигурация компьютера), в их подузлах **Windows Settings** (Конфигурация Windows) и **Software Settings** (Конфигурация программ)[1]. Как правило, они расширяют оба этих элемента, но по большей части — с разными опциями. В следующем списке приводятся встроенные расширения, входящие в Windows 2000.

- *Административные шаблоны* (Administrative Templates). Содержит основанные на реестре настройки политики, предназначенные для управления настройками реестра, которые отвечают за внешний вид и функциональность рабочего стола. Помимо этого, координирует дисковые квоты и функции удаленной инсталляции.
- *Параметры безопасности* (Security Settings). Это расширение устанавливает конфигурации систем безопасности на компьютерах в рамках объекта Group Policy. У вас есть возможность задать настройки безопасности локального компьютера, домена и сети.
- *Конфигурация программ* (Software Installation). Предназначено для координации распределения программных средств в рамках вашей организации.
- *Сценарии* (Scripts). Применяются в целях автоматизации запуска и отключения компьютера, а также регистрации в сети и выхода из нее.

Создание собственной оснастки Group Policy

Вы можете создать свою собственную групповую политику, содержащую выборку из расширений оснастки Group Policy. К примеру, можно создать встраиваемый компонент, который будет использовать только расширение Software Installation. Эта возможность позволяет заложить в создаваемую консоль установочные параметры по модульному принципу. Затем необходимо определить пользователей и группы, которым вы разрешите обращаться к объекту групповой политики (Group Policy Object, GPO), и связанное с ним местоположение в Active Directory.

Чтобы запустить Group Policy как автономную оснастку, выполните следующие шаги:

1. Выберите последовательно команды **Start, Run** (Пуск, Выполнить), введите код `MMC` и нажмите клавишу <Enter>.
2. В меню **Console** (Консоль) окна **MMC** (Консоль 1) выберите пункт **Add/Remove Snap-in** (Добавить/удалить оснастку).
3. Находясь на вкладке **Standalone** (Изолированная оснастка), нажмите кнопку **Add** (Добавить).

---

[1] Третьим подузлом является Administrative Templates. — *Ред.*

4. Находясь в диалоговом окне **Add Snap-in** (Добавить изолированную оснастку), выберите **Group Policy** (Групповая политика) и нажмите кнопку **Add** (Добавить).
5. Чтобы найти GPO, которым вы предполагаете управлять, нажмите кнопку **Browse** (Обзор), расположенную в диалоговом окне **Select Group Policy object** (Выбор объекта групповой политики).
6. Завершив выбор, вернитесь в диалоговое окно **Add/Remove Snap-in**.
7. Перейдите на вкладку **Extensions** (Расширения) и выберите расширения оснастки, которыми вы предполагаете пользоваться.
8. Нажмите кнопку **OK**. После этого откроется интегрируемое приложение Group Policy, в котором фокус будет наведен на указанный объект GPO.
9. Выбрав политики, которые вы предполагаете задействовать, выполните пункт **Save As** (Сохранить как) меню **Console** — так вы сможете сохранить выполненные настройки (сохраненный файл должен иметь расширение msc).

Чтобы установить полномочия доступа, перейдите на вкладку **Security** (Безопасность) страницы свойств (**Properties**) выбранного объекта GPO. Эти полномочия разрешают или запрещают возможность доступа к GPO со стороны заданных групп.

Права пользователя

Как только в среду Windows добавлен новый пользователь, ему можно незамедлительно назначить разнообразные права. В результате процесс создания новых пользовательских записей упрощается — набор прав и полномочий можно определить сразу; после этого пользователю остается лишь задействовать их.

Создание пользователей

Чтобы создать новую пользовательскую учетную запись в системе Windows 2000, выберите последовательно команды **Start, Administrative Tools, Computer Management** (Пуск, Администрирование, Управление компьютером). Выберите запись **Users** (Пользователи) в группе **Local Users and Groups** (Локальные пользователи и группы) дерева консоли. Нажмите кнопку **Action** (Действие); затем — кнопку **New User** (Новый пользователь).

Создание новой пользовательской учетной записи в среде Windows NT происходит аналогичным образом, но вместо сервисной программы Computer Management там применяется User Manager (Управление пользователями).

После этого введите все необходимые данные в диалоговое окно, изображенное на рис. 26.2 (оно применяется в системах Windows 2000 и XP, но в среде Windows NT искомая информация аналогична).

Пометьте или снимите флажки, соответствующие следующим настройкам:

- ❒ потребовать смену пароля при следующем входе в систему;
- ❒ запретить смену пароля пользователем;
- ❒ срок действия пароля не ограничен;
- ❒ отключить учетную запись.

Рис. 26.2. В диалоговом окне **New User** указываются данные об экранном имени пользователя и его реальном имени, а также опции, связанные с паролем

Чтобы создать еще одного пользователя, нажмите кнопку **Create** (Создать), и выполните вышеизложенный процесс еще раз. В противном случае, чтобы завершить действия по формированию новой пользовательской учетной записи, нажмите кнопку **Create**, а затем — кнопку **Close**.

Примечание

Имя пользователя не может быть идентичным любому другому имени пользователя или группы, существующем на компьютере, который вы администрируете. В нем может содержаться до 20 символов (в нижнем или верхнем регистре), кроме следующих:

```
"/\[];:|=,+*?<>
```

Кроме того, имя пользователя не может состоять исключительно из точек или пробелов.

В среде NT в сервисной программе User Manager (Управление пользователями) содержатся три редактора политик — они расположены в меню **Policies** и называются Account (Политики учетных записей), User Rights (Назначение прав пользователя) и Audit (Политика аудита). Они же присутствуют в оснастке Security Policy (Параметры безопасности) системы Windows 2000. Их назначение заключается в формировании однородной среды для пользователей, а также в учреждении некоторых средств защиты против слабых паролей, несанкционированных попыток регистрации и полномочий, присваиваемых пользователям по незнанию.

Редактор политики учетных записей, изображенный на рис. 26.3 (в данном случае приводится интерфейс Windows XP) позволяет получать полный контроль над свойствами паролей пользователей и возможность блокировки учетных записей всех пользователей, расположенных в данном домене. Критерии паролей можно устанав-

ливать исходя из их длины; кроме того, у вас есть возможность принуждать пользователей к смене их паролей по прошествии определенного периода времени. Более того, можно даже запретить повторное применение паролей на протяжении установленного периода предыстории. Блокировка учетных записей, как правило, применяется для отключения учетной записи после ряда неуспешных попыток регистрации. По существу, это является мерой защиты, способной предотвратить многократное повторение попыток угадывания паролей со стороны неуполномоченных пользователей. Настройки, устанавливаемые в отношении критериев паролей и блокировки учетных записей, обуславливаются тем, насколько надежен уровень защиты, который вы хотите применить к пользователям.

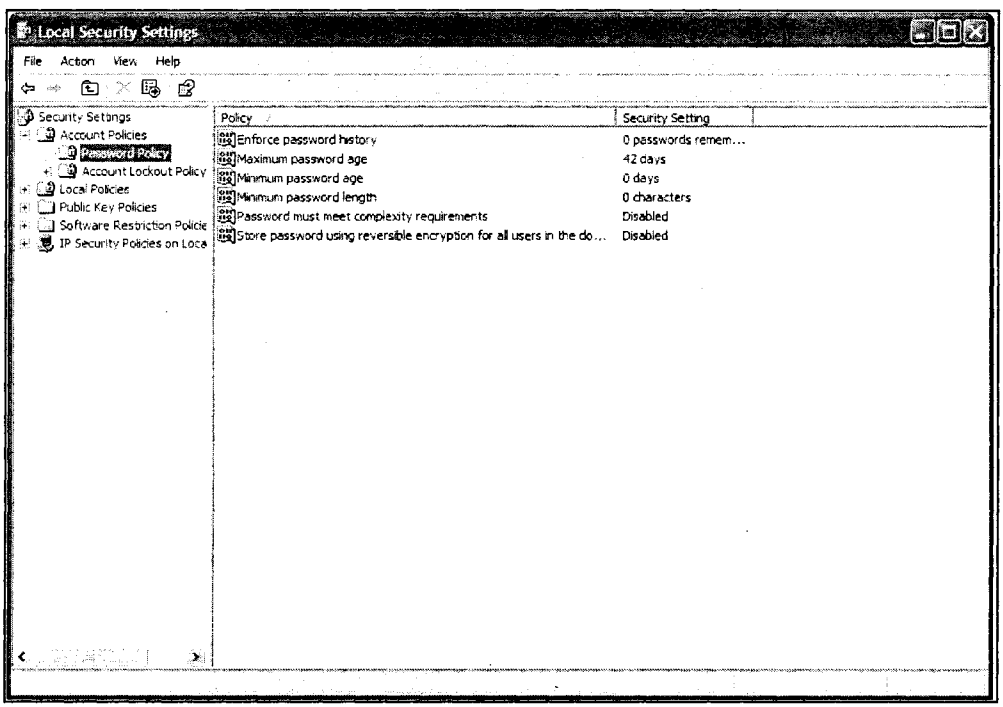


Рис. 26.3. В редакторе политик Account устанавливаются регистрационные политики для всех пользователей

Редактор политик User Rights (Назначение прав пользователя) предусматривает более точный контроль над тем, какими правами может обладать пользователь или группа. В системе Windows NT при выборе опции **Show Advanced User Rights** (Показать расширенные права пользователей) появляется список, состоящий более чем из 20 прав в диапазоне от простых (связанных, например, с возможностью изменения настроек времени) до более расплывчатых — к примеру, там упоминается возможность создания маркерного объекта. Скажем, на рис. 26.4 (где приводится снимок из системы Windows XP) право локальной регистрации на машине предоставляется Администраторам (Administrators), Операторам архива (Backup Operators), Гостям (Guests), Опытным пользователям (Power Users) и Пользователям (Users). Вы можете

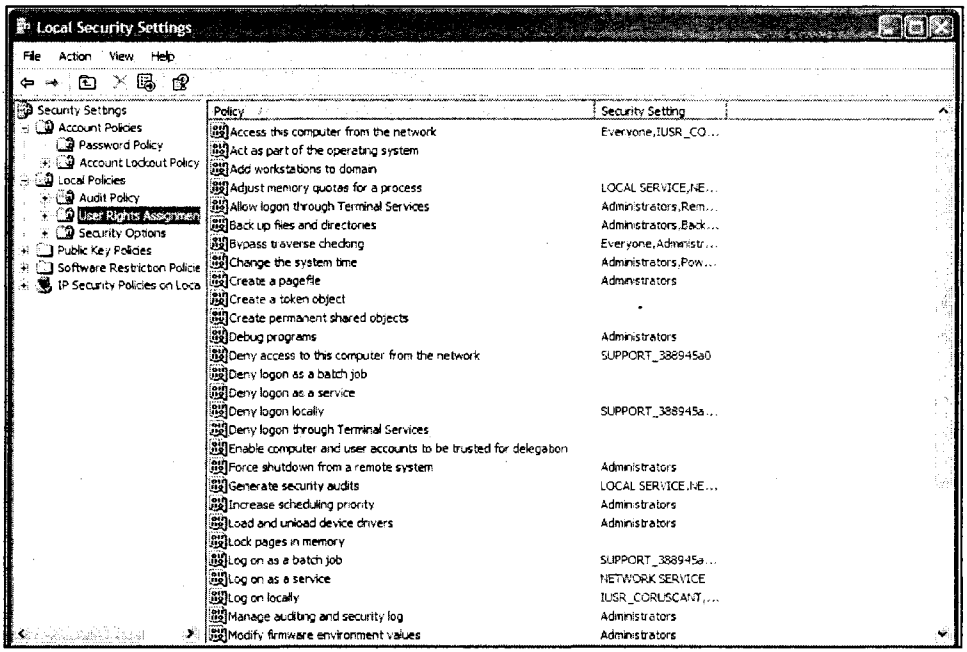


Рис. 26.4. С помощью редактора политик Rights Assignment пользователям и их группам назначаются конкретные права

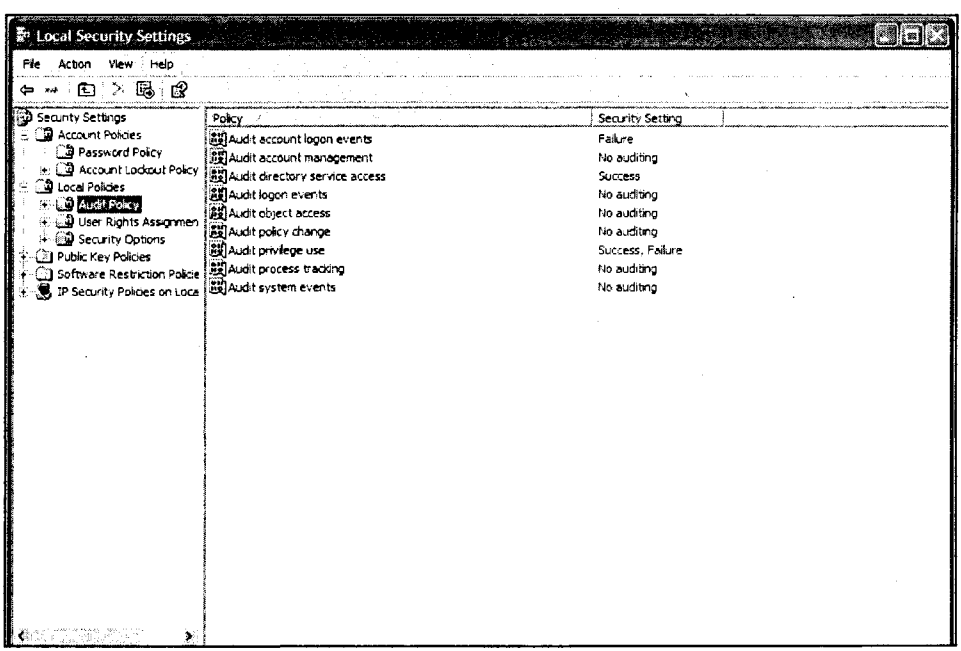


Рис. 26.5. В редакторе политик Audit указываются события, которые нужно регистрировать

запросто добавлять или удалять группы и пользователей, но при этом нужно осознавать последствия подобных действий — многие полномочия, возможно, не покажутся вам важными с точки зрения работоспособности учетной записи, но после их удаления может оказаться, что это именно так. Удаляя существующие полномочия и назначая новые, соблюдайте осторожность: результаты не всегда соответствуют ожиданиям!

Так как функцией политики аудита (Audit) является указание *системных* событий, сохраняемых в журнале безопасности, в контексте управления *пользователями* (User Manager) она кажется неуместной. Просмотр журнала безопасности производится с помощью оснастки Event Viewer (Просмотр событий) в составе группы **Administrative Tools** (Администрирование). На рис. 26.5 представлен графический пользовательский интерфейс, предназначенный для отбора событий, подлежащих аудиту. Изображение, приведенное на рис. 26.5, взято из Windows XP, но в других версиях Windows эта сервисная программа выглядит аналогично. Отсюда производится управление аудитом неуспешных попыток регистрации, успешных обращений к службам каталогов и всех вариантов проверяемых полномочий. При поиске способов устранения системных неисправностей и в процессе выявления потенциальных злоумышленников эта информация может оказаться довольно полезной.

Профили пользователя

Многие трудности, связанные с регистрацией, могут устраняться при помощи профилей пользователей. Эти настройки создаются для каждого пользователя, который впервые регистрируется на данном компьютере. Профили пользователей содержат более подробные (по сравнению с системными политиками) данные о пользовательском окружении. Они позволяют настраивать пользовательские рабочие столы таким образом, что любые вносимые ими изменения возобновляются при следующей регистрации. Если у пользователя есть перемещаемый профиль, такие настройки "преследуют" его на всех сетевых компьютерах, на которых он регистрируется — таким образом, обеспечивается устойчивость условий работы пользователя. Если администратор решает, что при каждой регистрации пользователя он должен работать в одной и той же настольной среде, возможно применение обязательных профилей.

Настройки

Профили пользователей содержатся в древовидной структуре подкаталогов каталога \%*Systemroot*%\Profiles\имя_пользователя, а также в файле данных ntuser.dat. Древовидная структура профиля содержит информацию о комбинациях клавиш, принтерах, недавно открытых файлах, а также другие прикладные данные. В файле ntuser.dat содержится кэшированная информация из реестра HKEY_CURRENT_USER Windows NT. В этом реестровом дереве хранятся данные об установленном программном обеспечении, настройках среды и общая информация о конкретном пользователе.

В профилях пользователей могут, к примеру, заключаться следующие настройки:

- *дисплей*: фон, заставка, цветовая схема;
- *меню*: запуск элементов меню и пиктограмм на рабочем столе;
- *мышь*: настройки мыши;

- *соединения*: сетевые и принтерные соединения;
- *окно*: схема, удерживающая размеры и положения окна;
- *Explorer*: все определяемые пользователем настройки Windows Explorer;
- *справка*: все закладки в системе справки Windows;
- *панель управления*: все определяемые пользователем настройки Панели управления;
- *приложения*: все изменения, вносимые в приложения Windows, с которыми работают отдельные пользователи, — например, Calculator, Clock, Paint, HyperTerminal и т. д.

Локальные профили

Существует три типа профилей, которые предоставляют вам возможность выбора: либо контролировать среду пользователя, либо разрешить ему управлять своими настройками рабочего стола. Локальный профиль создается, когда пользователь впервые проходит процесс регистрации. Для него назначается копия профиля, называемого Default User (Пользователь по умолчанию). С этого момента он вправе изменять свои настройки и надеяться на их сохранение по окончании работы. Во время следующей регистрации происходит загрузка его специализированного профиля. Локальные профили могут применяться только в одной системе. Если у пользователя есть учетные записи на нескольких машинах, в каждой из них хранится отдельный профиль. Внесение изменений в настройку на одной машине не приводит к модификации других профилей.

Перемещаемые профили

Перемещаемые профили (Roaming Profiles) позволяют пользователям создавать и сопровождать единый профиль, который применяется во всем домене. Независимо от того, на какой машине пользователь проходит процесс регистрации, он работает с одними и теми же настройками рабочего стола, изменения которых сохраняются и повторно применяются при следующей регистрации — опять же, вне зависимости от того, на каком компьютере она осуществляется.

В среде Windows 2000 (в случае применения Active Directory) профили сопровождают пользователей по всей сети. В Windows NT и в средах без Active Directory для организации пользовательских блуждающих профилей вы должны настроить путь к профилю каждого из них — эти данные указываются в программе User Manager for Domains (Диспетчер пользователей домена) под кнопкой **Profile** (Профили). При наличии множества пользователей можно создать запись наподобие \\имя_сервера \путь_к_профилю \%username%. Это позволяет производить многократное копирование данного пользователя, не меняя имя пути профиля — все благодаря переменной среды `%username%`. Затем вы должны перейти на вкладку **User Profiles** (Профили пользователей) окна **Systems Properties** (Свойства системы), запускаемого из Панели управления (Control Panel). Если для данного пользователя в User Manager задан путь, то здесь можно изменить тип профиля с Локального (Local) на Перемещаемый.

Важно отметить, что при необходимости копирования профиля от одного пользователя к другому применяется кнопка **Copy To**. Простое копирование файла ntuser.dat

и древовидной структуры профиля не приводит к созданию соответствующих записей в реестре. Windows NT не сможет узнать о том, как нужно загружать данный профиль.

Обязательные профили

Обязательный профиль (Mandatory Profile) — это вариант перемещаемого профиля, обновление которого пользователем невозможно. Администраторы и сотрудники технического отдела, без сомнения, оценят преимущества единообразия настроек рабочих столов всех пользователей. Такая логичность поможет сотрудникам находить решения проблем и объяснять их пользователям. Если прибавить к этому редактирование системных политик, то получается, что обязательный профиль способен предоставить вам серьезный контроль над пользовательской рабочей средой.

Чтобы заменить обычный перемещаемый профиль обязательным профилем, скопируйте его в другую учетную запись, внесите все необходимые изменения и переименуйте файл ntuser.dat в ntuser.man. После этого при регистрации данного пользователя (или пользователей, если один и тот же профиль намерены задействовать несколько человек), ваши настройки будут введены в действие, а все изменения, которые пользователю удастся внести в ходе текущего сеанса, не будут сохранены в профиле. Планируя изменения в будущем, вы можете вносить их в копию профиля в автономном режиме, а затем переносить в его рабочую версию.

Сценарии регистрации

Несмотря на то, что профили пользователей способны контролировать большинство аспектов пользовательской рабочей среды, бывают случаи, когда при регистрации пользователя вам все-таки приходится запускать программу или пакетный файл. Для этого, работая в **User Manager for Domains** (Диспетчер пользователей домена, NT), или в оснастке MMC Windows 2000 **Local Users and Groups** (Локальные пользователи и группы), вы вводите путь и имя сценария на вкладке **Profile** (Профиль) диалогового окна **User Properties** (Свойства: *<имя_пользователя>*). Так как в профилях пользователей можно указать, какие сетевые соединения нужно устанавливать, обозначать их в сценарии не нужно. Впрочем, клиенты других операционных систем, в которых профили пользователей не реализованы, также могут применять сценарии регистрации. Возможна и другая ситуация, когда сценарий регистрации задействуется для запуска конкретного приложения. К примеру, быть может, вы хотите, чтобы при регистрации каждый пользователь проводил операцию поиска вирусов.

Традиционно было принято помещать сценарные команды в пакетный файл, который запускался при регистрации. К примеру, подключить всех пользователей к совместно используемому диску можно было при помощи команды:

```
net use s: \\имя_сервера\имя_коллективного_ресурса
```

Поиск ошибок в сценариях

В системах Windows сценарии регистрации предназначены для задания среды, в которой пользователь должен выполнять регистрацию. Формирование сценария регистрации происходит в три этапа, варьирующихся в зависимости от конкретной вер-

сии операционной системы Windows. В Windows NT следует выполнить следующие действия.

1. Откройте User Manager for Domains (Диспетчер пользователей домена).
2. Дважды щелкните на записи пользователя в выведенном списке, и выберите вкладку **Profile** (Профиль).
3. Введите имя файла сценария регистрации в текстовом окне **Logon Script Name**.

В Windows 2000 и .NET этот процесс проходит аналогичным образом, но для его выполнения применяется консоль управления Microsoft.

1. Откройте оснастку MMC Local Users and Groups (Локальные пользователи и группы).
2. Дважды щелкните на записи пользователя в выведенном списке, и выберите **Profile** (Профиль).
3. Введите имя файла сценария регистрации в текстовом окне **Login Script**.

Вводя имя файла, важно обратить внимание на расширение файла, в котором хранится нужный сценарий регистрации. В среде Windows расширением должно быть bat. Расширение exe система Windows воспринимает как исполнимый файл и загружает его для выполнения. Если никакого приложения нет, сценарий регистрации не запустится. Ниже приводятся проблемы, которые могут возникнуть при разработке сценариев для регистрации в Windows, а также их решения.

Загрузка приложения, не вызванная командой сценария

Если пользователь жалуется на то, что каждый раз при регистрации происходит запуск ненужного приложения, в первую очередь проверьте сценарий регистрации. Если никаких компонентов, которые могли бы инициировать запуск приложения, в нем не обнаруживается, переходите к анализу файла autoexec.bat. Просмотрите этот файл целиком, строчка за строчкой, и проверьте, не обуславливает ли какая-либо запись файла autoexec.bat вызов приложения. Впрочем, вполне вероятно, что искомой команды нет ни в сценарии регистрации, ни в файле autoexec.bat.

Теперь нужно проверить реестр системы. Его открытие производится при помощи утилиты regedit.exe — перейдите к ключу HKEY_CURRENT_USER\Software \Microsoft \Windows\CurrentVersion. Этот ключ реестра содержит элементы конфигурации, которые задействуются при каждом запуске Windows.

Примечание

С реестром шутки плохи. Если у вас нет стопроцентной уверенности в том, что все, что вы делаете, правильно, не связывайтесь с реестром. Простая опечатка, допущенная в реестре, может привести к неисчислимым и крайне отрицательным последствиям для вашего компьютера!

Просмотрите данные, приведенные в записях подраздела **run**. Если вы встретитесь с какими-либо строками, указывающими на запускаемую программу, удалите такую запись.

Не надо изобретать колесо

Наличие стандартных сценариев может значительно упростить задачу назначения пользователям сценариев регистрации. При появлении нового пользователя вы мо-

жете присвоить ему тот же сценарий, который уже есть у других участников его группы. В результате процесс составления сценариев упрощается. Во-первых, отпадает необходимость в переписывании сценария. Во-вторых, этот метод гарантирует наличие у всех участников группы одинаковых свойств, заданных в общем для них сценарии. Наконец, это хороший способ избежать неприятностей. Поскольку вы знаете, что определенный сценарий уже работает у других участников группы, нет резона бояться того, что простая опечатка может привести к его неверному функционированию.

В среде Windows для установления сетевых полномочий, которыми вы предполагаете наделить пользователей, может применяться Group Policy. Тем не менее есть некоторые причины, по которым использование сценария оказывается предпочтительным. Во-первых, вполне может быть, что вы не намерены координировать полномочия пользователей. Кроме того, вероятен вариант подключения к ресурсу, управление которым средствами Group Policy окажется невозможным (например, к настройке, связанной с другой операционной системой, и т. д.).

Сейчас мы создадим небольшой сценарий — лишь для того, чтобы продемонстрировать его составляющие. В данном случае сценарий предоставляет пользователю доступ к открытым файлам на производственном сервере организации. Сценарий таков:

```
net use z:\\production\current
```

В этом примере присутствуют три компонента сценария:

- имя диска (в данном случае — `z:`);
- имя компьютера, к которому предоставляется доступ (в данном случае это производственный сервер);
- имя коллективного ресурса, в котором содержатся нужные файлы (в данном случае — `current`).

Теперь нужно присвоить сценарию имя (и не забыть, что он должен оканчиваться расширением bat). Можно назвать его production.bat. Затем — так, как показано ранее в этом разделе — указывается путь к сценарию регистрации.

Управление временем

В свойствах файла или каталога приводятся разнообразные данные, включая информацию о создавшем его пользователе, о времени создания, времени последнего обращения и т. д. Так как временные метки имеют столь серьезное значение, для обеспечения синхронизации клиентских машин с серверами разумно использовать сценарии регистрации.

Простой сценарий, с помощью которого производится временная синхронизация, выглядит следующим образом:

```
net time \\server /set /yes
```

В этом примере присутствуют следующие компоненты:

- `net time` — это команда;
- `\\server` — это имя сервера, с которым клиентская машина должна синхронизировать свои показания времени;

- `/set` — указывает клиентской машине на необходимость установки времени в соответствии со значением сервера;
- `/yes` — подтверждает ваше намерение изменить время и данные на клиентской машине в пользу значения сервера.

Средства создания сценариев

Для написания сценариев важно пользоваться текстовым редактором. В отсутствие точного, беспримесного текста ASCII (American Standard Code for Information Interchange — Американский стандартный код для обмена информацией) возможно неверное чтение сценария, появление ошибок и разнообразных трудностей. Вероятно, вы подумали, что для составления сценариев текстовый процессор наподобие Word не подходит. Правильно. Впрочем, если следующей вашей мыслью было обратиться к Windows Notepad, подумайте еще.

На первый взгляд Notepad производит впечатление редактора простого текста, но, тем не менее, задействовав символы Unicode, он может все испортить. Эти символы оказывают на сценарий негативное воздействие, мешая ему работать. Лучше всего воспользоваться редактором в среде MS-DOS.

Несмотря на то, что в одной из последних версий Windows компания Microsoft грозилась избавиться от командной строки DOS, она все же присутствует в новейших вариантах этой операционной системы. Чтобы открыть редактор MS-DOS, запустите командную строку, и введите команду `edit имя_файла.bat`. В результате откроется редактор MS-DOS, который сохранит файл сценария без всяких примесей постороннего кода.

Симптомы неисправностей

Наверное, вы читали и посмеивались над почтой из серии "невымышленный звонок в справочный стол". Обычно в них пишут об ужасно бестолковых поступках, на которые люди идут, не обращаясь к здравому смыслу — например, там рассказывалось про женщину, которая хотела узнать, как вынуть из компьютера подставку для кофе (оказалось, что она имела в виду CD-ROM), про парня, который все не мог засунуть во флоппи-дисковод компакт-диск, и его пришлось подрезать ножницами, так что он влез, "но проклятая пластинка все равно не хотела работать...".

Все это, конечно, забавно, но правда в том, что все мы время от времени притормаживаем мозгами. Наверное, мы не докатимся до того, чтобы рубить компакт-диск, но иногда мы забываем снять клавишу <Caps Lock>, да и контакт кабеля клавиатуры может отойти. Именно на обстоятельства такого рода нужно обращать внимание, приступая к поиску неисправностей.

Более коварными могут оказаться проблемы, которые проистекают от применения всех тех политик, которые позволяет создавать система Windows. Microsoft заслуживает похвалы за попытку сопровождения своих политик паролей максимальным количеством дополнительных опций, однако чем больше их появляется, тем более осторожным должен быть администратор, настраивая пароли и управляя ими.

Симптом 26.1. У меня неприятности с политиками паролей

Лучший способ избежать проблем с паролями заключается в планировании таких политик паролей, которые способны обеспечить нужный уровень безопасности, не

превращаясь при этом в сплошную кашу. В системах Windows 2000 и .NET политики паролей координируются при помощи инструмента Security Policy (Политика безопасности). В Windows NT они находятся в диалоговом окне **Account Policy** (Политика учетных записей). Управление политиками может производиться как для отдельных пользователей, так и для пользовательских групп.

Microsoft предусматривает возможность установки следующих настроек пользовательских паролей.

- **Maximum Password Age** (максимальный срок действия пароля) — от 1 до 999 дней, или **Password Never Expires** (срок действия пароля не ограничен).
- **Minimum Password Age** (минимальный срок действия пароля) — от 1 до 999 дней, или **Allow Changes Immediately** (допускаются немедленные изменения).
- **Minimum Password Length** (минимальная длина пароля) — от 1 до 14 символов, или **Permit Blank Password** (допускается пустой пароль).
- **Password Uniqueness** (уникальность пароля). Позволяет вам определить, сколько раз должен быть создан новый пароль, прежде чем у пользователя появится возможность воспользоваться старым. В отношении новых паролей значение может варьировать от 1 до 24. В Windows 2000 настройка присутствует в **Enforce Password History** (требовать неповторяемости паролей).
- **Account Lockout** (пороговое значение блокировки) — от **never** (никогда) до 999. Эта настройка определяет, сколько раз пользователь имеет право ввести неверный пароль, прежде чем Windows откажет ему в дальнейших попытках его ввода. Помимо прочего, в рамках этой политики необходимо установить счетчик сброса (**Reset Counter After**, от 1 до 99 999), который определяет промежуток времени в минутах, отделяющий любые две последовательные неудачные попытки регистрации. Настройка **Lockout Duration** (блокировка учетной записи на...мин.) указывает компьютеру на необходимость блокировки пользователя на перманентной основе (т. е. для разблокировки требуются действия со стороны администратора) или на протяжении определенного временного периода (от 1 до 99 999 минут), по прошествии которого учетная запись должна быть разблокирована.
- **User Must Logon in Order to Change Password** (для изменения своего пароля пользователь должен зарегистрироваться). Эта политика определяет, будет ли пользователь иметь право изменить свой истекший по сроку действия пароль, или же это должен делать только администратор. Если эта политика не задействована, пользователи смогут менять пароли, сроки действия которых истекли, не обращаясь к администратору.

На первый взгляд, эти политики должны прекрасно уживаться друг с другом. Тем не менее есть такие их сочетания, которые, как при смешивании кислоты со щелочью, просто напрашиваются на неприятности. Примеры — ниже.

- Если в рамках политики **Minimum Password Age** (максимальный срок действия пароля) задействовать опцию **Allow Changes Immediately** (допускаются немедленные изменения) и одновременно внедрить политику **Password Uniqueness** (уникальность пароля), начнутся трудности. По этой причине не следует включать политику **Password Uniqueness** — лучше установить переключатель в положение **Do Not Keep Password History** (Не накапливать предысторию паролей).

- Если вы решили задействовать политику **Password Uniqueness** (уникальность пароля), укажите в политике **Minimum Password Age** (минимальный срок действия пароля) минимальное количество дней.
- Политики, допускающие применение пустых паролей, с одной стороны, и минимальную длину паролей, с другой, не сочетаются. Пользуясь одной, отключите другую.
- Настраивая продолжительность блокировки, сделайте так, чтобы период времени, указанный в **Lockout Duration** (блокировка учетной записи на ... мин.), был равен значению **Reset Counter After** (сброс счетчика блокировки через) или превышал его. В противном случае такая конфигурация не будет работать.

Симптом 26.2. Пользователь забыл свой пароль

Только не надо слишком сильно злиться на пользователей, которые забывают пароли. Такое случается. По крайней мере, согласитесь: лучше пусть они обратятся за помощью к вам, чем будут записывать свои пароли на бумажки и приклеивать их к своим мониторам. Если в качестве систем для клиентских рабочих станций в сети применяются Windows XP, проблема разрешима и без вашего участия. Windows XP допускает применение диска восстановления паролей, благодаря которому пользователям, забывшим пароль, впредь не придется ударять лицом в грязь, потому как они смогут справляться с этой проблемой собственными силами.

Впрочем, если ваша система не поддерживает возможность создания дисков восстановления паролей, вам придется восстановить пользовательский пароль. Кроме того, вы можете заставить пользователя ввести новый пароль при следующей регистрации. Соответствующий флажок находится в диалоговом окне **User Properties** (Свойства: *<имя_пользователя>*).

Симптом 26.3. Снятие блокировки с пользовательской учетной записи

Как указывалось ранее в этом разделе, причины блокировки пользовательской учетной записи могут быть самыми разнообразными — это и истечение срока годности пароля, и превышение максимального количества попыток регистрации, и т. п. В вашем распоряжении есть несколько методов, позволяющих выполнить разблокировку пользователя.

Чтобы разблокировать рабочую станцию, откройте User Manager for Domains (диспетчер пользователей домена в NT) или консоль Local Users and Group MMC (в 2000 и .NET); после этого двойным щелчком выделите нужного пользователя. Флажок **Account Locked Out** (Заблокировать учетную запись) установлен — его нужно просто снять. Если срок блокировки истекает по прошествии предопределенного периода времени, пользователь может либо дождаться этого момента (впрочем, для этого он должен знать, какова продолжительность этого периода, и иметь желание ждать его истечения), либо прийти к вам со шляпой в руках и попросить разблокировать свою рабочую станцию.

Симптом 26.4. Предоставьте управление пользователю

При установке минимального и максимального значения, связанного с изменением паролей, Windows автоматически сообщает пользователю о необходимости устано-

вить другой пароль в течение 14 дней. Две недели — это значение по умолчанию, но вы можете заменить его любым сроком. К примеру, если вы решили, что пароли нужно менять еженедельно, 14-дневный срок не подходит. С другой стороны, вам может показаться, что пользователю необходимо 30 дней для привыкания к рутине смены паролей.

В любом случае изменить эту настройку можно путем редактирования реестра. Выполните следующие действия:

1. Откройте regedit.exe и перейдите к ключу HKEY_LOCAL_MACHINE \Software \Microsoft \WindowsNT\CurrentVersion\Winlogon.
2. Создайте элемент REG_DWORD под названием PasswordExpiryWarning.
3. Введите данные, устанавливающие количество дней до истечения срока действия пароля, когда пользователь должен получить соответствующее предупреждение.

Симптом 26.5. Пользователю не удается зарегистрироваться в домене из-за различий во времени

Когда вы интегрируете новый компьютер в домен Windows 2000, а затем пытаетесь зарегистрироваться в этом домене, на экране может появиться сообщение о том, что регистрация невозможна из-за различий во времени между клиентом и сервером.

Все дело в том, что протокол аутентификации Kerberos анализирует временную метку запроса аутентификации, который отсылается клиентом. Эта временная метка сравнивается с текущим временем по данным контроллера домена. Если между показаниями времени на двух машинах фиксируется значительное различие (по умолчанию — более 5 минут), аутентификация не выполняется.

Чтобы устранить эту проблему, убедитесь в том, что на клиенте и на сервере установлено одинаковое время. Более того, проверьте правильность задания на обоих компьютерах часовых поясов, т. к. Kerberos преобразует все временные значения в Гринвичское время, и только после этого выполняет сравнение.

Симптом 26.6. Домен не идентифицирует клиентский компьютер после его переименования

Довольно часто после переименования клиентского компьютера регистрационный домен отказывается идентифицировать новое имя. Чтобы избежать появления этой проблемы, при переименовании клиентов Windows необходимо выполнять следующие действия:

1. Создайте новую учетную запись компьютера под его новым именем.
2. Выйдите из домена, присоединившись к рабочей группе.
3. При появлении соответствующего приглашения Windows перезагрузите клиентский компьютер.
4. Присоединитесь к домену повторно — на этот раз с использованием нового имени компьютера.
5. При появлении соответствующего приглашения Windows перезагрузите клиентский компьютер.

Регистрация в Linux/UNIX

Несмотря на то, что Windows занимает лидирующие позиции в блоке клиентских операционных систем, во многих сетевых конфигурациях компьютеры Linux/UNIX все же превалируют. Довольно распространена ситуация, когда сервер Linux/UNIX поддерживает множество разнородных клиентских машин с самыми разными операционными системами.

В этом разделе рассматриваются различные клиентские компоненты среды Linux/UNIX. Анализу подвергаются не только вопросы, связанные с регистрацией, но также клиентские соединения, устанавливаемые посредством сетевой информационной службы (Network Information Service, NIS), и подключение Linux/UNIX к клиентским машинам других типов при помощи промежуточных средств, таких как Samba.

Сетевая информационная служба

В зависимости от требований и задач конкретной организации, компьютерные сети могут представлять собой сложные среды, в которых разные службы предоставляются в разных зонах. Может оказаться, что для обращения к определенному ресурсу пользователи и сетевые администраторы должны регистрироваться на другом компьютере. Когда пользователи обращаются к другим рабочим станциям, они ожидают оказаться в знакомой настольной и вычислительной среде. Как бы то ни было, предупреждение требований, предъявляемых пользователями при регистрации, и их реализация во всех частях сети превращается в кошмар.

Сетевая файловая система (Network File System, NFS) предусматривает наличие серверной среды, способной выполнять перемещение пользовательских настроек (об этом речь шла в *разд. "Перемещаемые профили" ранее в этой главе*). В рамках NFS существует сетевая информационная служба (NIS). NIS поддерживает распределенные базы данных, которые выполняют функцию сопровождения определенных общесетевых административных файлов, включающих данные о паролях и группах, а также адреса хостов.

Служба NIS была разработана в компании Sun Microsystems в 1980-е годы; долгое время она была известна под названием желтых страниц (Yellow Pages, YP). Со временем Yellow Pages превратилась в систему управления, которая называется NIS+. Несмотря на то, что NIS и NIS+ применяются в основных вариантах UNIX и, по существу, работают примерно одинаково, NIS+ предусматривает более серьезную по сравнению с NIS систему защиты.

Службы NIS/NIS+ работают в рамках клиент-серверной модели. Клиент NIS запускает процессы, которые запрашивают данные с серверов NIS. Приложения, использующие NIS/NIS+, не обязаны знать местонахождение компьютера, на котором хранится нужная им информация. Задача NIS/NIS+ заключается как раз в том, чтобы найти необходимую информацию на сервере NIS и предоставить ее приложению в нужном ему формате.

Существует два типа серверов NIS/NIS+ (оба они изображены на рис. 26.6).

- *Хозяева доменов* (Domain masters). На этих серверах хранятся все исходные файлы базы данных, относящиеся ко всему домену.

- *Подчиненные серверы* (Slaves). Так как службы NIS/NIS+ выполняют столь важную функцию, доступ к ним должен быть возможен даже в случае неисправности сервера NIS/NIS+. Таким образом, хозяин домена периодически отсылает копию всех своих исходных файлов подчиненному, т. е. резервному серверу.

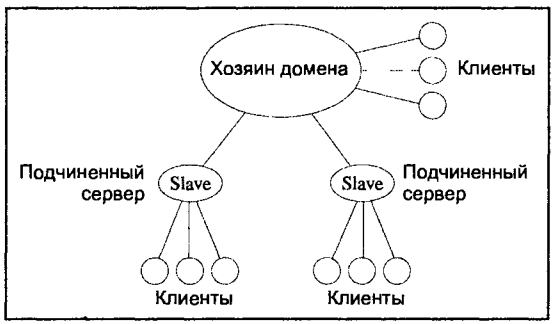


Рис. 26.6. Развертывание серверов NIS/NIS+

Службы NIS/NIS+ предусматривают механизм фильтрации, предназначенный для аутентификации пользователей, запрашивающих доступ к коллективным ресурсам. К примеру, если вы хотите обратиться к файлу, который хранится на другом компьютере сети, NIS/NIS+ определяет, имеете ли вы право на использование этого ресурса, причем делает это еще до того, как NFS выполнит его сборку. Более того, если вы собираетесь выполнить удаленный вызов процедур (remote procedure call, RPC), NIS/NIS+ обеспечивает доступ к нужной команде, а также к ресурсу, расположенному на другом сетевом компьютере.

Поймите правильно — служба NIS/NIS+ не выполняет аутентификацию. Она просто возвращает записи базы данных. К примеру, при обращении к базе данных паролей NIS/NIS+ определяет местонахождение нужной информации — приложение должно иметь данные о том, что пользователь располагает полномочиями, необходимыми для обращения к нему.

NIS+ применяется демоном rpc.nisd. Этот демон выполняет запуск службы NIS+ одним из следующих способов.

- NIS+ можно запустить вместе со всеми ее сервисными функциями.
- NIS+ можно запустить *в режиме совместимости* с NIS — для этого применяется опция `-YB`. В результате компьютеры, находящиеся в сети, получают возможность потребления ресурсов по образцу более устаревшей службы NIS.

Поиск неисправностей NIS

Службы NIS/NIS+ обеспечивают дополнительный уровень функциональности в средах UNIX, но с ним связаны и новые трудности. Ниже приводятся лишь некоторые проблемы, которые могут происходить в процессе работы NIS и NIS+.

Симптом 26.7. Пользователю не удается зарегистрироваться или воспользоваться командой *rlogin* в другом домене

Если пользователю для обращения к другому домену не удается задействовать `rlogin`, можно предположить самые разные причины, включая приведенные ниже.

- *Забытый пароль.* Если пользователь забыл свой пароль, откройте для него `nispasswd` на другом компьютере.
- *Неверно введенный пароль.* До боли знакомая проблема — убедитесь в том, что режим, устанавливаемый клавишей <Caps Lock>, отключен, а пользователи осведомлены о чувствительности паролей к регистру.
- *Срок действия.* Не закончился ли срок действия парольных полномочий пользователя?
- *Бездеятельность.* Пользователь превысил максимальное значение бездеятельности, заданное для его учетной записи.

Примечание

Более подробно команду `rlogin` мы рассмотрим далее в этом разделе.

Симптом 26.8. Новый пароль пользователя не функционирует

Если пользователь недавно изменил свой пароль, а теперь не может пройти регистрацию, или может, но на всех компьютерах, можно предположить две вещи:

- распространение новых паролей по всей сети занимает некоторое количество времени — попробуйте ввести старый пароль;
- изменение пароля было выполнено на компьютере, на котором NIS+ не функционирует.

Симптом 26.9. Пользователю не удается зарегистрироваться в удаленном домене

Если после ввода пользователем команды `rlogin` компьютер отвечает ему сообщением "полномочия отклонены", убедитесь в наличии локальных полномочий пользователя на данном компьютере. Перейдите в другой домен, и, чтобы проверить наличие в нем необходимых локальных полномочий, введите команду

```
nismatchимя_пользвателя.имя_домена.cred.org dir.
```

Чтобы назначить пользователю подходящие полномочия, сделайте следующее:

1. Создайте для пользователя полномочия в удаленном домене, введя в нем команду `nisaddcred`.
2. Отредактируйте файлы /etc/security/login.cfg, etc/security/user и /usr/lib/security /methods.cfg (или, если таковых не существует, создайте их) — в каждом из них должны присутствовать следующие строки:

```
NISPLUS
  program=/usr/lib/security/NISPLUS
```

Симптом 26.10. Пользователю не удается изменить свой пароль

Если пользователь не может изменить свой пароль, вероятнее всего, он неправильно ввел или забыл свой старый пароль. Возможны и другие причины:

- установленное минимальное (**Min**) значение пароля больше, чем его максимальное (**Max**) значение;
- пароль заблокирован, или срок его годности истек.

Симптом 26.11. У пользователя нет необходимых полномочий

Самая распространенная проблема, связанная с полномочиями, одновременно является самой легкоразрешимой. По сути, у пользователя нет полномочий для обращения к определенному сетевому ресурсу. Введите команду `niscat -o` в отношении объекта, к которому пользователь пытается обратиться; так вы сможете ознакомиться с его полномочиями. Все необходимые изменения может выполнить системный администратор или владелец объекта.

Симптом 26.12. У пользователя нет подходящего сертификата

Если у пользователя отсутствует необходимый сертификат, он не сможет выполнять множество операций. Чтобы проверить наличие нужного сертификата, введите команду `nismatch` по отношению к таблице сертификатов домашнего домена.

Симптом 26.13. Имя пользователя идентично имени компьютера

Ситуация, при которой имя пользователя ничем не отличается от имени компьютера, является недопустимой. Если пользователю присваивается имя, идентичное имени компьютера (или компьютеру назначается имя, идентичное имени пользователя), то первый объект теряет возможность выполнения операций, требующих применения полномочий безопасности, т. к. ключ второго объекта в таблице сертификатов записывается поверх ключа первого объекта. Более того, второй объект получает полномочия, которые первоначально присваивались первому объекту. Среди симптомов этой неисправности отмечаются следующие:

- пользователь или компьютер получает сообщения об ошибках "отклонения полномочий";
- пользователю или корневому пользователю компьютера не удается запустить `keylogin`;
- появляется сообщение об ошибке "Security exception on LOCAL system. UNABLE TO MAKE REQUEST" ("Ошибка исключения защиты в локальной системе. НЕ УДАЕТСЯ ОТПРАВИТЬ ЗАПРОС").

В такой ситуации лучше всего сначала изменить имя компьютера, а затем удалить запись этого компьютера из таблицы сертификатов. Затем с помощью команды `nisclient` нужно провести повторную инициализацию компьютера в качестве клиента NIS+. Возможно, вам придется заменить сертификат пользователя в таблице сертификатов.

Samba

Современные сетевые среды редко бывают однородными. К примеру, возможны ситуации, когда большинство сотрудников компании работают на клиентских машинах Windows, но в некоторых зонах присутствуют вкрапления в виде серверов или клиентов UNIX и Linux. Для того чтобы все эти компьютеры могли исправно взаимодействовать, необходимо средство, которое может удовлетворить потребность обращения клиентов одного производителя к клиентам другого производителя.

Примечание

В конце этой главы приводится ссылка на Web-сайт Samba, с которого вы можете загрузить копию этого пакета.

Очень распространенным методом предоставления клиентам Windows возможности доступа к дискам UNIX является серверный пакет Samba. Он представляет собой бесплатно распространяемую программу, которая работает на серверах UNIX и обеспечивает клиентам Windows доступ к сборкам UNIX. Прежде чем возмущаться идеей использования некоммерческого продукта в своей организации, вам следует знать, что пакет Samba, существуя уже довольно давно, получил широкое распространение как в академических условиях (где он и разрабатывался), так и на некоторых крупных корпоративных узлах. Samba — это надежный, качественно протестированный, хорошо документированный программный пакет, который стоит принять во внимание, если вашей целью является наделение клиентов в сети Windows возможностью считывания и сохранения файлов, хранящихся в системах UNIX.

Samba базируется на протоколе SMB (Server Message Block — блок серверных сообщений), который применяется в Windows для обеспечения коллективного доступа к файлам. Samba предусматривает поддержку протокола SMB со стороны UNIX. Демон Samba реагирует на запросы SMB, исходящие от сетевых клиентов Windows, и принимает на себя роль сервера, отвечающего на такие запросы.

Так как Samba — это процесс, полностью существующий в системах UNIX, системный администратор UNIX должен установить Samba-сервер. В то же время, для подключения клиентов сети к Samba-серверу от системного администратора Windows практически ничего не требуется. Если вас тревожат сомнения по поводу использования разнообразных вариантов UNIX, можете спать спокойно: пакет Samba совместим со всеми основными версиями UNIX (т. е., к примеру, с продуктами Apollo, HP, DEC, NeXT, SCO, Sun и SGI и других компаний). В этом разделе мы приведем краткое описание требований, соблюдение которых позволит Samba взаимодействовать с системами Windows.

Требования к сетевым клиентам NT

Никаких клиентских файлов Samba, которые нужно устанавливать на машинах Windows 9x, 2000, XP или NT, не существует; тем не менее, чтобы такие машины получили возможность подключения к компьютерам UNIX и обращения к их ресурсам, на них должны быть установлены все необходимые сетевые протоколы и службы. Требуется наличие стека протоколов TCP/IP и служб DNS.

Примечание

Если служба DNS не установлена, то имена и IP-номера DNS машины UNIX можно хранить в файле HOSTS, расположенном в каталоге %Systemroot%\System32 \drivers\etc.

Конфигурация UNIX

Настройки Samba-сервера задаются в файле smb.conf. Секционная структура этого текстового файла покажется знакомой всем, кому приходилось редактировать файл SYSTEM.INI. В нем присутствуют отдельные секции для каждого создаваемого коллективного ресурса — они позволяют определять действительных пользователей, полномочия чтения-записи и общего доступа. Ниже приводится пример файла smb.conf.

```
[global]
workgroup = ACCOUNTING
server string = Accounting Department's Samba Server
encrypt passwords = True
security = user
smb passwd file = /etc/smbpasswd
log file = /var/log/samba/log.%m
socket options = IPTOS_LOWDELAY TCP_NODELAY
domain master = Yes
local master = Yes
preferred master = Yes
os level = 65
dns proxy = No
name resolve order = lmhosts host bcast
bind interfaces only = True
interfaces = eth0 192.168.1.1
hosts deny = ALL
hosts allow = 192.168.1.4 127.0.0.1
debug level = 1
create mask = 0644
directory mask = 0755
level2 oplocks = True
read raw = no
write cache size = 262144

[homes]
comment = Home Directories
browseable = no
read only = no
invalid users = root bin daemon nobody named sys tty disk mem kmem users

[tmp]
comment = Temporary File Space
path = /tmp
read only = No
valid users = admin
invalid users = root bin daemon nobody named sys tty disk mem kmem users
```

В корпоративных средах с большим количеством клиентов очень серьезное значение имеют два раздела. Раздел `[homes]` автоматически разрешает пользователям, у которых уже есть учетные записи в системе UNIX, подключаться к своим домашних каталогам, не создавая отдельные коллективные ресурсы для каждой учетной записи. В разделе `[global]` устанавливаются некоторые свойства сервера. Чрезвычайно важную роль исполняют защитные опции, устанавливающие метод аутентификации пользователей. Есть три режима защиты, которые можно установить в записях `security=` секции `[global]`.

- `Security=share`. Запись `valid users`, присутствующая в разделах всех коллективных ресурсов, может определять отдельных пользователей и устанавливать их

права в пределах данного ресурса. Это довольно небезопасный метод; кроме того, он ограничен лишь теми пользователями, у которых уже есть учетные записи UNIX; таким образом, он малопригоден для обеспечения общего доступа для пользователей сети Windows в рамках предприятия.

- `Security=user`. В этом режиме вся аутентификация происходит при помощи пользовательских учетных записей UNIX. В случае, если у всех клиентов сети Windows есть учетные записи в системе Windows, такая схема представляется безопасной и эффективной. Этот вариант приемлем для тех предприятий, в которых каждый пользователь сети располагает учетной записью UNIX.
- `Security=server`. Этот режим, очевидно, подходит для ситуаций, когда учетные записи UNIX есть не у всех пользователей сети или не должны быть у всех ее пользователей. В таком режиме обращение со стороны пользователя аутентифицируется посредством сервера, отличного от UNIX Samba — к примеру, при помощи контроллера домена Windows 2000. В результате одна машина Windows получает возможность предоставлять доступ к ресурсам Windows 2000 и Samba, причем для этого используется единая база данных имен пользователей и их паролей. Помимо прочего, серьезным преимуществом этой схемы является то, что пользователям не приходится менять свои пароли на двух разных системах. Когда в секции `[global]` делается такая запись, имя сервера, который будет проводить аутентификацию, необходимо указать в записи `password server=`.

Примечание

Таким именем будет имя NetBIOS сервера. Чтобы эту машину можно было найти, ее необходимо указать в файле /etc/hosts в системе UNIX.

Недостатком пакета Samba является то, что он применим лишь в том случае, если на всех клиентских машинах используются протоколы SMB. Таким образом, пакет может работать с клиентами Windows 9x, 2000, XP и NT, но не с NetWare и не с Macintosh.

Проблемы регистрации в Linux/UNIX

Так как UNIX является многопользовательской системой, для предоставления доступа к файлам в ней необходимо указать пароль. В случае ввода неверного пароля вы, вероятно, увидите следующее:

```
login: wildbill
Password:
Login Incorrect
login:
```

Приглашение **Password:** появится даже в том случае, если вы введете неверное или несуществующее регистрационное имя. Это не упущение — так делается умышленно, чтобы предотвратить ситуации угадывания регистрационных имен и получения приглашений **Password:** в случае правильных догадок.

Администратор может определить максимальное количество случаев ввода неверных имен и паролей; после превышения этого лимита локальное сетевое или наборное соединение разрывается. Более того, можно сделать так, чтобы системному админи-

стратору в случае неудачных попыток регистрации приходили оповещения. Если пользователь не зарегистрируется в течение предопределенного временного периода (к примеру, в течение минуты), соединение также прерывается.

В случае возникновения проблем при регистрации нужно в первую очередь проверить, не была ли нажата клавиша <Caps Lock>. Так как системы UNIX/Linux чувствительны к регистру, нажатие клавиши <Caps Lock> приводит к тому, что серверу отсылаются неверные имя пользователя и пароль.

Существует четыре способа входа в многопользовательскую систему UNIX. В зависимости от того, какой из них вы предпочитаете, при регистрации могут возникать разные проблемы.

Прямое подключение

Первый способ подключения предполагает использование прямого соединения. В рамках этой схемы рабочие станции и ПК подключены к системе UNIX. Конфигурация этого типа чаще всего встречается в специализированных системах, небольших офисах и лабораториях. После загрузки ПК, вызова терминального эмулятора и нажатия клавиши возврата каретки или <Enter> на экране появляется приглашение системы UNIX:

```
login:
```

Наборный доступ (dial-in access)

Другой метод подразумевает подключение к системе UNIX при помощи наборного соединения. Для набора номера доступа к системе UNIX применяется эмулятор терминала. Как только вы слышите знакомый звук модема, на экране появляются некоторые символы. Если они не появились, нажмите клавишу <Enter>.

Затем должна быть выведена строка регистрации в системе UNIX. Возможно, на экране появятся какие-то странные символы (например, "]]]{{kDFwr|>>f:"). Вероятно, это означает, что система имеет возможность подключения на разных скоростях, но для данного наборного соединения выбрана неверная скорость. Чтобы устранить эту неприятность, нажмите клавишу <Return> или <Break>. При каждом новом нажатии <Return> или <Break> система пытается выполнить отправку данных на терминал на другой скорости соединения. В конечном итоге, когда нужная скорость будет определена, вы увидите знакомое приглашение:

```
login:
```

Если на экран продолжает выводиться мусор, нужно проверить настройки четности и выполнить еще одну попытку.

Локальная сеть

Локальная сеть — это самое распространенное средство подключения к серверу UNIX. Применяемые в этом случае настройки обуславливаются конфигурацией локальной сети. Их несколько, и в их числе — LAN Manager и NetWare. Каждая конфигурация локальной сети содержит комплект программного обеспечения, которое совместно с сетевой платой (NIC) позволяет вам подключать клиентский компьютер к серверу.

На клиентских и серверных машинах могут быть установлены системы Windows или UNIX; как мы уже выяснили, возможны и их сочетания. Чаще всего для подключения клиентских компьютеров к серверам применяется протокол TCP/IP; впрочем, широкое распространение в локальных сетях получили и такие протоколы, как IPX и SPX. К примеру, группу клиентских компьютеров Windows можно подключить к серверу, на котором установлена система UnixWare 7, Solaris или Linux.

Намереваясь обратиться к системе UNIX через локальную сеть, вы в первую очередь должны настроить свой компьютер таким образом, чтобы он мог опознать ту систему, к которой будет подключаться. Так вы гарантируете наличие необходимых протоколов.

Интернет

Четвертый способ подключения к системе UNIX — это подключение через IP-сеть, например через Интернет или внутреннюю сеть. В этом случае для обращения к любому компьютеру, расположенному в сети и допускающему такие соединения, применяется команда `telnet`. На компьютере, к которому вы обращаетесь, может быть установлена UNIX или другая операционная система. Этот компьютер может быть расположен через два помещения от вашего рабочего места, или на другом конце страны.

Удаленная регистрация

Среда UNIX содержит в себе удаленные команды Berkeley. Их часто называют командами r*, т. к. они все начинаются с буквы r. Эти команды используют для выполнения различных функций на удаленных машинах, соединенных с вашим компьютером через TCP/IP. В данном случае нам наиболее интересна команда `rlogin`, которая используется для регистрации на удаленном хосте.

Регистрация на удаленном компьютере UNIX в сети TCP/IP может понадобиться по разным причинам. При помощи команды `rlogin` вы регистрируетесь на удаленном компьютере так, как будто это локальный компьютер. Схема применения команды такова:

```
$ rlogin имя_компьютера
```

Команда `rlogin` предоставляет удаленной машине ваш идентификатор пользователя, а также сообщает ей о типе вашего терминала, отсылая значение переменной `TERM`. Кроме того, вы можете регистрироваться на удаленном терминале при помощи другого идентификатора пользователя и пароля. Это достигается путем применения опции `-l` в сочетании с командой `rlogin`. К примеру, чтобы зарегистрироваться на компьютере gilligan при помощи идентификатора пользователя skipper, нужно ввести следующую команду:

```
$ rlogin -l skipper gilligan
```

Примечание

Этот вариант регистрации отличается от применяемого в Telnet, т. к. Telnet позволяет осуществлять удаленный доступ к компьютерам, на которых установлены разные операционные системы. Telnet не передает удаленному компьютеру информацию о конфигурации вашей машины, а `rlogin` — передает.

При использовании `rlogin` бывают случаи, когда для регистрации на удаленной машине даже не приходится вводить пароль. В других ситуациях указание пароля может потребоваться. В некоторых случаях вам вообще не удастся зарегистрироваться, потому как в базе данных паролей нужного компьютера не окажется вашей записи.

Если в базе данных паролей есть ваша запись, а ваш компьютер обозначен в файле /etc/hosts.equiv удаленной машины, регистрация должна пройти успешно, т. к. удаленная машина находится в доверительных отношениях с вашей локальной машиной.

Кроме того, вы можете зарегистрироваться, не указывая пароль, даже в том случае, если имя вашей локальной машины отсутствует в файле /etc/hosts.equiv, но в домашнем каталоге регистрации, в файле .rhosts есть строка, содержащая имя вашего локального компьютера (если регистрационное имя соответствует вашему имени, или если есть указание на имя вашего локального компьютера и на ваш регистрационный идентификатор).

Если вашей записи нет в базе данных паролей удаленного компьютера, но имя вашего компьютера указывается в файле /etc/hosts.equiv, а в файле .rhosts в домашнем каталоге регистрации удаленной машины нет подходящей строки, удаленный компьютер попросит вас указать пароль. Впрочем, даже если вы введете верные имя пользователя и пароль, ваши полномочия будут ограничены, и они не позволят вам запускать удаленные процессы.

Если вы попытаетесь воспользоваться командой `rlogin` для регистрации на удаленном компьютере, о котором не знает ваш локальный компьютер, последний проведет поиск в своей базе данных, а затем отправит обратно сообщение с указанием на то, что удаленный компьютер не найден:

```
$ rlogin gilligan
gilligan: unknown host
```

Регистрация в NetWare

Последний раздел этой главы посвящен рассмотрению вопросов и сред регистрации NetWare. Вначале приводится обзор службы каталогов Novell и одного средства регистрации, которое делает обращение сразу к нескольким ресурсам довольно простой задачей. Далее идет обсуждение регистрации в NetWare и проблем поиска неисправностей, связанных с этим процессом.

Служба каталогов Novell

В *гл. 5* служба каталогов Novell (Novell Directory Services, NDS) рассматривалась значительно подробнее, чем здесь. Тем не менее важно знать, что NDS допускает возможность расположения сетевых объектов (принтеров, пользователей, файлов и т. д.) в любом месте сети. В результате задача поиска ресурсов пользователями и приложениями значительно упрощается.

При регистрации в NDS все данные представлены пользователю в виде древовидной структуры, т. е. менее крупные объекты помещаются ниже, чем более крупные.

К примеру, пользователи и жесткие диски любого приведенного компьютера будут располагаться ниже самого этого компьютера. Файлы, расположенные на жестком диске, обозначаются ниже этого диска — именно так это показано на рис. 26.7.

Рис. 26.7. Пользователям NDS сетевые ресурсы представлены в виде древовидной структуры

Цель, которую поставила перед собой компания Novell, заключалась в том, чтобы упростить процедуры регистрации при помощи пакета однократной регистрации Novell (Novell Single Sign-on Bundle, пакет NSSO) и службы аутентификации NDS (NDS-AS) 3.0. Оба этих продукта применяются в NDS eDirectory.

В пакете NSSO сочетаются два отдельных продукта регистрации:

- Novell Single Sign-on 2.0;
- v-GO для Novell Single Sign-on.

NSSO Bundle применяется для обращения к большинству Windows-, Web- и централизованных приложений. В целях содействия NSSO, NDS-AS реализует аутентификацию пользователей в масштабах множества платформ и традиционных приложений, независимо от того, используют ли они NSSO Bundle. NSSO Bundle и NDS-AS применяются для единовременной регистрации в нескольких платформах, включая:

- Windows 2000 и NT;
- OS/390;
- Solaris;
- HP-UX;
- AIX;
- Linux;
- Radius;
- информационный сервер Интернета (Internet Information Server, IIS).

Пакет NSSO собирает регистрационные данные от источника при помощи пользовательской рабочей станции или удаленного компьютера, а затем хранит пароли в виде зашифрованных файлов в SecretStore — защищенном месте в рамках NDS.

Когда пользователь обращается к приложению или Web-сайту, защищенному паролем, необходимое сочетание имени и пароля извлекается из SecretStore и предоставляется этому приложению или Web-сайту — таким образом, пользователю не приходится вводить регистрационные данные вручную.

Кроме того, NSSO Bundle выполняет все задачи, связанные с управлением паролей, включая регистрацию, подбор пароля, его изменение и сброс. Вдобавок к этому,

администраторам не приходится координировать несколько паролей, принадлежащих каждому отдельному пользователю. Настройки хоста или пользователя устанавливаются администратором при помощи единой консоли. Пользователи выигрывают от применения NSSO Bundle, т. к. им не приходится запоминать большое количество паролей — таким образом, уменьшается вероятность компрометации сетевой системы защиты в результате письменной фиксации паролей и последующей потери этой записи.

Регистрационная информация шифруется Международной криптографической инфраструктурой Novell (Novell International Cryptographic Infrastructure, NICI). Кроме того, если пользователь отлучается с рабочего места, заставка NDS заставляет его выполнить повторную регистрацию в системе.

NDS-AS усиливает систему защиты NDS функциями наподобие:

- выявления злоумышленников;
- правил паролей;
- лишения пользователей прав работы на других платформах.

NDS-AS — это серверное приложение, защищающее сеть путем препятствования доступу хакеров к паролям через рабочие станции или удаленные консоли.

Регистрация в сети

Процесс регистрации на отдельном сервере NetWare довольно прост. Пользователь вводит свое имя и пароль в диалоговое окно, а затем нажимает кнопку **Login** (Регистрация). Кроме этого, NetWare предусматривает еще два способа регистрации на серверах: регистрацию на нескольких серверах и регистрацию из командной строки.

Регистрация на нескольких серверах

Чтобы зарегистрироваться на нескольких серверах через NetWare Access Manager (Диспетчер доступа NetWare), войдите в меню **Server** и выберите пункт **Login (Multiple Servers)** (Регистрация (Множество серверов)). В окне **NetWare Login Manager** будет выведен список серверов NetWare, на которых вы можете зарегистрироваться. Для выполнения регистрации сделайте следующее:

1. По умолчанию флажок **Reuse Login Name and Password** (Повторное применение регистрационного имени и пароля) помечен. Эта конфигурация предусматривает возможность применения одного сочетания имени пользователя и пароля для регистрации на нескольких серверах. Если на разных серверах вы регистрируетесь с применением разных сочетаний имен и паролей, снимите этот флажок.
2. Регистрация на нескольких серверах выполняется одним из двух способов:
   - Намереваясь зарегистрироваться только на выбранных серверах, отметьте их записи в списке и нажмите кнопку **Login** (Регистрация).
   - Намереваясь зарегистрироваться на всех выведенных серверах, нажмите кнопку **Login (All Servers)** (Регистрация (Все серверы)).
3. В зависимости от того, применяете ли вы единое сочетание имени пользователя и паролей на всех серверах или нет, следует выполнить одно из следующих действий:

- Если флажок **Reuse Login Name and Password** помечен, введите регистрационный пароль NetWare, и нажмите кнопку **Login** (Регистрация).
- Если флажок **Reuse Login Name and Password** снят, на экран будут выводиться приглашения на ввод отдельных имен пользователя и паролей для каждого из выбранных серверов.

4. В окне **Message** (Сообщение) будут зафиксированы все попытки регистрации, завершившиеся успешно и неуспешно.
5. Нажмите кнопку **OK**.
6. В окне **NetWare Login Manager** откройте раскрывающееся меню **Server** и выберите пункт **Exit** (Выход).

Регистрация из командной строки

С другой стороны, для регистрации на серверном компьютере NetWare вы можете воспользоваться командной строкой клиента UNIX или Linux. Для этого применяется команда `nwlogin` — она имеет следующий синтаксис:

```
nwlogin [-p] имя_сервера [/имя_пользователя]
```

Имя пользователя может применяться лишь в том случае, если оно указывается в команде `nwlogin`. Если имя пользователя не указано, `nwlogin` задействует регистрационное имя клиента. `nwlogin` выводит приглашение на ввод пароля NetWare и пользуется им для регистрации на указанном сервере NetWare. Вход на сервер NetWare осуществляется после подтверждения указанных имени пользователя и пароля. Если регистрация прошла успешно, ее результаты на экран не выводятся.

В числе прочих у команды `nwlogin` есть следующие опции:

- `-p` — отменяет вывод приглашения и принимает в качестве пароля NetWare следующую строку стандартного ввода;
- `имя_сервера` — имя файлового сервера, в котором вы намереваетесь зарегистрироваться;
- `имя_пользователя` — регистрационное имя пользователя NetWare. Если это значение не указано, применяется ваше текущее регистрационное имя клиента.

Проблемы регистрации в NetWare

Смешанная операционная среда возникает, когда при обращении к ресурсам, хранящимся на сервере с операционной системой одного типа (например, NetWare), клиенты пользуются операционной системой другого типа (например, Windows). В данном случае возможность проблем при регистрации должна быть очевидной. Одно дело, когда программисты и разработчики пытаются совместными усилиями разрешить проблемы, связанные с соединением компьютеров с одинаковыми операционными системами, и совсем другое дело — когда соединению подлежат две совершенно разные операционные системы.

Ниже приводятся некоторые общие проблемы, которые могут проявляться в смешанной операционной среде NetWare/Windows.

Симптом 26.14. У меня неприятности со сценариями регистрации

При подключении к серверу NetWare, а также при работающей службе NetWare Client Services, вполне вероятно применение сценария регистрации NetWare, т. к. он является единственным методом определения настроек среды и пользователя. Среди распространенных ошибок составления сценариев нужно упомянуть следующие.

- *Ошибка подключения при попытке формирования резервного диска.* Если вы сталкиваетесь с ошибкой, в которой говорится о произошедшей попытке подключения сетевого диска, не связанного с NetWare, возможно, что подключение дисков, заданное в вашем сценарии, направлено на подключение уже подключенного диска.
- *Неудача при исполнении команды* `ENDIF`. Если ваш сценарий работает в контексте клиентской службы для NetWare (Client Services for NetWare, CSNW) или шлюзовой службы для NetWare (Gateway Services for NetWare, GSNW) и при этом содержит команду `ENDIF`, появляется сообщение о невозможности интерпретации строки, в которой указывается эта команда. Дело в том, что `ENDIF` может применяться только в сценарии на клиентской машине NetWare. При работе с CSNW и GSNW необходимо отказываться от применения команды `ENDIF` в пользу `END`.

Симптом 26.15. В смешанной среде появились проблемы

При работе в смешанной операционной среде могут появляться и другие проблемы — например, следующие.

- *Новый сценарий не работает.* Если сценарий только что составлен, вполне возможно, что он еще не распространился на контроллеры доменов. Можете подождать репликации вашего домена в NT или его синхронизации в 2000/.NET. Впрочем, если для вас важна оперативность, синхронизацию можно провести силовым методом — для этого нужно перейти в командную строку и ввести следующую команду:

```
net accounts /sync
```

- *Проверьте полномочия.* Если ваш сценарий регистрации хранится на сервере с файловой системой NTFS, то пользователю, которому этот сценарий принадлежит, нужно предоставить права чтения. Если проблема заключается именно в этом, ее можно выявить: когда права чтения не назначены, никаких сообщений о неудачном исполнении скрипта не выводится.

Симптом 26.16. Трудности с командой *Net Use*

Команда `Net Use` может стать источником противоречий между операционными системами Windows и NetWare. Нередко появляются сообщения об ошибках, в которых утверждается, что представленный пользователем сетевой пароль неверен. В данном случае проблема заключается не в точности ввода пароля, а в настройках NetWare. Устранить ее довольно просто — для этого нужно обратиться к файлу Startup.ncf. Если в нем присутствует строка `SET ENABLE IPX CHECKSUMS=2`, замените `2` на `0`. Дело в том, что контрольные суммы применяются в NetWare, но отсутствуют в Windows. Значение `2` сообщает клиенту, что контрольные суммы нужно задействовать. Значение `0` отключает их.

Как и при выполнении большинства других задач, связанных с поиском неисправностей, в процессе регистрации есть несколько пунктов их типичной локализации.

Как правило, поиск проблемы нужно начинать с очень простого вопроса — не включен ли режим <Caps Lock>? Не отключена ли клавиатура? Такие советы могут показаться чуть ли не оскорбительными, но вы удивитесь, узнав, как часто источником неприятностей является именно это. Проблемы могут возникать в средах, в которых присутствуют смешанные системы. Независимо от того, какова конфигурация вашей сети, поиск неисправностей при регистрации обязательно должен включать тщательную проверку точности настроек.

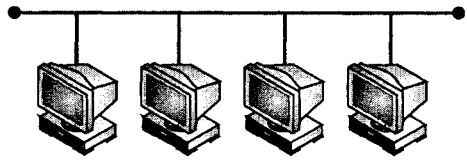
Дополнительные ресурсы

Samba: **http://samba.anu.edu.au/samba/**.

Novell: **www.novell.com**.

Microsoft: **www.microsoft.com**.

Linux: **www.linux.org**, **www.linux.com**, **www.linuxjournal.com**.



ГЛАВА 27

Производительность сети и базовые показатели

Одной из наиболее трудных задач, связанных с сопровождением сетей, является выявление различия между правильным и неправильным поведением сети. Зачастую сети представляют собой сложные, обладающие запутанной структурой среды, в которых прогнозирование запросов каждой рабочей станции (а также определение реакции сети в каждом возможном случае) представляется почти что невозможным. Следовательно, поиск неисправностей в сетях нередко базируется на сравнении текущих эксплуатационных характеристик с эталонным уровнем производительности (базисом, Baseline). Именно этот параметр определяет, что является "нормальным" для данной сети. Если уровень производительности сети опускается ниже установленных базисов, администратор или технический специалист может произвести количественное измерение изменений, проанализировать их, и даже использовать эти данные в качестве довода для проведения модернизации.

Сложность заключается в том, чтобы выявить базис и поддерживать его актуальность. Зачастую сети развертываются без определения ясного базиса. Хуже того, по мере развития и изменений, происходящих в сети, базисы не обновляются. В случае возникновения проблемы (например, снижения производительности вследствие избыточности трафика) перед техническими специалистами встает задача ее точного описания. В этой главе аргументируется важность поддержания сетевого базиса и очерчиваются разнообразные методики, направленные на решение этой задачи, включая применение программы анализа протоколов Observer Suite и оснастки System Monitor, входящей в состав операционной системы Windows 2000 Server (аналогичные приложения можно найти и для систем UNIX/Linux).

Анализ протоколов

Независимо от того, организуете ли вы сеть на пустом месте, или принимаете должность от другого администратора, крайне важно при первой возможности постараться создать качественный сетевой базис. В базисе устанавливаются характеристики производительности сети, характеризуется ее нормальное функционирование. При возникновении неисправности простое сравнение текущей производительности с базисной помогает быстро локализовать потенциально проблемные области. Если вы планируете проведение модернизации сети, обязательно выявите базис перед и

после обновления — таким способом вы сможете обзавестись прекрасной оценкой любых изменений производительности, произошедших после проведения модернизации.

К примеру, было бы странно пытаться получить "нормальные" значения на основе производительности сети в самое напряженное время дня (или недели). Равным образом нельзя взять данные за несколько дней и считать их эталонными. Вместо этого необходимо проследить за сетью, по меньшей мере, на протяжении недели, причем делать это нужно в то время года, когда "дела идут как обычно" — если же вы можете себе позволить взять более длительную выборку (например, несколько недель или месяц), тем лучше. Можно распечатать эти данные в текстовом и графическом формате и хранить их вместе с сетевой документацией.

В случае возникновения неисправности вы можете сделать аналогичные замеры, и сравнить их с базисом — выяснить, какие из собранных статистических данных соответствуют базису, а какие не соответствуют. Предположим, что уровень использования 2-го сегмента вашей сети никогда не превышает 20 процентов; кроме того, при нормальных условиях в нем никогда не фиксируется коэффициент ошибок выше 2 процентов. Если вы обнаруживаете, что уровень использования этого сегмента неожиданно подскочил до 65 процентов, а коэффициент ошибок — до 12 процентов, получается, что сегмент требует дальнейшего анализа. Нетрудно себе представить, что, когда приходит время локализации неисправностей, такая информация оказывается крайне полезной. С другой стороны, если выясняется, что трафик этого сегмента постепенно уменьшается, хотя в нем работает все большее количество пользователей, считайте, что у вас на руках уже есть информация, на основе которой можно рекомендовать проведение модернизации сети, направленной на обеспечение соответствия объемам обработки.

Средства мониторинга сетей

Естественно, одного осознания значимости сетевого базиса недостаточно; следующая задача заключается в определении тех статистических данных, которые нужно учитывать в базисе. Аналитические инструментальные средства наподобие анализаторов протоколов способны захватывать и фиксировать значительные объемы данных — именно их удобно считать наиболее практичными данными, учет которых проводится в базисе.

Уровень использования

По существу, уровень использования — это процентное отношение, выражающее количество бит, перемещающихся по сети, разделенное на общее количество бит, передачу которого эта сеть может обеспечить. Числитель обычно называется выработкой (throughput), а знаменатель — пропускной способностью (bandwidth) сети. Таким образом, формула принимает следующий вид:

Уровень использования = (*выработка/пропускная способность*) × 100%

К примеру, если пропускная способность вашей сети приравнивается к 100 Мбит/с, а выработка фиксируется на уровне 50 Мбит/с, значит, уровень использовании сети равен 50 процентам (50/100 × 100%). В таком случае можно сказать, что используется 50 процентов пропускной способности. Этот уровень является приемлемым в

условиях сети типа маркерного кольца, но в сетях Ethernet он способствует снижению производительности (повышение уровня использования может привести к падению производительности вследствие избыточных конфликтов).

Для сетевого администратора данные об уровне использования представляют исключительную ценность. Если в провода втискивается больше информации, чем они могут обработать, происходит перенасыщение, результатом которого может стать повреждение данных. К примеру, одна рабочая станция, отправляющая широковещательные сообщения, может задействовать всю пропускную способность и не позволить другим пользователям передавать и принимать данные. Уровень использования обычно представляется в форме минимального, максимального и среднего значений. Полезно знать, что при значительном повышении сетевой активности в сети фиксируются пики, но в среднем уровень использования должен принимать значение, подходящее для данной сетевой архитектуры. Критические процентные показатели уровня использования для сетей Ethernet и маркерного кольца неодинаковы. К примеру, считается, что при среднем уровне использования в 30 процентов сеть Ethernet пора сегментировать; в то же время сеть типа маркерного кольца зачастую выдерживает уровень использования до 65—75 процентов, и необходимость в ее сегментации возникает лишь после превышения этого уровня. Имейте в виду, что это лишь общие нормы. Известны случаи, когда в клиент-серверных средах с хорошим сопровождением и ограниченным количеством станций допустимый уровень использования достигал 90 процентов — зачастую причиной возникновения конфликтов, которые, в свою очередь, ограничивают уровень использования, является наличие слишком большого количества станций.

Примечание

Некоторые анализаторы протоколов предусматривают более детальное распределение уровня использования по протоколам — в таком случае у вас появляется возможность выявления протоколов, непомерно использующих пропускную способность сети.

Проверка уровня использования

Инструментальные средства наподобие Observer Suite (пакет наблюдателя) предусматривают возможность отслеживания уровня использования, причем управление этой процедурой осуществляется одной кнопкой. Результатом нажатия кнопки **Utilization History (UH)** (Предыстория использования) является вывод диалогового окна **Utilization History** (рис. 27.1). График обновляется каждые 30 секунд. Исходя из представленного на рис. 27.1 графика, мы выясняем, что максимальный (пиковый) уровень использования, зафиксированный за краткий период тестирования, составил 10 процентов, а средний уровень использования равен лишь 0,2 процента. Показания индикатора **Utilization History** сбрасываются нажатием кнопки **Clear** (Очистить), причем его данные можно сохранить в файле с разделяющими запятыми — для этого нужно выбрать в главном меню Observer пункты **File, Save Mode in Comma Delimited Format** (Файл, Сохранить в формате с разделяющими запятыми).

Проверка эффективности

Тест Efficiency History программы Observer Suite создает снимок текущей эффективности локальной сети. Этот инструмент часто используется для оценки эффективности

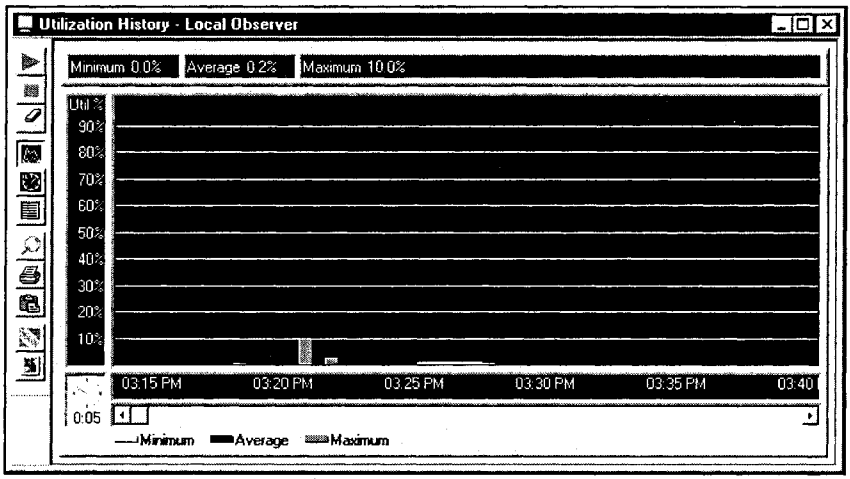


Рис. 27.1. Уровень использования выражает степень потребления доступной пропускной способности сети

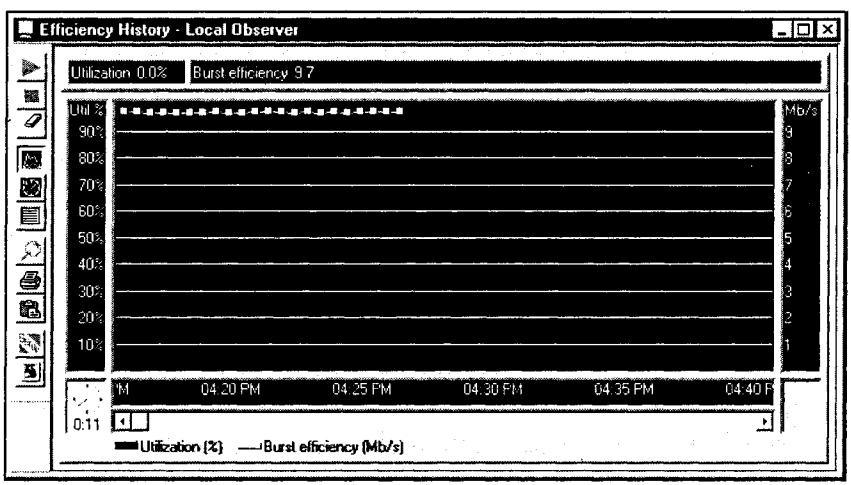


Рис. 27.2. Эффективность выражает способность локальной сети к передаче данных и помогает измерять действенность обновлений и реконфигурации сети

(или неэффективности) изменений и преобразований установок или настроек сети. Многие администраторы задействуют этот инструмент как измеритель, данные с которого снимаются перед внесением в сеть изменений, и сразу после их завершения. Если эффективность снижается, вы понимаете, что изменение оказало негативное воздействие на способность локальной сети к передаче данных. Если показатель повышается, значит, воздействие было благоприятным. Нажатие кнопки **Efficiency History (EH)** (Предыстория эффективности) приводит к появлению диалогового окна **Efficiency History** (рис. 27.2). В соответствии с приведенными на

рис. 27.2 показателями, эффективность локальной сети приблизительно равна 97 процентам (9,7 Мбит/с в сегменте с пропускной способностью 10 Мбит/с).

Когда инструмент Efficiency History находится в активном состоянии, тест выполняется каждые 10 секунд. Он заключается в передаче программой Observer в локальную сеть 70 (для Ethernet и Fast Ethernet) или 30 (для маркерного кольца) пакетов. Эти пакеты анализируются на предмет способности локальной сети принять информационный поток. Результаты выводятся в Мбит/с. Генерируемый средством Efficiency History сетевой трафик незначителен — он не оказывает сколько-нибудь серьезного влияния на общую производительность сети.

Модели трафика

Анализ моделей сетевого трафика может предоставить администратору еще больше ценной информации — например, при помощи этой процедуры выявляются сегменты (и конкретные рабочие станции), генерирующие избыточный трафик и приводящие к снижению производительности. Скажем, если два узла забивают сегмент своим трафиком, то администратору, вероятно, придется изолировать их, поместив в разные сетевые сегменты.

Чтобы определить, какой тип трафика передается по сети, нужно провести его анализ — измерить количество кадров и их средние длины. Короткие кадры могут свидетельствовать о большом количестве запросов баз данных, а большие кадры — о передаче файлов. Зная, какой вид трафик перемещается в сети (и когда возникают пиковые периоды), вам будет удобнее планировать время для выполнения конкретных действий. К примеру, если какой-то пользователь каждое утро отправляет файлы другому узлу, возможно, эти передачи следует перенести на ночь, когда сеть не настолько загружена.

Основные источники сообщений

Утилиты наподобие Observer Suite способны генерировать списки основных источников сообщений, присутствующих в сети. Функция Top Talkers ("самые разговорчивые") показывает все станции локальной сети, а также выводит статистические данные по широковещательным/многоадресным передачам. Эти данные представляют собой детальную статистику по потоку трафика; в них могут содержаться указания на отклоняющиеся от нормы станции, широковещательные/многоадресные штормы или несбалансированный коммутатор. Нажатие кнопки **Top Talker (TT)** приводит к открытию диалогового окна **Top Talkers Statistics** (рис. 27.3). На его графике статистические данные могут выстраиваться как по MAC-адресу (аппаратному сетевому адресу), так и по IP-адресу. Нажатие кнопки **MAC** или **IP** на панели выбора помогает выбрать нужное представление. К примеру, на рис. 27.3 показано, что станция 162.168.168.6 является самой загруженной в пределах данного сегмента; за ней следует широковещательный трафик, исходящий от 255.255.255.255.

Примечание

Если вы собираетесь установить коммутатор, имейте в виду, что данные Top Talker помогают эффективно разделить станции. После установки коммутатора включите коммутационную версию этого режима и проверьте сбалансированность нагрузки на порты.

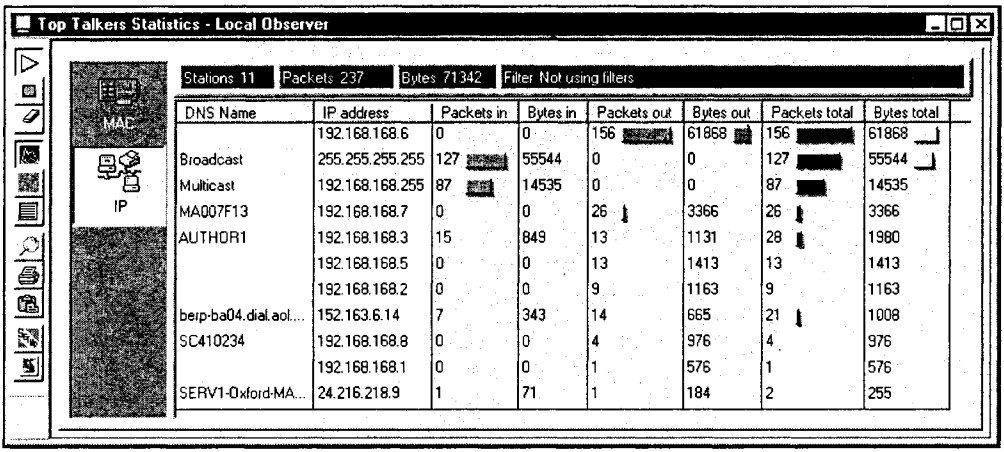


Рис. 27.3. Данные Top Talkers помогают выявить станции, генерирующие большую часть трафика в пределах указанного сегмента

Проверка сетевой активности

Дисплей сетевой активности (Network Activity Display, NAD) — это один из инструментов Observer Suite; он демонстрирует критический уровень использования сети и данные о широковещании, представленные перпендикулярно линии отсчета пакетного трафика. На графике выводится информация о степени исправности локальной сети; здесь же выводятся предупреждения о предстоящих замедлениях, обусловленных опознанными широковещательными или многоадресными штормами (storm). Нажатие на кнопку **Network Activity Display (NAD)** приводит к появлению диалогового окна **Network Activity Display** (рис. 27.4). На графике в четырех квадрантах представлены многоадресные сообщения, пакеты, уровень использования и широковещательные сообщения.

Индикаторные линии меняют цвет, облегчая таким способом задачу просмотра конкретных сетевых состояний. Если индикаторная линия окрашена в желтый цвет, NAD демонстрирует состояние практического бездействия сети (общий уровень использования сети ниже 5 процентов). В таком случае процентная доля широковещательных или многоадресных сообщений в сравнении с реальным трафиком может оказаться высоким. Впрочем, поскольку уровень трафика не высок, такое состояние не имеет статистической значимости. Если отрезок индикаторной линии становится зеленым, NAD демонстрирует нормальное состояние сети. Если отрезок индикаторной линии становится красным, NAD извещает о состоянии нагрузки — оно не обязательно связано с какой-либо неприятностью, но, по меньшей мере, вы должны об этом знать.

Состояния нагрузки могут означать разные вещи, в зависимости от того, где они появляются. Обычно красная линия обозначает превышение некоего порога. Синие линии отображаются в положении, где этот порог может свидетельствовать о появлении неисправности. По умолчанию красные линии могут появиться, если многоадресный и широковещательный трафики составляют более 10 процентов общего уровня использования сети (или если общий уровень использования сети превышает

35-процентный порог). Данные NAD можно сохранить в файле с разделяющими запятыми — для этого нужно выбрать в меню **File** пункт **Save Mode in Comma Delimited Format**.

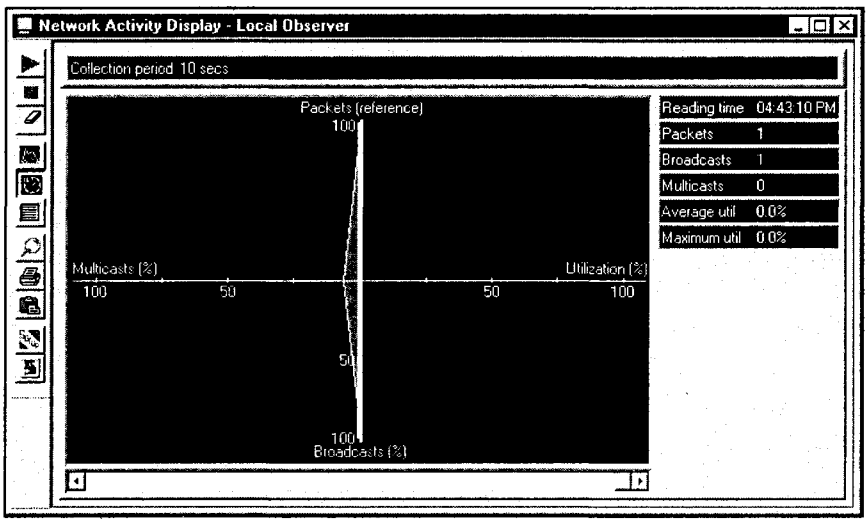


Рис. 27.4. Инструмент Network Activity Display иллюстрирует количество пакетов в сравнении с количеством многоадресных и широковещательных сообщений и уровнем использования

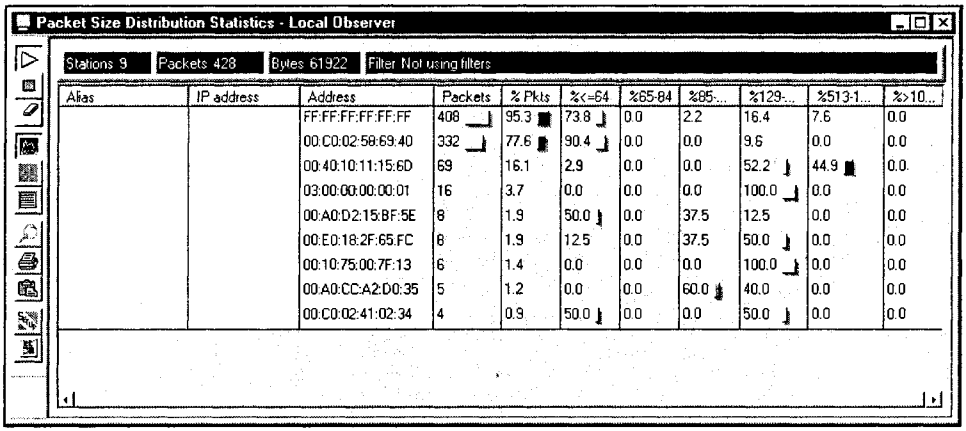
Распределение по размеру пакетов

Инструмент Packet Size Distribution Statistics анализирует состав трафика каждой станции локальной сети и выделяет соответствующие этим станциям модели трафика (разделяемые по размеру пакетов). Эта информация может помочь быстро определить проблемы сети, связанные с потоком трафика, и выявить станции или маршрутизаторы, которые отправляют по большей части небольшие пакеты, а также другие станции и маршрутизаторы — те, которые обычно отправляют более крупные пакеты. Нажатие кнопки **Packet Size Distribution Statistics (SDS)** (статистика распределения пакетов по размерам) приводит к появлению диалогового окна **Packet Size Distribution Statistics** (рис. 27.5). Для каждой станции выводятся данные о количестве пакетов, процентный показатель трафика и процентная доля пакетов в нескольких размерных диапазонах:

- 64 байт или менее;
- 65—84 байт;
- 85—128 байт;
- 129—512 байт;
- 513—1024 байт;
- 1025 байт и более.

Коэффициенты ошибок

Способность измерять и анализировать ошибки, возникающие в сети, также имеет огромное значение. Узел, отправивший кадр с ошибкой, должен осуществить его повторную передачу. Неисправный узел, выполняющий повторную передачу пакетов,



Alias	IP address	Address	Packets	% Pkts	%<=64	%65-84	%85-...	%129-...	%513-1...	%>10...
		FF:FF:FF:FF:FF:FF	408	95.3	73.8	0.0	2.2	16.4	7.6	0.0
		00:C0:02:58:69:40	332	77.6	90.4	0.0	0.0	9.6	0.0	0.0
		00:40:10:11:15:6D	69	16.1	2.9	0.0	0.0	52.2	44.9	0.0
		03:00:00:00:00:01	16	3.7	0.0	0.0	0.0	100.0	0.0	0.0
		00:A0:D2:15:BF:5E	8	1.9	50.0	0.0	37.5	12.5	0.0	0.0
		00:E0:18:2F:65:FC	8	1.9	12.5	0.0	37.5	50.0	0.0	0.0
		00:10:75:00:7F:13	6	1.4	0.0	0.0	0.0	100.0	0.0	0.0
		00:A0:CC:A2:D0:35	5	1.2	0.0	0.0	60.0	40.0	0.0	0.0
		00:C0:02:41:02:34	4	0.9	50.0	0.0	0.0	50.0	0.0	0.0

Рис. 27.5. Распределение пакетов по размеру помогает определить характеристики трафика для каждой станции, присутствующей в локальной сети

может создавать большие объемы ненужного сетевого трафика. Возросшие коэффициенты ошибок в отдельных сегментах или на отдельных станциях в любом случае нуждаются в анализе, т. к. они являются первыми свидетельствами предстоящей неисправности оборудования (концентраторов, коммутаторов, сетевых плат и т. д.). Анализатор пакетов способен оперативно выводить данные об обычных ошибках, предшествующих появлению неисправностей в сети (подробное обсуждение процедур поиска неисправности с помощью анализатора пакетов приводится в *гл. 30*).

Проверка пакетов

Анализаторы, подобные Observer Suite, могут захватывать и отображать статистические данные о пакетах. Нажатие кнопки **Packet Capture (PC)** (Захват пакета) приводит к открытию диалогового окна **Packet Capture**. По умолчанию на экран выводится график, а для того, чтобы просмотреть результаты в табличной форме, нужно переключиться в представление **List** (список) (рис. 27.6). В дополнение к базовой информации о трафике, вы увидите перечисление выброшенных пакетов и указания на другие ошибки, связанные с контролем на основе циклического избыточного кода (CRC), выравниванием и крайне малым размером кадров. Когда количество таких ошибок становится существенным, необходимо предпринимать меры. К примеру, рост количества выброшенных пакетов в рамках сегмента сети может свидетельствовать об избыточном объеме трафика и служить заблаговременным указанием на необходимость модернизации. Естественно, что, когда такие проблемы появляются внезапно или нерегулярно, их нужно устранять.

Проверка основных показателей

Режим Network Vital Signs в программе Observer Suite демонстрирует текущую активность локальной сети с ее привязкой к текущим сбойным состояниям в этой сети. Этот индикатор разрабатывался с расчетом на вывод комплексного снимка сбойных состояний (и обозначение важности этих состояний в сравнении с текущей активностью в локальной сети). Нажатие кнопки **Network Vital Signs** (Основные показатели сети) приводит к открытию диалогового окна **Ethernet Vital Signs and Collision**

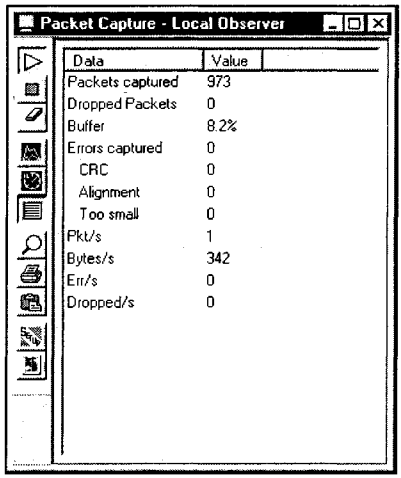


Рис. 27.6. Анализатор пакетов может применяться для оперативного подсчета обычных ошибок трафика

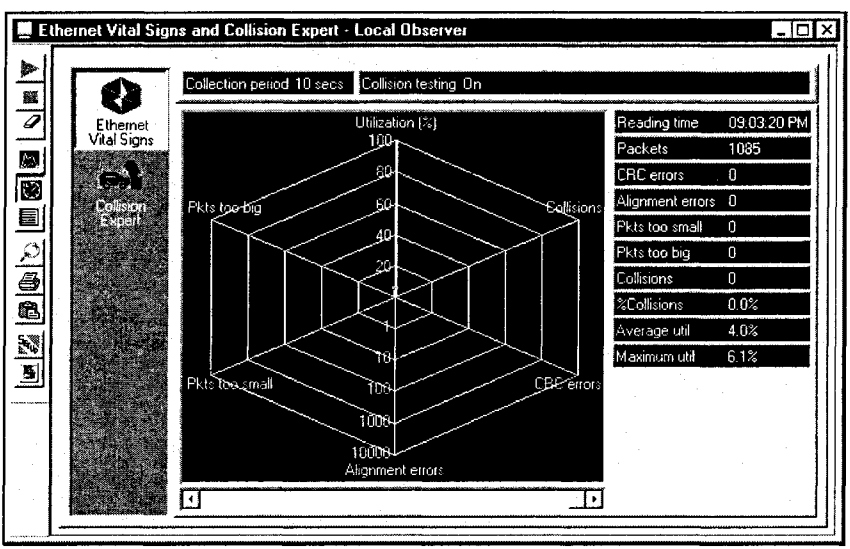


Рис. 27.7. Некоторые анализаторы пакетов способны отображать уровень использования сети с учетом обычных ошибок; таким способом они предоставляют вам возможность быстро оценить серьезность сетевых ошибок

Expert (Эксперт важнейших признаков и коллизий сети Ethernet) (рис. 27.7). Индикатор информирует вас о состоянии ошибки и ее серьезности с учетом состояний трафика; при этом графические формы сочетаются с определенными цветовыми кодами.

Как и в случае с индикатором Network Activity Display, у применяемых здесь цветов есть смысловая нагрузка. Желтая линия, присутствующая в каком-либо месте гра-

фика, обозначает состояние простоя. Другими словами, независимо от отображаемых данных, активность настолько низка, что все ошибки не имеют статистической важности. Зеленая линия демонстрирует нормальную сетевую активность и подсчет ошибок. Красная линия говорит о том, что количество ошибок выходит за рамки "нормального" диапазона. Когда на экране изображается красная линия, синяя линия соединяет это состояние ошибки с предположительно связанными с ней или попадающими под ее влияние частями графика. Красная линия появляется на индикаторе в случае появления следующих ошибок:

- уровень использования превышает 35-процентный порог;
- ошибки, связанные с контролем CRC и чрезмерно малым размером пакетов, встречаются более чем в 25 процентах общего объема трафика;
- ошибки, связанные со слишком большим размером пакетов, встречаются более чем в 1 проценте общего объема трафика.

Анализ сетевых тенденций

Для эффективного управления локальной сетью зачастую требуется анализ тенденций сетевого трафика, причем длительность этого анализа может исчисляться днями, неделями, и даже месяцами. Вместо того чтобы собирать и знакомиться с текущей сетевой статистикой, режим Network Trending программы Observer Suite (совместно с Network Trending Viewer) позволяет администраторам автоматически собирать, хранить, просматривать или анализировать статистику сетевого трафика, относящуюся к продолжительным периодам — именно эта функция Observer Suite является важнейшей из всех, связанных с определением базиса. Статистические данные хранятся в формате, который можно без труда сжать и просмотреть на любом узле с установленной утилитой анализа сетевых тенденций (Network Trending Viewer). После сбора данных их можно представить в виде графика или в формате списка, причем информация масштабируется и может распространяться на всю сеть, на каждую присутствующую в этой сети станцию, на любой момент времени в течение периода сбора. Кроме того, анализ сетевых тенденций помогает создавать текстовые отчеты о сетевых состояниях в указываемые периоды.

Сбор информации

Для выявления базиса сети требуется некоторое время, и чем дольше период сбора данных, тем лучше получается базис. Одновременно с открытием программы Observer Suite автоматически запускается инструментальная панель анализа сетевых тенденций (рис. 27.8). На этой инструментальной панели представлен постоянный управляемый индикатор общих сетевых тенденций, тенденций сети Интернет и состояний центральных процессоров в рамках наблюдаемого сегмента. Есть два маркера хода выполнения (улитки). На одном демонстрируется ход выполнения анализа сетевых тенденций, а на другом — ход выполнения анализа наблюдаемых тенденций в Интернете. К примеру, если интервал сбора данных равен одному часу, то для того, чтобы переползти с левой стороны полосы выполнения на ее правую сторону улитке потребуется один час — таким образом, вы получаете возможность быстрого определения состояния сбора данных.

Панель **Network Trending** (Сетевая деятельность) состоит из следующих элементов.

- **Interval**. Период времени, отведенный на сбор данных.
- **Stations**. Количество сетевых станций, осуществивших отправку трафика за указанный период времени.
- **Packets**. Количество пакетов, отправленных по сети за указанный период времени.
- **Bytes**. Количество байт, отправленных по сети за указанный период времени.
- **Start Time**. Начальный момент указанного периода времени.
- **End Time**. Конечный момент указанного периода времени.
- **Current Time**. Текущее время.

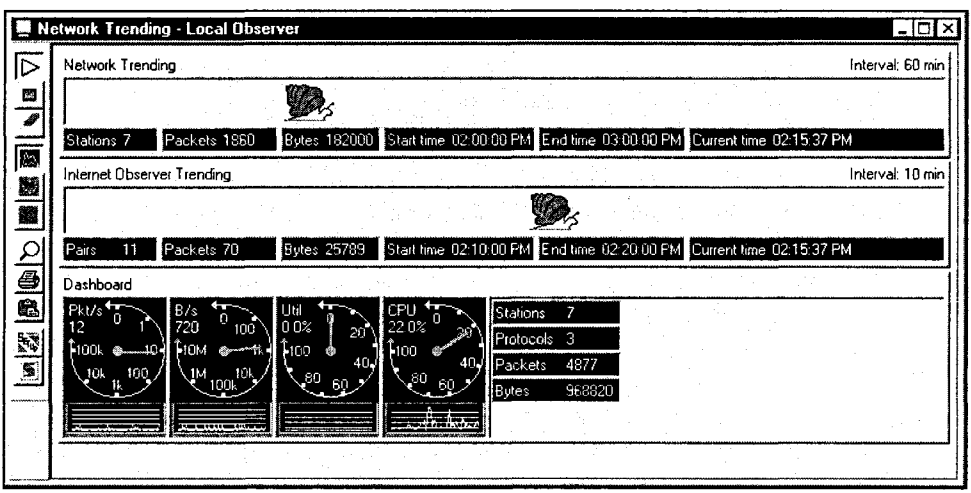


Рис. 27.8. Анализ сетевых тенденций позволяет отслеживать поведение локальной сети во времени для последующего изучения и анализа

Панель **Internet Observer Trending** (Наблюдение тенденций в Интернете) содержит следующие элементы.

- **Pairs**. Количество пар сетевых станций, осуществивших обмен IP-трафиком за указанный период времени.
- **Packets**. Количество IP-пакетов, отправленных по сети за указанный период времени.
- **Bytes**. Количество байт, отправленных в сетевых IP-пакетах за указанный период времени.
- **Start Time**. Начальный момент указанного периода времени.
- **End Time**. Конечный момент указанного периода времени.
- **Current Time**. Текущее время.

Кроме того, есть четыре индикатора с круговыми шкалами.

- **Packets per second (Pks/s)**. Отображает данные о частоте отправки пакетов (пакеты в секунду) на круговой шкале и в виде истории прошедших событий (график под круговой шкалой).
- **Bytes per second (B/s)**. Отображает частоту отправки данных (байт в секунду) на круговой шкале и в виде истории прошедших событий (график под круговой шкалой).
- **Bandwidth Utilization (Util)**. Отображает уровень использования пропускной способности в рамках наблюдаемого в текущий момент сегмента — данные выводятся на круговой шкале и в виде истории прошедших событий (график под круговой шкалой).
- **Processor Utilization (CPU)**. Отображает текущий уровень использования процессора на локальном (испытуемом) компьютере, — данные выводятся на круговой шкале и в виде истории прошедших событий (график под круговой шкалой).

Наконец, справа от индикаторов с круговыми шкалами есть еще четыре дополнительных элемента.

- **Stations**. Количество станций в сети, осуществивших отправку трафика во время текущего сеанса анализа сетевых тенденций.
- **Protocols**. Количество протоколов, задействованных в сети во время текущего сеанса анализа сетевых тенденций.
- **Packets**. Количество пакетов, отправленных по сети во время текущего сеанса анализа сетевых тенденций.
- **Bytes**. Количество байт, отправленных по сети во время текущего сеанса анализа сетевых тенденций.

Программа Observer позволяет вам выполнять специальные настройки анализатора сетевых тенденций путем добавления или редактирования подчиненных протоколов IP (которые должны быть включены в анализ), изменения дней и времени проведения анализа тенденций, а также определения интервалов между сеансами сбора данных.

Просмотр результатов

После сбора данных для составления базиса их нужно обработать и проанализировать — результаты этих действий помогут вам сформулировать выводы и документировать сеть. Для предоставления данных о тенденциях в Observer Suite применяется утилита просмотра сетевых тенденций (Network Trending Viewer). Эта утилита может выводить собранные статистические данные в виде графиков или списков, распространять эти данные на сеть в целом, на каждую отдельную станцию, установленную в сети, и на любой момент времени. Нажатие кнопки **Load Network Trending Viewer** (Загрузить утилиту просмотра сетевых тенденций) приводит к появлению на экране диалогового окна **Network Trending Viewer** (рис. 27.9).

Дерево просмотра, расположенное слева, содержит перечень имеющихся и готовых для анализа данных, связанных с тенденциями. На рис. 27.9 данные относятся к среде, 9 января 2002 года. Ветви, корневые записи которых оканчиваются на

"Observer" или "Probe", содержат данные результатов анализа сетевых тенденций. Ветви, корневые записи которых оканчиваются на "(Internet)", содержат данные Internet Observer. Ветви, корневые записи которых оканчиваются на "(Switch)", содержат данные анализа коммутации. Пиктограммы, расположенные в левой части рабочего пространства, предназначены для выбора следующих статистических данных.

- **Station activity time**. Вывод времени первого и последнего наблюдения каждой станции в локальной сети.
- **Top talkers**. Вывод списка всех станций с указанием общего количества исходящих и входящих пакетов и общего объема исходящих и входящих байт для каждой станции (см. рис. 27.9).
- **Packet size distribution**. Отображение распределения пакетов по размеру.
- **Bandwidth utilization**. Эта опция демонстрирует уровень использования пропускной способности (максимальный, средний и минимальный) за указанный день (или дни).

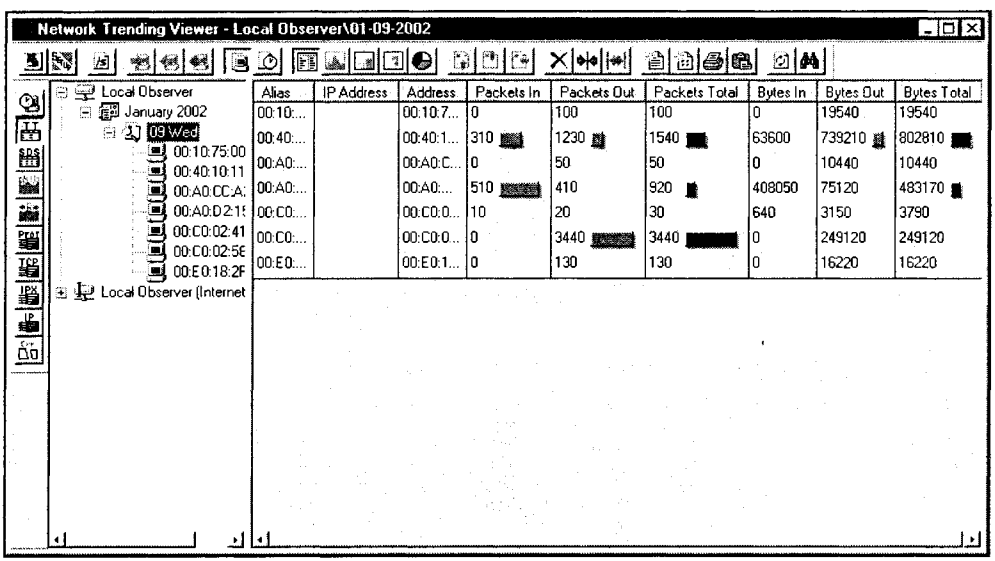


Рис. 27.9. После проведения анализа сетевых тенденций вы можете просмотреть его результаты (например, данные об основных источниках сообщений) за указанные дни

- **Router bandwidth utilization**. Вывод данных об уровне использования пропускной способности маршрутизатора в общем пакетном или процентном форматах. Помните, что для просмотра статистических данных в этом диалоговом окне, в режиме Router Observer программы Observer нужно выбрать маршрутизатор и скорость маршрутизатора, и в соответствующем списке указать нужный маршрутизатор.
- **Protocols**. Вывод данных о протоколах, наблюдаемых в локальной сети. Среди возможных типов числятся TCP/IP, IPX/SPX, NetBIOS (включая NetBEUI), AppleTalk, DECNET, SNA и Other (Другие).

- **TCP/IP subprotocols**. Отображение информации о подчиненных протоколах TCP/IP, наблюдаемых в локальной сети; они классифицируются по типам, среди которых числятся ARP, RARP, IP, TCP, UDP, ICMP и Other (Другие).
- **IPX Subprotocols**. Эта опция выводит данные о подчиненных протоколах IPX/SPX, наблюдаемых в локальной сети; они классифицируются по типам, среди которых числятся SPX, IPX, SAP, NCP, RIP, NetBIOS, Diagn (Diagnostic), WatchDog, Serializ (Serialization) и Other (Другие).
- **IP Applications**. Выводить данные о настраиваемых (на основе портов) IP-приложениях. Их настройка производится в диалоговых окнах **Network Trending Setup**.
- **Errors**. Содержание этого режима отображения зависит от топологии анализируемой сети (могут фиксироваться, к примеру, ошибки кадров маркерного кольца, Ethernet или FDDI).

Отбор отдельных статистических данных позволяет вам идентифицировать станции, для работы которых требуется необычно большие объемы сетевого времени; станции, отсылающие необычно крупные (или мелкие) пакеты, применяющие непредвиденные протоколы, сталкивающиеся с ошибками, и т. д. К примеру, если вы укажете конкретную станцию на левой панели (00:10:75:00:7F:13), выберите **Packet Size Distribution (SDS)**, а затем перейдете в режим **Alternate Columns Graph** (Диаграмма чередующихся столбцов) (рис. 27.10), вы без труда обнаружите, что размер пакетов, в пересылке которых участвовала эта станция, в основном, составлял 129—512 байт.

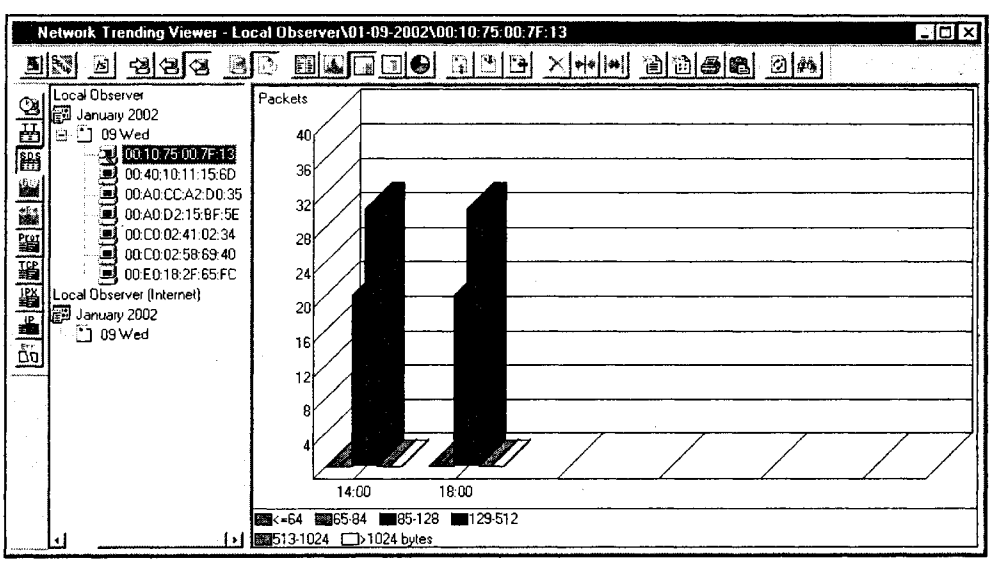


Рис. 27.10. Инструменты вычерчивания графиков позволяют без труда сравнивать данные анализа тенденций в локальной сети

Наконец, строка пиктограмм в верхней части рабочего пространства представляет доступные опции; в целом, эти пиктограммы позволяют выбирать опции представ-

ления (например, график, круговая шкала или список), управляющие методом вывода статистических данных, создавать и распечатывать отчеты, выполнять другие операции.

Дополнительная статистика

Статистические данные, оценивающие трафик и ошибки, без сомнения, помогают определить надежный базис для вашей сети, однако есть множество других атрибутов производительности сети, которые можно измерить и учесть при выявлении базиса. Инструментальные средства, подобные Observer Suite, предусматривают возможность измерения производительности сетевых маршрутизаторов, Web и Интернета; сейчас мы вкратце рассмотрим эти функции.

Производительность маршрутизаторов

В Observer Suite есть режим Router Observer, который позволяет наблюдать за маршрутизатором (или группой маршрутизаторов) в реальном времени и замерять уровень его использования. Вполне возможно, что с помощью этого режима вы довольно быстро обнаружите, что маршрутизатор является узким местом, и сможете выявить, какие пакеты препятствуют нормальной работе этого устройства: входящие или исходящие (или, может быть, и те, и другие). Путем анализа предыстории вы сможете определить, является ли выявленная проблема постоянной (что может свидетельствовать о необходимости обеспечения более высокой скорости соединения), или выбросом, указывающим на некий сбой. Observer выполняет пассивные измерения, так что анализатор не оказывает неблагоприятного воздействия на производительность маршрутизатора. Чтобы перейти в режим Router Observer, выберите **Router Observer** на панели инструментов программы Observer — в результате появится диалоговое окно **Router Observer**. В этом окне отобразятся данные о скорости передачи пакетов (пакеты в секунду), скорости передачи данных (байт в секунду) и процент использования IP-адреса указанного маршрутизатора.

Web Observer

Этот режим предназначен для проведения анализа Web-сервера с точки зрения входящего и исходящего потоков трафика для данного сервера. Работая в этом режиме, Observer сосредотачивается на всем трафике, проходящем через порт 80 (это порт, принимаемый по умолчанию для Web-трафика), или на всем исходящем и входящем трафике указанного устройства. Чтобы перейти в режим Web Observer, нажмите кнопку **Web Observer** — в результате откроется диалоговое окно **Web Observer** (рис. 27.11). На его основном индикаторе обозначается адрес Web-сервера и круговая шкала времени отклика на тест ICMP Ping. Если сервер выходит из строя, индикатор круговой шкалы превращается в индикатор прерванного соединения. Чтобы выполнить необходимые настройки, нажмите кнопку **Setup**:

- вы можете выбрать **Select a Web server from the list** (Выберите Web-сервер из списка), чтобы указать IP-адрес сервера (включая псевдоним и комментарий);
- вы можете использовать текстовое поле **Remove inactive IP addresses after (min)** (Удалить неактивный IP-адрес через (мин)) для определения периода времени, в течение которого IP-адреса сохраняются в таблице и по прошествии которого они считаются неактивными.

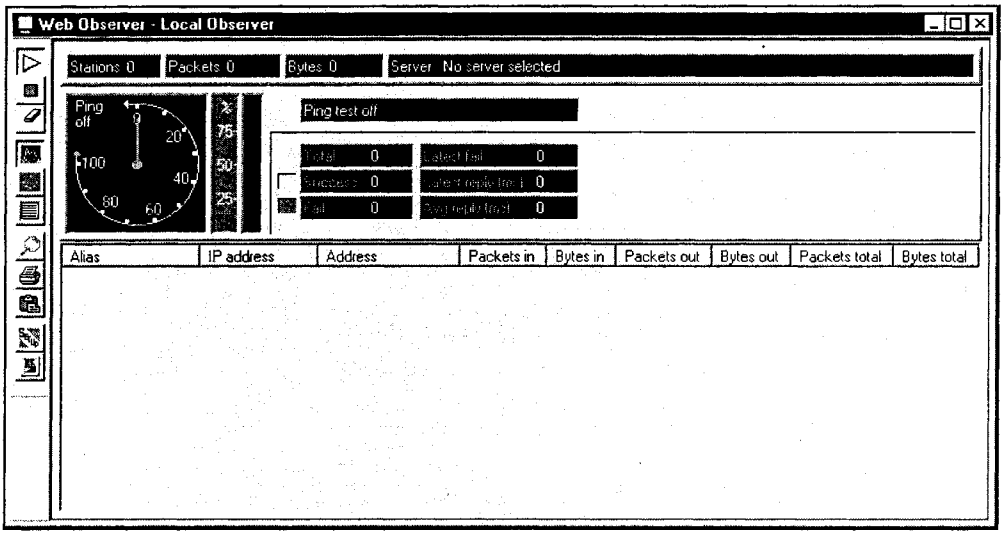


Рис. 27.11. Инструментальные средства, подобные Web Observer, позволяют выявить базис функционирования Web-сервера

Утилита Web Observer отображает следующие элементы.

- **Stations**. Количество станций, осуществивших обмен трафиком с указанным сервером, во время работы Web Observer, минус станции, чьи IP-адреса были удалены из таблицы.
- **Packets**. Общее количество пакетов, переданных и полученных указанным сервером во время работы Web Observer.
- **Bytes**. Общее количество байт, переданных и полученных указанной станцией во время работы Web Observer.
- **Server**. Здесь выводятся имя, IP-адрес и MAC-адрес указанного Web-сервера.
- **Overall average packets per second**. Здесь выводится среднее количество пакетов, обрабатываемых указанным Web-сервером за одну секунду.
- **Overall average bytes per second**. Здесь выводится среднее количество байт, обрабатываемое Web-сервером за одну секунду.
- **Overall average utilization**. Здесь выводится средний уровень использования указанного Web-сервера.

На индикаторе нижней панели Observer приводит список IP-адресов, которые в данный момент осуществляют обмен данными с определенным Web-сервером. При этом указывается следующая информация.

- **Alias**. Здесь выводится имя, присвоенное зарегистрированной станции в режиме Discover Network Names.
- **IP Address**. IP-адрес зарегистрированной станции.
- **Address**. MAC-адрес зарегистрированной станции.

- **In packets**. Здесь приводится количество пакетов, отправленных к выбранной станции от указанного Web-сервера.
- **In bytes**. Здесь приводится количество байт, отправленных к выбранной станции от указанного Web-сервера.
- **Out packets**. Здесь приводится количество пакетов, отправленных.
- **Out bytes**. Здесь приводится количество байт, отправленных от выбранной станции к указанному Web-серверу.
- **Total packets**. Здесь приводится общее количество пакетов, отправленных в обоих направлениях между выбранной станцией и указанным Web-сервером.
- **Total bytes**. Здесь приводится общее количество байт, отправленных в обоих направлениях между выбранной станцией и указанным Web-сервером.
- **In % util**. Суммарный процентный показатель уровня использования для сообщений, полученных выбранной станцией от указанного Web-сервера.
- **Out % util**. Суммарный процентный показатель уровня использования для сообщений, полученных указанным Web-сервером от выбранной станции.

Internet Observer

Режим Internet Observer предусматривает возможность анализа интернет-трафика в локальной сети. Его можно применить для мониторинга общего уровня использования Интернета со стороны отдельной станции или станций. Кроме того, показатель использования Интернета можно разделить по подчиненным протоколам (например, для того чтобы определить, какую часть интернет-трафика занимает WWW или почта POP). Отслеживание уровня использования Интернета может производиться при помощи представлений **Internet Patrol**, **IP Pairs (Matrix)** и **IP SubProtocols**. Чтобы перейти в режим Internet Observer, нажмите на главной панели инструментов кнопку **Internet Observer** — в результате на экране появится диалоговое окно **Internet Observer**.

В представлении **Internet Patrol** выводятся данные о трафике между MAC-адресами и IP-адресами 3-го уровня. Если для истинного MAC-адреса назначен псевдоним, то указываться будет именно он. Кроме того, IP-адреса узлов назначения будут разрешаться средствами DNS. Такое представление интернет-трафика оптимально для анализа локального сетевого трафика в направлении Интернета и из Интернета, а также для узлов, применяющих DHCP. Так как DHCP часто перераспределяет IP-адреса, идентификация IP-адресов источника на узле DHCP бесполезна. В представлении **IP to IP Pairs (Matrix)** приводится трафик между истинными IP-адресами 3-го уровня. Это представление интернет-трафика оптимально для локальных сегментов, взаимодействующих с Интернетом, а также для магистрального потока трафика. В локальной сети это представление полностью отражает уровень использования Интернета лишь в том случае, если IP-адреса являются статическими. Если же в локальной сети применяется DHCP, то просмотр интернет-трафика должен производиться в режиме **Internet Patrol**. В представлении **IP Subprotocols** приводится поток трафика между IP-адресами 3-го уровня, разделенный по подчиненным протоколам. Подчиненные протоколы определяются в диалоговом окне настройки. Предусматривается возможность создания двенадцати таких протоколов, настраиваемых

пользователем (метка "Other" обозначает протокол, не соответствующий ни одному из этих 12 определяемых пользователем протоколов).

Не забывайте о своей безопасности

Безопасность — это еще один фактор, который необходимо принимать во внимание, пользуясь анализатором протоколов. Не забывайте, что анализатор протоколов может собирать пакеты данных, перемещающиеся по всей сети — по этой причине существует возможность копирования в вашу систему или ваш отдел конфиденциальной информации. Если вы практикуете отправку захваченных данных сторонней компании, которая занимается их анализом, угроза безопасности может стать еще более насущной. Все данные, собранные посредством анализатора протоколов, следует считать конфиденциальными — подобно корпоративной почте, информации о заработной плате и материалам бухгалтерского учета, которые обычно проходят через сеть. Сетевые администраторы должны разрабатывать процедуры обеспечения защиты совместно с сотрудниками юридического отдела — так они смогут убедиться в соблюдении единых для всей организации требований по неразглашению и конфиденциальности, и только после этого передавать любую подобного рода информацию сторонним лицам.

Примечание

Чтобы обеспечить дополнительный уровень безопасности, не допускайте к анализатору протоколов посторонних лиц.

Системный монитор

Инструментальные средства, подобные Observer Suite, прекрасно подходят для определения базисов обмена информацией в сети, однако вам может потребоваться проведение проверки или документирования аппаратно-ориентированной производительности многочисленных присутствующих в вашей сети серверов. Установление базиса для памяти, процессора и уровня использования диска впоследствии поможет выявить необычные нагрузки на сервер и определить необходимость обновлений — например, установки дополнительных модулей оперативной памяти или второго процессора. В этой части главы мы рассмотрим методы анализа сервера при помощи утилиты System Monitor (Системный монитор) (присутствующей в комплекте Windows 2000 Server).

Узкие места и настройка

Узкое место (Bottleneck) образуется в том случае, когда потребление одного или нескольких ресурсов сервера становится настолько значительным, что производительность сервера снижается. К примеру, для запуска тех приложений, которые должны работать на сервере, может не хватить памяти. В результате происходит дополнительное обращение к диску (к файлу подкачки), приводящее к ухудшению производительности сервера. В качестве другого примера можно привести ситуацию, когда избыточный сетевой трафик наблюдается только на одном порте сетевой платы —

невзирая на то, что таких портов на сервере несколько. В подобном случае, для того чтобы добиться равномерности использования портов сетевой платы, могут потребоваться действия, направленные на балансирование сетевого трафика. Узкое место может возникнуть по следующим причинам:

- недостаточно ресурсов (например, не хватает оперативной памяти), и необходимы дополнительные компоненты или модернизация существующих;
- неравномерно распределена рабочая нагрузка между ресурсами и необходимо их балансирование;
- неисправен и требует замены ресурс (например, вышел из строя порт сетевой платы, который приводит к возрастанию объема трафика, проходящего через оставшиеся порты);
- конкретный ресурс монополизирован программой; для устранения этой проблемы может потребоваться переход на другую программу, переделка программы разработчиком, добавление или модернизация ресурсов, или запуск программы в периоды низкой нагрузки;
- неверно сконфигурирован ресурс, и необходимо изменить настройки конфигурации.

Выявив узкое место и сформулировав гипотезу относительно его устранения, разработанное решение необходимо реализовать — настроить сервер, ослабив негативное влияние этого узкого места и повысив производительность. Вне зависимости от того, в чем заключается проблема, единовременно следует выполнять лишь одно изменение. В некоторых случаях неисправность, которая, как вам представляется, связана с одним компонентом, может оказаться результатом наличия узких мест в нескольких компонентах. По этой причине необходимо соблюдать осторожность. Выполнение нескольких изменений за один раз может привести к невозможности оценки влияния каждого из них в отдельности.

Кроме того, мониторинг нужно повторять после каждого изменения. Это позволяет определить воздействие данного изменения и необходимость в последующей регулировке. К примеру, если вы считаете, что узкое место связано с системной памятью, установите дополнительную память, а затем еще раз измерьте производительность — таким путем вы сможете проверить, действительно ли приращение объема памяти привело к устранению проблемы. Помните, что любое отдельное изменение может воздействовать на другие ресурсы, так что после каждого изменения необходимо полностью обновлять комплект базисов. К примеру, установленная дополнительная память способна уменьшить зависимость сервера от дисковой подсистемы (файла подкачки) — следовательно, вполне возможно, что обновление памяти привело к повышению видимой производительности дисковой подсистемы. Путем повторного составления комплекта базисов вы получаете свежее представление о производительности сервера.

Примечание

Не забывайте просматривать журналы регистрации событий — при наличии некоторых проблем, связанных с производительностью, генерируются выходные данные, которые можно вывести в Event Viewer (Просмотр событий).

Выбор компьютера

При удаленном мониторинге компьютера у вас есть несколько возможностей по сбору данных. К примеру, проводить регистрацию производительности можно на компьютере администратора, постоянно извлекая данные с каждого из удаленных ПК. С другой стороны, вы можете запустить службы сбора данных на каждом ПК и использовать пакет программ (с некоторой периодичностью) для передачи этих данных на компьютер администратора, где будет производиться их анализ и архивирование.

Централизованный сбор данных (сбор данных с удаленных ПК, мониторинг которых вы выполняете на локальном компьютере) прост в реализации, т. к. для этого требуется лишь одна служба регистрации. Сбор данных из нескольких систем может производиться в единый файл регистрации. Однако метод вызывает дополнительный сетевой трафик и может ограничиваться доступной памятью на компьютере администратора. Открыв на вашем локальном компьютере утилиту System Monitor, используйте диалоговое окно **Add Counters** (Добавить счетчики) для выбора удаленного ПК. Распределенный сбор данных (сбор данных производится на удаленных ПК, мониторинг которых вы выполняете) не подвержен проблемам с памятью и сетевым трафиком, характерным для централизованного метода сбора. Однако в этом случае данные поступают с задержкой, т. к. предполагается их доставка на компьютер администратора в целях проведения анализа. При распределенном сборе данных выбор удаленного компьютера, на который нужно переправлять данные, следует осуществлять средствами управления локального ПК.

При проведении мониторинга удаленных компьютеров к каждому из таких ПК могут подключиться только те пользовательские учетные записи, которые располагают необходимыми для этого полномочиями. Чтобы запустить мониторинг удаленных систем со своего компьютера, вы должны запустить службу Performance Logs and Alerts (Оповещения и журналы производительности), воспользовавшись для этого учетной записью, которая содержит полномочия на обращение к тем удаленным ПК, за которыми предполагается установить текущее наблюдение. По умолчанию, эта служба запускается с "системной" учетной записью локального компьютера, которая в большинстве случаев предполагает полномочия, подходящие только для обращения к службам локального компьютера. Чтобы запустить эту службу с другой учетной записью, выберите в окне **Computer Management** (Управление компьютером), группу **Services** (Службы), и откорректируйте свойства службы Performance Logs and Alerts.

Производительность памяти

Процесс определения базиса вашего сервера мы начнем с измерения производительности его памяти. Ресурсы процессора и памяти чрезвычайно сильно влияют на функционирование сервера, и поэтому необходимо понять, как программы потребляют эти ресурсы. Для анализа основных элементов процессора и памяти нужна оснастка System Monitor. Запустите System Monitor, и добавьте (кнопка "+", Add — Добавить) в область графика (рис. 27.12) счетчики **Process\% Processor Time** (Процесс\% загруженности процессора) и **Process\Working Set** (Процесс\Рабочее множество памяти). Счетчик **% Processor Time** выражает процентный показатель продолжительности исполнения процессором всех потоков конкретного процесса (если

система не загружена, этот показатель обычно высок для процесса Idle (незанятый)). **Working Set** — это текущее количество байт физической памяти, используемое процессом. Это значение может превышать минимальное количество байт, фактически требующееся процессу. Оно же может включать физические байты, коллективно используемые несколькими процессами.

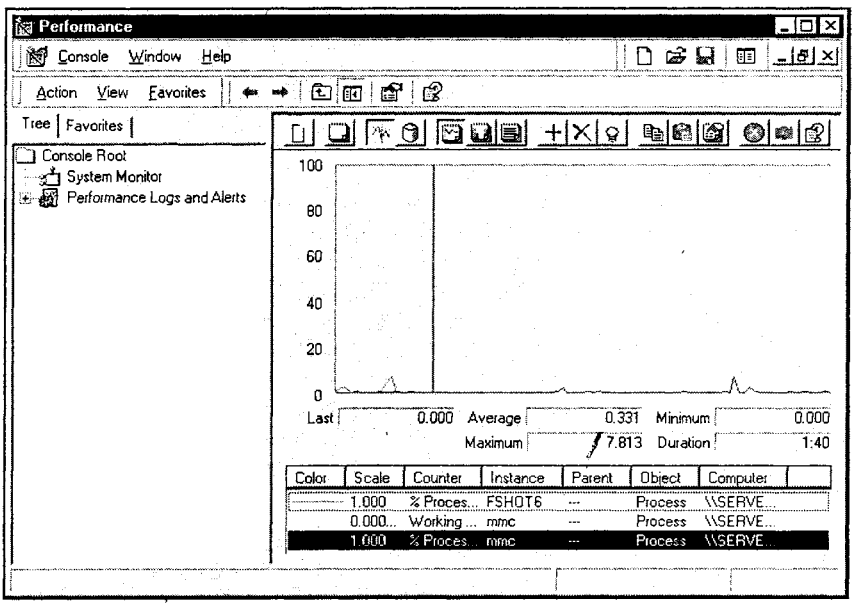


Рис. 27.12. Для формирования базиса производительности памяти и обоснования модернизации серверной памяти применяется утилита System Monitor

При запуске новой программы значения счетчика **Process\% Processor Time** сначала резко увеличиваются для каждой работающей программы, затем снижаются, и наконец, выравниваются. Важно иметь в виду, что при запуске программы уровень потребления ресурсов процессора значительно возрастает; по этой причине высокие значения, полученные временно при запуске, разумно исключить из данных текущего контроля — так вы сможете получить более точную картину типичного использования процессора программами. После запуска на графике должны отражаться периоды повышения активности процессора, которые соответствуют периодам активности программ (связанным, к примеру, со считыванием оснасткой System Monitor очередного комплекта значений счетчика). Вы можете заметить это, изменив интервал обновления System Monitor. Обратите внимание: если System Monitor настроена на короткий интервал обновления, она считывает данные чаще и вызывает большую активность процессора по отношению к себе. Чем длиннее интервал обновления, тем меньше генерируемая активность процессора.

Для каждой программы, исполняемой на компьютере, операционная система выделяет часть физической памяти (working set). Даже если программа демонстрирует полное отсутствие активности, операционная система продолжает выделять ей память. Величина этой памяти начинает представлять интерес, когда показания счет-

чика **Memory\Available Bytes** (Память\Доступно байт) падают ниже заданного порога. Windows 2000 отвечает на запросы программ, связанные с памятью, выделением свободной памяти. По мере того как свободной памяти становится все меньше, операционная система начинает извлекать память из рабочего множества наименее активных программ. Следовательно, вы сможете наблюдать за тем, как значения доступной памяти одной программы будут повышаться, а аналогичные значения других программ — понижаться. Если в системе нет объема памяти, которого могло бы хватить для удовлетворения требований всех активных программ, происходит страничная подкачка памяти и понижение уровня производительности программ.

Недостаточный объем памяти

Для мониторинга ситуации с недостатком памяти нужно воспользоваться счетчиками **Memory\Available Bytes** (Память\Доступно байт) и **Memory\Pages/sec** (Память\Страниц/с). Счетчик **Available Bytes** обозначает количество байт памяти, доступное в текущий момент для потребления процессами. Низкие значения **Available Bytes** (4 Мбайт или менее) могут свидетельствовать об общем недостатке ресурсов памяти на данном компьютере (или о том, что программа не освобождает память). Показатель **Pages/sec** ("страниц в секунду") демонстрирует количество страниц, которые были либо приняты с диска из-за сбоев страницы диска, либо записаны на диск для освобождения пространства рабочего множества в связи с ошибками отсутствия страниц. Если значение **Pages/sec** равняется 20 или более, то анализ активности, связанной с разбиением на страницы, следует продолжать. Высокое значение **Pages/sec** может и не быть свидетельством какой-либо проблемы с памятью, но являться результатом выполнения программы, применяющей отображение файла в памяти.

Если у вас есть основания подозревать наличие утечки памяти (программы, которая не освобождает память), то для анализа поведения памяти нужно задействовать параметры **Memory\Available Bytes** (Память\Доступно байт) и **Memory\Committed Bytes** (Память\Выделено байт), а для мониторинга процессов, которые, по вашему мнению, обуславливают утечку памяти, — параметры **Process\Private Bytes** (Процесс\Байт исключительного пользования), **Process\Working Set** (Процесс\Рабочее множество памяти) и **Process\Handle Count** (Процесс\Счетчик дескрипторов). Кроме того, если вы считаете, что причиной утечки является процесс режима ядра, проведите мониторинг параметров **Memory\Pool Non-paged Bytes** (Память\Байт в невыгружаемом страничном пуле), **Memory\Non-paged Allocs** (Память\Распределений в невыгружаемом страничном пуле) и **Process <*имя_процесса*>\Pool Non-paged Bytes** (Процесс <*имя_процесса*>\Байт в невыгружаемом страничном пуле). Если утечка памяти вызывается выполнением отдельной программы, следует связаться с ее производителем — возможно, вы сможете получить заплату или обновление (кроме того, имеет смысл перейти к использованию другой, аналогичной программы).

Чрезмерное разбиение на страницы

Результатом чрезмерного разбиения на страницы может быть существенное потребление ресурсов жесткого диска; кроме того, нехватку памяти, приводящую к разделению на страницы, довольно просто перепутать с узким местом, локализующимся на диске, которое также приводит к разбиению на страницы. Таким образом, пытаясь установить причины разбиения на страницы (в случае, если нехватка памяти не

очевидна), обязательно проверьте показания таких счетчиков уровня использования диска, как **Physical Disk\% Disk Time** (Физический диск\% активности диска) и **Physical Disk\Avg. Disk Queue Length** (Физический диск\Средняя длина очереди диска) — разумеется, помимо счетчиков самой памяти.

К примеру, примите во внимание показания **Page Reads/sec** (Скорость чтения страниц с диска) вместе с **% Disk Time** и **Avg. Disk Queue Length**. Если низкая скорость операций считывания страниц сочетается с высокими значениями **% Disk Time** и **Avg. Disk Queue Length**, разумно предположить, что узкое место имеет отношение к диску. С другой стороны, если увеличение длины очереди не сопровождается уменьшением скорости считывания страниц, налицо нехватка памяти. Чтобы определить влияние избыточного страничного разбиения на активность диска, помножьте показатели счетчиков **Physical Disk\Avg. Disk sec/Transfer** (Физический диск\Среднее время обращения к диску) и **Memory\Pages/sec** (Память\Страниц/с). Если произведение показателей этих счетчиков превышает 0,1, значит, операции разбиения на страницы занимают более 10 процентов времени обращения к диску. Если такая ситуация наблюдается в течение продолжительного периода, значит, вам, вероятно, нужно больше памяти.

Теперь проверьте, не связано ли чрезмерное разделение на страницы с исполняемыми программами. Если возможно, остановите программу с наивысшим значением **Working Set** и посмотрите, насколько серьезно это повлияет на интенсивность разбиения на страницы. Если вы предполагаете факт чрезмерного разбиения на страницы, проверьте показания счетчика **Memory\Pages/sec**. Он отражает количество страниц, которые необходимо считывать с диска, из-за их отсутствия в физической памяти. Опять же, высокая интенсивность разбиения на страницы может свидетельствовать о потребности в увеличении ресурсов памяти.

Файлы подкачки

Если вы пришли к выводу о том, что на производительность сервера воздействует разбиение на страницы, у вас есть несколько вариантов управления файлом подкачки, которые могут помочь повысить производительность. К примеру, файл подкачки можно поместить на другие дисководы. Если в системе присутствует несколько жестких дисков, разделение файла подкачки между ними может привести к ускорению времени доступа. При наличии двух жестких дисков и при разделении файла подкачки оба этих жестких диска могут обращаться к его данным одновременно, тем самым значительно увеличивая производительность. Впрочем, если у вас есть два жестких диска, но один из них работает быстрее другого, более эффективным, вероятно, окажется вариант хранения файла подкачки только на быстрейшем из двух дисков. Чтобы определить оптимальную для данной системы конфигурацию, вам, вероятно, придется немного поэкспериментировать.

Кроме того, в ваших силах увеличить размер файла подкачки. При запуске операционная система Windows 2000 автоматически создает файл подкачки (pagefile.sys) на том диске, на котором она установлена. Этот файл нужен Windows 2000 для того, чтобы сформировать виртуальную память. Рекомендованный размер файла подкачки равен объему оперативной памяти, установленной в системе, помноженному на 1,5. Впрочем, размер файла также зависит от объема свободного дискового пространства на момент его создания. Выяснить, насколько велик системный файл подкачки, можно, взглянув на размер pagefile.sys в Проводнике Windows Explorer. Если пользо-

ватели обычно запускают несколько программ одновременно, то увеличение размера файла подкачки, вероятно, приведет к тому, что некоторые из этих программ будут запускаться быстрее.

Вы, несомненно, можете переопределить как исходный, так и максимальный размеры файла подкачки, однако в большинстве случаев более эффективным вариантом представляется расширение лишь исходного размера файла подкачки — лучше сделать так, чем позволить операционной системе выделять более значительное пространство для файла подкачки при запуске программ (что сопровождается фрагментированием диска). Если размер файла подкачки достигает максимума, на экран выводится предупреждение остановом системы. Чтобы выяснить, не приближается ли размер файла подкачки к своему максимальному уровню, прежде чем это действительно случится, определите фактический размер этого файла, и сравните его с настройкой максимального размера файла подкачки, которая устанавливается при помощи утилиты **System** (Система) в **Control Panel** (Панель управления) (рис. 27.13). Если эти два показателя близки, нужно либо увеличить исходный размер файла подкачки, либо уменьшить количество действующих программ.

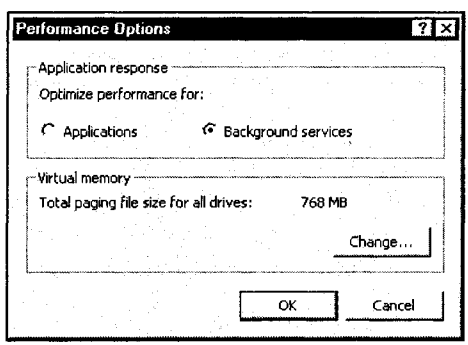


Рис. 27.13. В диалоговом окне **Performance Options** указывается максимальный размер файла подкачки

Счетчики файла подкачки представляют собой еще один способ проверки достаточности размера файла pagefile.sys. Откройте System Monitor и отследите статистику показателей счетчиков **Paging File\% Usage** (Файл подкачки\% использования) и **Paging File\% Usage Peak** (Файл подкачки\% использования (пик)). Если значение **% Usage Peak** приближается к настройке максимального размера файла подкачки (или если значение **% Usage** приблизительно равно 100 процентам), разумно увеличить исходный размер файла. Если несколько файлов подкачки распределены по нескольким дисководам, то имя пути к каждому из них представлено как экземпляр типа объекта Paging File. Вы можете либо добавить по счетчику для каждого из файлов подкачки, либо посредством экземпляра _Total оценить суммарные данные по уровню использования всех файлов подкачки вместе взятых.

Производительность диска

Осуществлять мониторинг активности диска также довольно важно. Статистика использования диска помогает выравнивать рабочую нагрузку между сетевыми серве-

рами. Утилита System Monitor содержит ряд счетчиков, связанных с физическими дисками и предназначенных для поиска неисправностей, планирования загрузки и измерения активности в каждом физическом томе. Как минимум, вы должны проводить мониторинг показаний следующих счетчиков (рис. 27.14):

- **Physical Disk\Disk Reads/sec** и **Disk Writes/sec** (Физический диск\Обращений чтения с диска/с и Обращений записи на диск/с);
- **Physical Disk\Current Disk Queue Length** (Физический диск\Текущая длина очереди диска);
- **Physical Disk\% Disk Time** (Физический диск\% активности диска);
- **LogicalDisk\% Free Space** (Логический диск\% свободного пространства);
- среди дополнительных счетчиков, подлежащих мониторингу, могут числиться **Physical Disk\Avg. Disk sec/Transfer** (Физический диск\Среднее время обращения к диску (с)), **Avg. Disk Bytes/Transfer** (Средний размер одного обмена с диском (байт)) и **Disk Bytes/sec** (Скорость обмена с диском (байт/с)).

Примечание

При тестировании производительности диска старайтесь регистрировать результирующие данные на другом диске (или компьютере) — с тем, чтобы они не вмешивались в работу испытуемого диска.

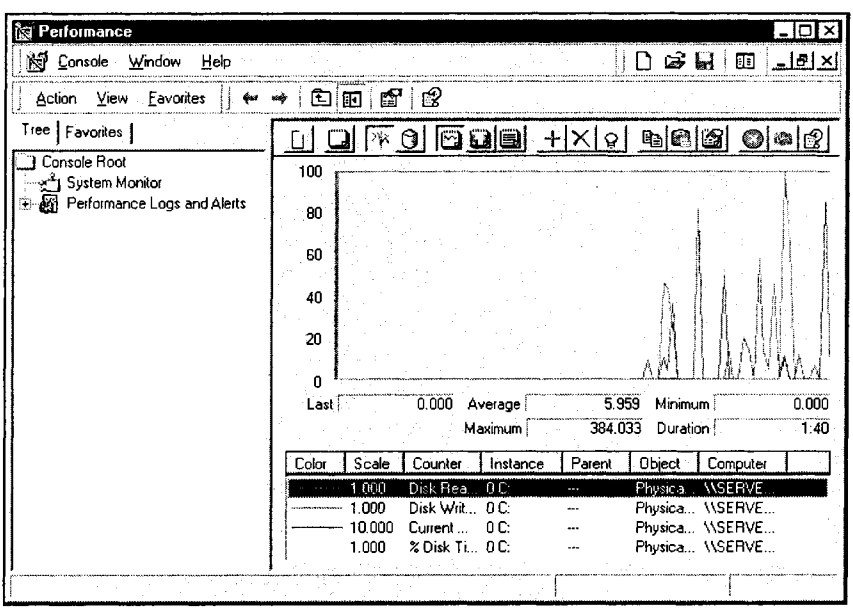


Рис. 27.14. При помощи оснастки System Monitor устанавливается базис производительности дисковой подсистемы, выравнивается нагрузка между разными дисками, аргументируются обновления

Счетчик **Avg. Disk sec/Transfer** определяет, сколько времени диску требуется для выполнения запросов. Высокое значение может свидетельствовать о том, что кон-

троллер диска постоянно выполняет повторные обращения к диску, и происходит это из-за сбоев. Такие выпадения увеличивают среднее время передачи с диска. Для большинства дисков значения времени передачи с диска, превышающие 0,3 секунды, считаются значениями выше среднего. Помимо прочего, вы можете проверить значение счетчика **Avg. Disk Bytes/Transfer**. Значение, превышающее 20 Кбайт, указывает на то, что производительность дисковода, в целом, приемлема — низкие значения появляются в тех случаях, когда приложение обращается к диску неэффективно. К примеру, приложения, которые нерегулярно обращаются к диску, способствуют увеличению показателя **Avg. Disk sec/Transfer**, т. к. для выполнения случайных передач требуется увеличение времени поиска. Счетчик **Disk Bytes/sec** отражает производительность подсистемы диска.

Примечание

По умолчанию, операционная система не собирает данные логического диска. В командной строке нужно ввести `diskperf -yv`. В результате драйвер статистики производительности диска, предназначенный для сбора данных о производительности диска, будет сообщать данные, относящиеся к логическим дискам или томам запоминающего устройства.

Выравнивание рабочей нагрузки

Сбалансированная между разными дисководами рабочая нагрузка помогает достичь максимальной эффективности работы сервера. Чтобы выровнять распределение нагрузок между дисководами на сетевых серверах, вы должны знать, насколько заняты эти дисководы в настоящий момент. С помощью счетчика **Physical Disk\% Disk Time** определяется процентный показатель времени, в течение которого дисковод находится в активном состоянии. Если показания счетчика **% Disk Time** высоки (превышают 90 процентов), проверьте данные счетчика **Physical Disk\Current Disk Queue Length** и выясните, сколько системных запросов ожидают возможности доступа к диску. Количество ожидающих запросов I/O (Input/Output — Ввод/Вывод) должно быть не больше, чем количество шпинделей, составляющих физический диск, помножено на 1,5 или 2. На большинстве дисков присутствует один шпиндель (хотя на RAID-устройствах их обычно больше). Аппаратное RAID-устройство должно быть представлено в System Monitor как один физический диск, а программные RAID-устройства — как ряд дисков (экземпляров).

Можно отслеживать показания счетчиков Physical Disk для каждого физического диска (не относящегося к RAID), а при помощи экземпляра _Total производится мониторинг показателей, относящихся ко всем дисководам компьютера. Для выявления узких мест, связанных с дисковой подсистемой, существуют счетчики **Current Disk Queue Length** и **% Disk Time**. Если значения **Current Disk Queue Length** и **% Disk Time** являются устойчиво высокими, имеет смысл обновить дисковод(ы) или перенести некоторые файлы на дополнительный диск или сервер.

Примечание

При наличии RAID-устройства счетчик **% Disk Time** может выводить значения, превышающие 100 процентов. В таком случае следует проверить показания **Avg. Disk Queue Length** — с его помощью вы сможете определить, сколько системных запросов (в среднем) ожидают своей очереди на обращение к диску.

Рекомендации по работе с дисками

Чтобы повысить общую производительность системы дисков, разумно реализовать следующие предложения.

- Замените существующий диск другим, более скоростным (или поставьте дополнительные диски); обновите контроллер дисков и шину.
- На серверах при помощи утилиты Disk Management (Управление дисками) организуйте расслоенные тома на нескольких физических дисках. Это решение повышает фактическую пропускную способность, т. к. команды ввода/вывода в этом случае могут подаваться одновременно.
- Проводите распределение программ между серверами. Для выравнивания рабочей нагрузки можно задействовать распределенную файловую систему (Distributed File System, DFS).
- Задачи, предполагающие интенсивное использование дискового ввода/вывода, следует назначить на отдельные физические диски или контроллеры дисков.
- Для оптимизации дискового пространства пользуйтесь утилитой Disk Defragmenter (Defrag).
- Чтобы повысить эффективность обращений к диску, старайтесь устанавливать самые последние версии программных драйверов хост-адаптеров.

Производительность процессора

Каждое приложение и каждая программа, работающая на сервере, требует некоторого времени на обработку процессором. Мониторинг показаний счетчиков объектов Processor и System позволяет получить ценную информацию об уровне использования процессоров и помогает определить, есть ли на вашем сервере узкое место, связанное с обработкой. Уровень использования процессора вычисляется при помощи счетчика **Processor\% Processor Time** (Процессор\% загруженности процессора). Этот счетчик выражает процентный показатель времени, затраченного процессором на выполнение активного потока (Thread — нить). Более подробные данные можно получить на основе показаний счетчиков **Processor\% User Time** (Процессор\% работы в пользовательском режиме) и **% Privileged Time** (Процессор\% работы в привилегированном режиме). Наконец, для выявления узких мест разумно проверить показания счетчика **System\Processor Queue Length** (Система\Длина очереди процессора) (рис. 27.15).

При определении уровня использования процессора следует учитывать роль компьютера и тип выполняемой задачи. В зависимости от того, какую операцию компьютер выполняет, высокие значения использования процессора могут означать, что система эффективно справляется со значительной рабочей нагрузкой, или что она изо всех сил старается удовлетворить все запросы. К примеру, если вы выполняете мониторинг компьютера, который используется для проведения вычислений, вычислительная программа вполне может потреблять 100 процентов времени процессора — даже если от этого страдает производительность других приложений, работающих на том же ПК. Решение этой проблемы, вероятно, заключается в перераспределении рабочей нагрузки. С другой стороны, показатели, приближающиеся к 100 процентам, на сервере, который обрабатывает клиентские запросы, могут свидетельствовать о том, что процессы встают в очередь (в ожидании обработки), а это

приводит к формированию узкого места. Столь устойчивый высокий уровень использования процессора неприемлем для сервера.

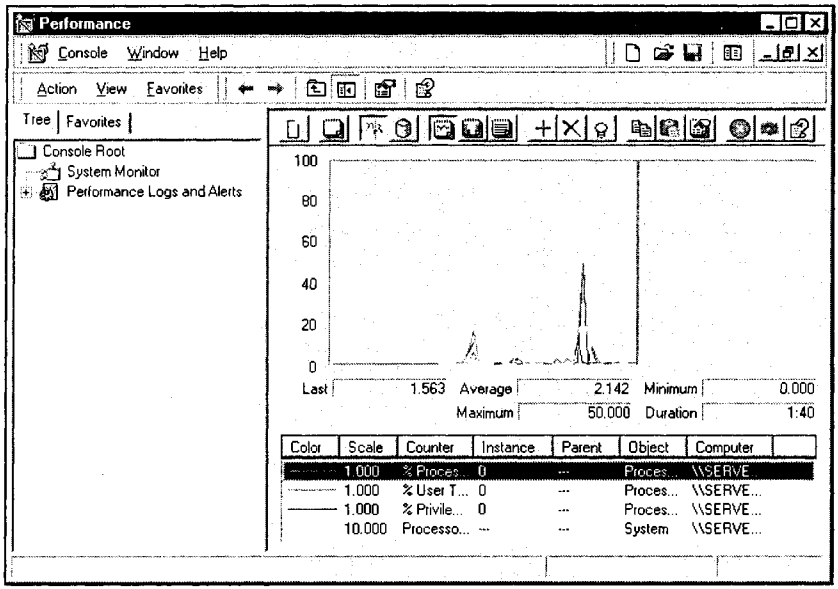


Рис. 27.15. При помощи System Monitor определяется базис производительности процессора, аргументируется установка дополнительных процессоров или увеличение их быстродействия

Узкие места процессора

Узкое место процессора формируется в случае, если потоки процесса требуют большего количества циклов процессора, чем возможно. При этом выстраиваются длинные очереди на обработку, снижается реактивность системы. Двумя наиболее распространенными причинами узких мест процессора являются программы и драйверы, ограниченные его возможностями, и компоненты подсистем (как правило, сетевые или дисковые компоненты), генерирующие избыточные прерывания.

Чтобы выявить узкое место процессора, сформированное в результате повышения потребности в выделении времени обработки, проверьте показатель счетчика **System\Processor Queue Length**. Очередь, в которой находятся два или более элементов, свидетельствует о появлении узкого места. Если за большую часть времени обработки соревнуется довольно значительное количество программных процессов, то повышения производительности можно достичь путем установки более быстродействующего процессора. Установка дополнительного процессора поможет исполнению многопоточных процессов, но при этом нужно иметь в виду, что прочие преимущества увеличения количества процессоров могут быть весьма ограниченными. Помимо прочего, счетчик **Server work Queues\Queue Length** (Рабочие очереди сервера\Длина очереди) отслеживает текущую длину рабочей очереди и, соответственно, помогает обнаруживать узкие места процессора. Устойчивая длина очереди, составляющая более 4 элементов, свидетельствует о возможности перегрузки процессора.

Чтобы проверить, не является ли активность прерываний причиной возникновения узкого места, проверьте показатели счетчика **Processor\Interrupts/sec** (Процессор\Прерываний/с) — он позволяет измерить интенсивность запросов на обслуживание, поступающих от устройств ввода/вывода. Если в показателях этого счетчика наблюдается значительный прирост, не сопровождаемый увеличением системной активности, налицо аппаратная неисправность. Кроме того, косвенным индикатором драйверов дисков, сетевых адаптеров и других устройств, которые генерируют прерывания, является счетчик **Processor\% Interrupt Time**. Наконец, для поиска аппаратных неисправностей, способных воздействовать на производительность процессора (например, конфликтов IRQ, Interrupt ReQuest — запрос на прерывание), нужно ознакомиться с показателями счетчика **System\File Control Bytes/second** (Система\Байт управления файлами/с).

Производительность многопроцессорной системы

Для проверки производительности многопроцессорного компьютера, опять же, применяется утилита System Monitor. Счетчик **Process\% Processor Time** сообщает о суммарном времени обработки каждым процессором всех потоков процесса. Счетчик **Processor (_Total)\% Processor Time** измеряет активность процессора в отношении всех процессов в компьютере. Таким образом, суммируется среднее активное время всех процессоров в рамках выборочного интервала, а затем полученное значение делится на количество процессоров. К примеру, если все процессоры заняты на протяжении половины выборочного интервала (в среднем), показатель счетчика равен 50%. То же самое значение получается, если одна половина процессоров занята на протяжении всего выборочного интервала, а вторая половина процессов в это время простаивает. Наконец, для отслеживания времени обработки отдельного потока применяется счетчик **Thread\% Processor Time**.

Чтобы направить отдельный процесс или программу на обработку одним процессором и, таким образом, повысить ее производительность (за счет других процессов), откройте Task Manager и выберите **Set Affinity** (Установить родственность). Эта опция присутствует только в многопроцессорных системах. Установка привязки к процессору может повысить производительность, уменьшив количество операций очистки кэшей процессоров по мере перехода потоков с одного процессора на другой — это оптимальный вариант для специализированных файловых серверов. Впрочем, привязка программы к определенному процессору может привести к тому, что потоки других программ не смогут переходить к менее загруженному процессору.

Производительность сети

Помимо прочего, утилита System Monitor применяется для определения базиса и мониторинга активности сервера в сети. Мониторинг сети обычно заключается в фиксации уровней использования ресурсов сервера и измерении общего сетевого трафика. Статистические данные по получаемым за одну секунду широковещательным кадрам (Network Segment\Broadcast frame received/sec — Сетевой сегмент\Получено широковещательных кадров/с) при условии продолжительного наблюдения могут помочь установить базис. Значительные отклонения от базиса подлежат дальнейшему анализу, который помогает определять причину проблемы. Так как любой компьютер обрабатывает каждое широковещательное сообщение, высокие уровни широковещания связаны с ухудшением производительности. Счетчик **Network**

Segment\% Network utilization (Сетевой сегмент\% использования сети) показывает, насколько уровень использования сети близок к полной нагрузке. При этом конкретный порог зависит от инфраструктуры и топологии сети. Если показатели этого счетчика превышают 30—40 процентов, конфликты могут приводить к неисправностям. Наконец, счетчик **Network Segment\Total frames received/sec** (Сетевой сегмент\ Получено кадров/с) позволяет узнать о переполнении мостов и маршрутизаторов.

Анализ сетевой производительности предполагает мониторинг активности на различных сетевых уровнях. Канальному уровню (на котором находится сетевая плата) соответствует объект Network Interface (Сетевой интерфейс) с показателями **Bytes total/sec** (Байт/с), **Bytes sent/sec** (Отправлено байт/с) и **Bytes received/sec** (Получено байт/с). На сетевом уровне работают счетчики объекта IP — например, **Datagrams Forwarded/sec** (Препровождено датаграмм/с), **Datagrams Received/sec** (Получено датаграмм/с) и **Datagrams Send/sec** (Отправлено датаграмм/с). Транспортному уровню соответствуют счетчики объекта TCP: **Segments Received/sec** (Получено сегментов), **Segments Retransmitted/sec** (Переотправлено сегментов/с), **Segments/sec** (Сегментов/с) и **Segments Sent/sec** (Отправлено сегментов/с). При высоком коэффициенте повторных передач возможна аппаратная неисправность. При использовании протокола NetBEUI применяются счетчики NetBEUI наподобие **Frame Bytes Received/sec** (Получено кадров байт/с), **Frames Received/sec** (Получено кадров/с), **Frames Rejected/sec** (Отвергнуто кадров/с) и **NetBEUI Resource\Times Exhausted** (Ресурсы NetBEUI\Ресурсы были исчерпаны).

Учитывайте ресурсы

Отклонение от нормы показателей сетевых счетчиков часто свидетельствует о наличии проблем, связанных с серверной памятью, процессором или дисками. По этой причине лучшим подходом к мониторингу сервера представляется наблюдение сетевых счетчиков совместно со счетчиками **Processor\% Processor Time**, **PhysicalDisk\ % Disk Time** и **Memory\Pages/sec**. К примеру, если значительное увеличение показателя **Pages/sec** сопровождается снижением показателя обработки данных сервером **Bytes Total/sec**, разумно предположить, что для выполнения сетевых операций компьютеру не хватает физической памяти. Если в системе наблюдается избыточное разделение на страницы, значит, большая часть ее физической памяти, вероятно, выделена на выполнение сетевых операций, в результате чего в распоряжении процессов, которые в данный момент пользуются страничной памятью, остался незначительный объем физической памяти. Чтобы проверить это предположение, откройте системный журнал регистрации событий, и поищите записи, указывающие на отсутствие свободных ресурсов страничной или неперемещаемой памяти.

Что касается уровня представления и прикладного уровня, то для мониторинга сервера предназначены счетчики объекта Server, а для мониторинга клиентского компьютера — счетчики объекта Redirector. Счетчики объекта Redirector осуществляют сбор данных о запросах, передаваемых службой Workstation, а счетчики объекта Server собирают информацию о запросах, полученных и интерпретированных службой Server. При мониторинге необходимо пользоваться, по меньшей мере, одним счетчиком объекта Redirector (в отношении клиентских машин) или Server (в отношении серверов) — **Bytes Total/sec**. Каждый из этих объектов предусматривает еще несколько счетчиков, показаниями которых имеет смысл воспользоваться в случае подозрения на неисправность службы Workstation или Server:

- Redirector\Current Commands (Перенаправитель\Активных команд);
- Redirector\Network Errors/sec (Перенаправитель\Сетевых ошибок/с);
- Redirector\Reads Denied/sec (Перенаправитель\Отказов на операцию чтения);
- Redirector\Writes Denied/sec (Перенаправитель\Отказов на операцию записи);
- Redirector\Server Sessions Hung (Перенаправитель\Отключений от сервера);
- Server\Sessions Errored Out (Сервер\Сеансов, закрытых из-за возникновения ошибки);
- Server\Work Item Shortages (Сервер\Нехваток рабочих элементов);
- Server\Pool Paged Peak (Сервер\Выгружаемый пул (пик));
- Server\Nonpaged Pool Failures (Сервер\Отказов невыгружаемого страничного пула).

Рекомендации по работе с сетью

Чтобы повысить общую производительность сети, вы можете реализовать следующие предложения.

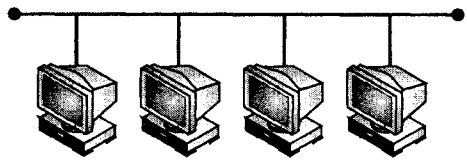
- Настройте сеть таким образом, чтобы системы, коллективно используемые одной группой людей, находились в одной подсети.
- Откажитесь от связывания нерегулярно применяемых сетевых адаптеров.
- В случае применения нескольких протоколов установите порядок, в соответствии с которым рабочая станция и программное обеспечение NetBIOS будут привязываться к каждому из них. Если протокол, употребляемый чаще других, находится в начале списка связывания, среднее время соединения уменьшается. Кроме того, в условиях определенных сетевых топологий некоторые протоколы работают быстрее, чем другие. При оптимизации клиентского ПК повышения его производительности можно добиться, поместив самый быстрый протокол на первую позицию в списке связывания.
- Установите на сервере высокопроизводительную сетевую плату. Если на сервере применяется 16-битовый адаптер, вы сможете добиться резкого повышения производительности, заменив его мощным 32-битовым адаптером.
- Устанавливайте несколько сетевых адаптеров. К примеру, Windows 2000 обеспечивает поддержку нескольких адаптеров для отдельного протокола и нескольких протоколов для отдельного адаптера. Несмотря на то, что такая конфигурация может привести к формированию автономных сетей, не способных к взаимодействию, это хороший метод повышения эффективности коллективного использования файлов.

Дополнительные ресурсы

Network Instruments: **www.networkinstruments.com**.

Agilent: **www.agilent.com**.

Hewlett-Packard: **www.hp.com**.



ГЛАВА 28

Управление сетью

Любой профессионал подтвердит, что администрирование сети — это сложное и трудоемкое занятие. Слежение за множеством пользователей, серверов и системных ресурсов, пусть и в небольшой сети — все это с трудом выдерживает даже самый острый ум. Каждый год организации инвестируют громадное количество технических средств сбора информации об операциях, выполняемых в сети и присутствующих в ней устройствах. К примеру, вообразите себе время, необходимое для проведения инвентаризации 150 рабочих станций с целью проверки версии BIOS видеосистемы, наличия свободного пространства на жестких дисках, работоспособности вентиляторов, и уровней напряжения центральных процессоров, или других свойств.

Идея *сетевого управления* развивалась, чтобы помочь администраторам и техническим специалистам установить некий уровень контроля над сетевыми устройствами. Во многих случаях инструментальные средства сетевого управления позволяют администратору провести инвентаризацию аппаратного и программного обеспечения всех станций, даже не взглянув на них. Кроме того, средства управления зачастую позволяют выполнять базовые задачи сопровождения компьютеров (например, дефрагментацию жесткого диска или обновление драйвера) удаленным способом, с центральной "консоли управления" — и даже автоматически направлять отчеты о некоторых возникающих проблемах (например, о нехватке дискового пространства или о сбоях охлаждающих вентиляторов) непосредственно администратору.

Сегодня основные производители ПК поставляют мощные инструментальные средства управления, такие как HP OpenView, Compaq Insight Manager 7, Dell OpenManage или менеджер событий Gateway ManageX. Эти инструменты могут устанавливаться как на серверах, так и на рабочих станциях; они отсылают на консоль управления детальные отчеты о состоянии каждого управляемого устройства. В этой главе рассматриваются основные технологии, связанные с сетевым управлением, и описываются возможности современных инструментальных средств управления.

Принципы управления

Администрирование и сопровождение сети зачастую предъявляет серьезнейшие требования к информационно-технологическим ресурсам. Чтобы осознать важность

управления сетью, вы должны уяснить некоторые базовые задачи, которые в тот или иной момент должен выполнять администратор.

- Необходимо устанавливать и настраивать новые рабочие станции и серверы.
- Необходимо модернизировать существующие рабочие станции и серверы.
- Необходимо обновлять операционные системы и драйверы.
- Необходимо устанавливать, исправлять и обновлять приложения (например, средства антивирусной защиты).
- Необходимо устанавливать и настраивать такие устройства, как концентраторы, коммутаторы и маршрутизаторы.
- Необходимо монтировать новые межсоединения (и заменять неисправные).
- Необходимо создавать и проверять резервные копии данных.
- Необходимо следить за имуществом (например, вести журнал конфигурации и ремонта каждого компьютера или сервера).
- Необходимо обновлять документацию, вводя в нее данные о новейших изменениях и обновлениях.
- Необходимо организовывать генерирование аварийных сигналов и предупреждений, регистрировать их, решать, что с ними делать.
- Необходимо периодически проводить количественный анализ сетевой производительности, отслеживать ее развитие.

Естественно, это лишь краткий перечень. Традиционно, каждая из этих задач должна была выполняться администратором или техническим специалистом, причем довольно часто — в каждой отдельной системе. К примеру, для установки антивирусного клиентского программного обеспечения обычно приходилось проводить долгие ночи за выполнением ручной инсталляции на каждом из клиентских компьютеров. Так как сети становились крупнее и сложнее, требования ко времени и способностям, необходимым для выполнения таких задач, быстро стали очень значительными. До начала 1990-х годов, когда отделы информационных технологий (ИТ) распоряжались крупными бюджетами, а сотрудников в них было достаточно, проблем не возникало. Но современные тенденции к сокращению персонала компаний и урезанию бюджетов часто вынуждают отделы ИТ прилагать огромные усилия, чтобы удовлетворить потребности сетевых пользователей.

Необходимость в управлении

Управление сетью предусматривает упрощенный мониторинг, поиск неисправностей и сопровождение. Для примера возьмем среднего размера офисную сеть с 50 пользователями, несколькими серверами и разнородными концентраторами и коммутаторами. Предположим, что администратор собирается провести обновление операционных систем. Будучи хорошим администратором, он в первую очередь сверит имеющееся аппаратное обеспечение компьютеров со списком совместимого оборудования и убедится в том, что существующие системы справятся с предполагаемым обновлением (или выяснит, какие из существующих систем нуждаются в модернизации). Впрочем, обычно для этого требуется проверить каждый компьютер в отдельности и от руки составить опись аппаратных средств всех осмотренных ПК. При наличии инструментальных средств сетевого управления администратор может

провести автоматическую инвентаризацию "управляемых компьютеров" и вывести подробный отчет об аппаратной и программной конфигурациях каждой системы — лишь одна эта возможность может сэкономить многие дни усилий.

Рассмотрим другой пример. Предположим, что ваша компания вводит антипиратскую политику, которая запрещает "коллективное использование" программных средств на рабочем месте. На практике, администратор может провести такую политику в жизнь единственным способом: пройти все компьютеры, вручную проверить каждый из них и сравнить установленное ПО с исходными установочными компакт-дисками (или со множеством установочных лицензий). Инструментальные средства управления способны провести инвентаризацию установленных программ и вывести отчеты, которыми администратор может незамедлительно воспользоваться.

Помимо этого, средства управления могут проверять "здоровье" компьютеров, отслеживая основные параметры аппаратуры наподобие питающих напряжений, температур, оборотов охлаждающих вентиляторов, свободного дискового пространства и т. д. Серьезный сбой (например, остановка кулера) приводит к немедленному формированию сообщения электронной почты или страницы вызова технического специалиста. Незначительная неисправность (например, замедление вентилятора или повышение температуры системных блоков) инициирует обычный порядок осмотра оборудования, таким образом, обеспечивая некоторый уровень профилактики — проблемы можно устранить до того, как они станут серьезными.

Но управление распространяется не только на персональные компьютеры. Инструментальные средства управления могут применяться для установки и настройки устройств (таких как маршрутизаторы), соответствующих конкретной схеме управления. Это позволяет администратору действовать при помощи стандартной консоли управления, а не пользоваться специализированным программным обеспечением, поставляемым вместе с каждым устройством. В дополнение к установке и конфигурации, средства управления могут принимать от устройства сообщения о состоянии и об ошибках — при возникновении ошибок администратор получает сообщение по электронной почте (они даже могут приходить на пейджер).

Функциональные группы задач управления

Управление сетью часто определяется как процесс регулирования сложной сети с целью максимизации эффективности и производительности как самой сети, так и действий ответственного за нее ИТ-персонала. Естественно, это очень широкое определение, а, кроме того, оно ограничено применяемыми в вашей организации средствами управления и степенью их ввода в эксплуатацию. К примеру, установка средств мониторинга аппаратного обеспечения только на нескольких компьютерах будет случаем ужасного недоиспользования инструментов управления. Равно как эффект от установки измерительных средств на все ПК сети будет ограничен, если не составлять регулярные инвентарные отчеты и не генерировать аварийные сигналы. Управление сетью обычно разделяется на пять функциональных групп.

Сетевые проблемы

Эта область подразумевает разрешение проблем и вопросов поиска и устранения неисправностей сетевых станций (включая рабочие станции и серверы), ресурсов (в том числе NAS-серверов и принтеров), коммутирующих блоков (наподобие кон-

центраторов и коммутаторов) и межсоединений. Из содержания *гл. 29* станет ясно, что умение справиться с аварийной ситуацией подразумевает выполнение нескольких важнейших шагов:

- формулировка задачи;
- идентификация и локализация источника неисправности;
- устранение неисправности или замена дефектных элементов;
- повторное тестирование сети.

Ключом к умению успешно справиться с проблемой является ее обнаружение — осознание самого факта существования проблемы (или возможности ее возникновения). В обычной ситуации регулирование проблемы (или поиск неисправностей, Troubleshooting) начинается в тот момент, когда пользователь сообщает о своих трудностях, и должно выполняться вручную с помощью таких инструментов, как кабельный тестер, мультиметр, анализатор протоколов и т. д. Инструментальные средства управления сетью позволяют администратору и техническому специалисту решить более широкий диапазон проблем с большей эффективностью. Эти средства (Platform management) могут опрашивать элементы сети "по требованию" или на регулярной основе, осуществляя мониторинг правильности их функционирования. Когда сетевое устройство перестает нормально работать, средства управления обнаруживают это событие (которое зачастую приводит к сбою или ухудшению производительности сети), устанавливают приоритет *предупреждения* (Alert), вносят необходимые исправления (если это возможно), и сообщают техническому специалисту о необходимости заняться решением проблемы или обратить на нее особое внимание. К примеру, средства аварийного управления способны оповестить о таких характерных для каждой отдельной системы проблемах, как напряжение или температура — автоматически сгенерировать *аварийный сигнал* (Alarm) и вызывать технического специалиста прежде, чем система выйдет из строя. При этом многие распространенные неисправности (например, недостаток свободного дискового пространства или избыточная фрагментация) могут быть устранены автоматически, без вмешательства человека.

Примечание

Между аварийным сигналом и предупреждением есть разница. Аварийный сигнал свидетельствует о серьезной неисправности, требующей немедленного действия. Предупреждение сообщает о проблеме, на которую нужно обратить внимание, как только у технического специалиста появится такая возможность.

Установка и настройка сети

Как вы могли заметить, читая предшествующие главы, установка и конфигурация одного устройства может оказать решающее воздействие на функционирование всех остальных устройств и сети в целом. Для технических специалистов и администраторов проблемой является сохранение следов о такой конфигурационной информации, и необходимы время и силы, чтобы проверить или обновить настройки каждого устройства. Инструментальные средства управления сетью зачастую позволяют собирать и резюмировать настройки управляемых устройств, причем особое внимание уделяется их аппаратной и программной настройке. Когда в сеть нужно внести какие-либо изменения, при помощи управляющего программного обеспечения тех-

нический специалист может запросто обратиться к нужным управляемым устройствам и перенастроить их (хотя, возможно, что для завершения процесса понадобится выполнить некоторые действия по физической реконфигурации кабелей и соединений). Кроме того, планируя проведение сетевых обновлений и действия по сопровождению сети, вы можете проанализировать и сравнить настройки и конфигурацию нескольких устройств.

Возможно, все это кажется простым, но на самом деле представляет собой крайне сложную задачу. Управление настройкой и конфигурацией, по существу, предполагает ведение подробных записей о версиях программного обеспечения и аппаратных сборках для большинства (если не на всех) устройств сети. К примеру, предположим, что всем пользователям сети нужно установить Service Pack 2 для Windows 2000 (или более новый сервисный пакет), выпущенный компанией Microsoft. В отсутствие платформы сетевого управления вам пришлось бы проводить ручную инвентаризацию каждого компьютера, выясняя, какие версии Windows на них установлены. В то же время, функции управления конфигурацией, поддерживаемые средствами сетевого управления, позволяют по требованию выполнять автоматическую инвентаризацию подключенных ПК. В качестве другого примера предположим, что вы обнаружили новую версию прошивки (встроенных программно-аппаратных средств) для ответственного коммутатора. Вместо того чтобы отключать этот коммутатор от сети и искать текущую версию прошивки, обозначенную на корпусе устройства, воспользуйтесь программой управления конфигурацией — она позволяет запросить коммутатор на предмет текущей версии его прошивки, а также данных о его производителе и модели, необходимых для выбора нужного файла обновления встроенных программно-аппаратных средств.

Безопасность сети

Управляющая программа помогает защитить ваши сетевые ресурсы. Обычно под этим подразумевается слежение за пользователями сети и их деятельностью. К примеру, функции защиты сети способны определить, какие пользователи обращались к секретным файлам (например, к платежным ведомостям), и были ли это санкционированные действия. Естественно, большинство современных операционных систем поддерживают подробную регистрацию событий безопасности, предполагающую сбор аналогичных данных. Тем не менее, благодаря интегрированным средствам составления отчетов о безопасности администратору не приходится ходить от сервера к серверу, проверяя журналы безопасности в поисках неисправности. О случаях неудачной регистрации и другой несанкционированной деятельности администратор может узнавать со своей консоли управления, и уже после этого проводить необходимые расследования.

Функционирование сети

Администратор должен измерять количество операций и производительность сети, а инструментальные средства, необходимые для измерения производительности, присутствуют во многих платформах управления. Администраторы получают возможность выполнять текущий контроль широкого спектра рабочих характеристик, помогающий определить жизнеспособный сетевой базис и выявить любые отклонения от этого базиса, определив их как потенциальные сетевые неисправности или узкие места, формирующиеся по мере роста сетевого трафика. Кроме того, отслеживание

таких измерений во времени позволит сделать модель развития предсказуемой и реализуемой еще до того, как проявится дефицит чего-либо (например, недостаток пространства хранения) или образуются серьезные узкие места, ограничивающие производительность. Более подробная информация о производительности сети и построении базиса приводится в *гл. 27.*

Анализ затрат на сеть

Работа в сети стоит денег, и любая отдельная сеть может предоставить человеку или группе ограниченное количество ресурсов. Зачастую администратору приходится выполнять расчеты, связанные с тем, как именно используется сеть. Вручную такие вычисления производить трудно (а иногда и невозможно), но инструментальные средства управления часто содержат средства анализа затрат, которые позволяют администратору выполнять мониторинг сети так, как будто это — расходуемый ресурс, и помещать пользователей сети в финансовое измерение. Когда администратор получает возможность проводить количественный анализ пользователей и их деятельности, он может увязывать затраты с этими пользователями. В некоторых случаях функции анализа затрат, присутствующие в программах управления сетью, даже позволяют организации взимать плату за доступ к сети.

Вне зависимости от финансовых вопросов, менеджеры учета сетевых средств должны знать тех пользователей, которые обращаются к определенным сетевым ресурсам (включая серверы, приложения, принтеры, маршрутизаторы, или другие элементы сети). Путем выявления четких моделей использования сети (а, возможно, и сравнения уровня использования с проблемами производительности) администратор часто получает возможность проведения эффективных обновлений или внесения исправлений, направленных на улучшение работы сети. К примеру, предположим, что определенная группа сотрудников вашей организации интенсивно работает с одним из серверов, ограничивая возможности этого сервера для других групп. Исходя из полученных данных об уровне использования, вы могли бы принять обоснованные решения о модернизации и выделить этой группе отдельный сервер. В результате вы добились бы разгрузки существующего сервера для всех остальных пользователей.

Введение в SNMP

Для реализации управления сетью необходим стандартный протокол, способный поддерживать широкий круг разнородных сетевых устройств (независимо от их архитектуры). Простой протокол сетевого управления (Simple Network Management Protocol, SNMP) был предложен в 1988 году в виде пакета Запросов на комментарии (Requests for Comments, RFC). Документы RFC определяли основные принципы и методы реализации протокола, который должен стать стандартом мониторинга и управления в Интернете. Впоследствии этот протокол мог стать единственной "универсальной" заменой огромному количеству специализированных в зависимости от конкретного производителя решений, предлагавшихся в то время. С этого момента SNMP завоевал большую популярность в среде сетевых администраторов. Несмотря на то, что существуют и другие протоколы управления, именно SNMP получил широкое распространение и стал стандартом сетевого управления. В архитектурах большинства операционных систем (включая системы UNIX/Linux, NetWare,

Windows 98/ME и Windows NT/2000/XP) предусматриваются агенты SNMP, а большинство ведущих производителей компьютерного аппаратного обеспечения в настоящее время предлагают вниманию клиентов линейки сетевых продуктов, обеспечивающих поддержку SNMP (включая сетевые платы, концентраторы, мосты, маршрутизаторы, коммутаторы, модули CSU/DSU и принтеры).

В последующих документах RFC, касающихся SNMP, были устранены многие проблемы; кроме того, SNMP был дополнен базой данных, специфицированной в новом стандарте и названной базой управляющей информации (Management Information Base, MIB). По стандарту, MIB (описанная в документах RFC1066 и RFC1213) определяет границы десяти групп сетевых объектов — это группы систем, интерфейсов, трансляции адресов, IP, ICMP (Internet Control Message Protocol — протокол управляющих сообщений в сети Интернет), TCP, UDP, EGP (Exterior Gateway Protocol — протокол внешней маршрутизации), передачи и SNP. Впрочем, производители постоянно внедряют в свои продукты новые возможности и функции, некоторые из которых не охватываются стандартными объектами и группами MIB. С целью управления дополнительными функциями при помощи SNMP производители аппаратного и программного обеспечения разработали собственные, специальные версии MIB.

Примечание

Внедрение агента SNMP в сетевое аппаратное обеспечение часто увеличивает цену продукта, так что производители обычно предусматривают версии с поддержкой SNMP и без нее.

На заре 1990-х исходные спецификации SNMP были пересмотрены и обновлены. Появились новые группы MIB, а некоторые из существующих объектов MIB устарели. В основном, новая спецификация MIB, названная MIB II (или MIB-2), совместима с исходной MIB, которую теперь обозначают как MIB I (или MIB-1).

К концу 1991 года стандартная спецификация SNMP MIB подверглась расширению в виде появившейся базы MIB удаленного сетевого мониторинга (Remote Network Monitoring MIB, RMON). RMON поддерживает ряд объектов SNMP, относящихся к сетевому анализу и мониторингу. Информация, которую предоставляет RMON, по своему масштабу несколько отличается от типичных данных SNMP, поставляемых сетевыми устройствами. Обычно устройство SNMP собирает информацию о самом себе (касательно работы этого устройства или его отношения к сети). Для сравнения, агент RMON пытается собирать информацию о сетевом трафике, исходящем и входящем в другие устройства сети (за исключением устройства-агента). Среди этой информации фиксируется сетевая статистика, предыстория, данные о хостах сети, соединениях и событиях. Агент RMON может устанавливать фильтры и захватывать трафик, входящий и исходящий из определенных устройств сети.

Проблемы, связанные с безопасностью SNMP, в конечном счете подтолкнули к разработке защищенной версии SNMP под названием S-SNMP, причем первые документы RFC, связанные с S-SNMP, появились в середине 1992 года. S-SNMP предусматривает усиление защиты по сравнению с исходным протоколом SNMP, но не содержит никаких дополнительных функций иного рода. Впрочем, S-SNMP несовместим с исходным SNMP. Примерно в то же время серьезные усилия разработчиков были направлены на улучшение самого SNMP, включение в его состав функций

обеспечения безопасности, присутствовавших в S-SNMP, а также внедрение новых функций MIB. Результатом этой работы стал протокол SNMP версии 2 (SNMPv2). SNMPv2 был плохо воспринят многими производителями программного и аппаратного обеспечения, некоторые из которых приложили значительные усилия к проектированию агентов SNMP MIB I и MIB II (а вопросы защиты зачастую не представляли для пользователей важности). Даже сегодня многие агенты, предлагаемые производителями, совместимы с SNMP MIB II (но не с SNMPv2).

Примечание

Имейте в виду, что SNMP MIB II и SNMPv2 — это разные вещи.

К началу 1999 года группа IETF утвердила проект стандарта SNMPv3. Спецификации SNMPv3 базируются на операциях протокола и транспортных соответствиях проекта стандарта SNMPv2 (RFC1905—1907), а также на возможностях защиты и удаленной конфигурации, свойственных SNMP. Тем не менее SNMP MIB II часто встречается и до сих пор. К примеру, Compaq Insight Manager 7 обеспечивает поддержку только оригинальных v1-совместимых агентов и MIB. Следовательно, если вы как сторонняя организация собираетесь составлять собственные базы MIB в Compaq Insight Manager 7, не забудьте достать v1-совмстимую версию SNMP.

Примечание

Подробное описание функций разных версий SNMP дается в документе RFC2570, опубликованном по адресу: **ftp://ftp.isi.edu/in-notes/rfc2570.txt**.

Станции и агенты SNMP

В схеме SNMP есть два основных элемента: *менеджер* (Manager) (или управляющая станция, Management station) и агенты (Agents) (их часто называют управляемыми агентами, Managed Agents). С помощью управляющей станции сетевой администратор может просматривать, анализировать и даже управлять локальными сетевыми устройствами. На практике, в качестве управляющей станции может выступать специализированный компьютер, рабочая станция, или программное обеспечение, работающее на универсальной рабочей станции (например, SNMP Extension на компьютере с системой Windows 98/ME/NT/2000/XP). Агентом SNMP, по существу, является программа, работающая на управляемом устройстве (например, на мосте, маршрутизаторе, концентраторе или рабочей станции) и собирающая данные о том, как это устройство функционирует. К примеру, если объектом является маршрутизатор TCP/IP, то его агент может собирать данные о сетевом трафике, проходящем через этот маршрутизатор, и о его поведении в разных режимах нагрузках.

Каждый агент SNMP делает записи в базе управляющей информации (MIB). Впоследствии MIB используется агентом для отслеживания и систематического обновления данных. Информация, содержащаяся в MIB, организуется в виде древовидной структуры, в которой каждый блок данных можно считать листком различных ветвей этого дерева. Отдельные блоки данных называются объектами данных. Когда управляющая станция испытывает необходимость в получении данных от агента SNMP, она отправляет ему запрос SNMP (спецификация SNMP позволяет станции в одном запросе выставлять требования на несколько объектов MIB).

Когда агент SNMP получает запрос, пришедший от управляющей станции SNMP, он ищет свою локальную MIB, находит текущие значения запрошенных данных, формирует ответный пакет и отправляет его обратно управляющей станции. Та принимает ответный пакет, декодирует его, а затем предоставляет полученные данные в виде списка или в графическом формате — таким образом, чтобы сетевой менеджер мог просмотреть, проанализировать и внести в эту информацию изменения. Приложения, предназначенные для управления агентами SNMP, сильно отличаются друг от друга по сложности и полезности. Некоторые из них просты — они лишь отправляют на некоторые устройства запросы и генерируют для администратора базовые отчеты. Более сложные приложения способны отображать топологию сети, проводить мониторинг сетевого трафика и перехватывать отдельные события (сопровождая их появление аварийными сигналами). Самое развитое программное обеспечение консоли управления даже может генерировать отчеты об анализе тенденций для планирования загрузки — эти данные помогают администраторам планировать обновления и перестройки сети.

Сообщения SNMP

Как вы могли заметить, принцип работы SNMP заключается в обмене запросами SNMP между управляющей станцией, с одной стороны, и агентами SNMP, рассредоточенными по всей сети, с другой стороны. Обычно запросы передаются частями в виде данных пакетов IP (UDP), хотя есть реализации SNMP для TCP, IPX/SPX и других протоколов. Что касается UDP, то управляющая станция SNMP по сети отправляет агенту запросы на номер порта UDP 161. Запросное сообщение SNMP состоит из двух частей:

- заголовок SNMP, в состав которого входят номер версии SNMP, данные о размере запроса и пароль (называемый групповым именем);
- блок из одного или нескольких запрошенных объектов, которые совместно отсылаются в ответном пакете.

Программа управления и агенты устройств обмениваются информацией при помощи ограниченного набора операций, которые называются *примитивами*. Эти примитивы предназначены для того, чтобы создавать запросы и отправлять данные между менеджером и агентами. Программой управления инициируются следующие примитивы.

- `GetRequest`. Управляющая станция пользуется примитивом `GetRequest` для извлечения из агента значений одного или нескольких объектов. Эти значения обычно бывают сингулярными, а не колоночными (как в таблице). Когда агент получает команду `GetRequest`, он проводит анализ пакета, в котором она содержится, на предмет ошибок, находит значения MIB, соответствующие данным в запросном пакете, а затем отправляет управляющей станции пакет `GetResponse`.
- `GetResponse`. Когда необходимые данные обнаруживаются в агентской базе MIB, агент отправляет управляющей станции пакет `GetResponse`. Если в запросном пакете содержится ошибка, то и в пакете `GetResponse` вместо запрошенных данных помещается сообщение об ошибке. Управляющая станция узнает обо всех ошибках.
- `GetNextRequest`. Управляющая станция отсылает пакет `GetNextRequest` для извлечения из агента одного или нескольких объектов и их значений. Обычно это

несколько объектов, расположенных в рамках таблицы. Чтобы извлечь все строки таблицы, управляющая станция начинает с начала таблицы, и продолжает отсылать пакеты `GetNextRequest` вплоть до считывания всех записей таблицы. В отсутствие ошибок агент возвращает пакеты `GetResponse` в ответ на каждый из пакетов `GetNextRequest`.

- `SetRequest`. Пакет `SetRequest` применяется управляющей станцией для изменения значения объекта на агенте SNMP. В отсутствие ошибок агент устанавливает новое значение указанного объекта, и для подтверждения успешности этой операции возвращает пакет `GetResponse`.
- Ловушки (Traps). Агент отправляет управляющей станции ловушки SNMP как оповещение о предопределенном событии. Формат пакета ловушки отличается от формата остальных четырех сообщений SNMP. При использовании UDP ловушки отсылаются на порт 160 управляющей станции. Так как сообщения ловушек могут отсылаться множеством различных агентов, в заголовке ловушечного пакета указывается корпоративный идентификатор объекта (Object Identifier, OID), а также адрес агента, после чего следуют общие и конкретные типы ловушек, временная метка и поле связывания переменных. Существует семь типов общих ловушек.
  - *ColdStart*. Агентское устройство SNMP производит повторную инициализацию методом, который позволяет реконфигурировать это устройство или агента.
  - *WarmStart*. Агентское устройство SNMP производит повторную инициализацию методом, который не позволяет реконфигурировать это устройство или агента.
  - *LinkDown*. Агент SNMP обнаружил сбой в канале связи.
  - *LinkUp*. Сбой канала связи устранен.
  - *AuthenticationFailure*. Управляющая станция SNMP не была должным образом аутентифицирована на агентском устройстве.
  - *EGPNeighborLoss*. Одноранговый узел EGP агента SNMP не функционирует.
  - *EnterpriseSpecific trap*. Агент SNMP оповещает управляющую станцию о событии, определенном производителем устройства. Более подробная информация зависит от конкретного типа ловушки.

Сетевые объекты и базы MIB

Примитивы, обеспечивающие взаимодействие между управляемыми объектами SNMP, были бы бессмысленны, не будь других данных, предназначенных для определения конкретного объекта и его состояния (или другого содержимого). Инструментальные средства управления хранят информацию об объектах в базе данных MIB (или MIB-II), имеющейся на каждом агентском устройстве сети. В некоторых случаях устройство может вести несколько баз MIB. MIB не просто фиксирует подробные данные о конкретном агенте — вся существенная информация, сбором которой занимается агент, также хранится в его MIB. К примеру, в MIB управляемого коммутатора может быть включена информация, конкретизирующая производителя этого устройства, его модель, уровень программно-аппаратных средств; кроме того, в той же базе могут отслеживаться статистические данные о входящем трафике, по-

врежденном трафике, адресах назначения и т. д. Когда управляющая станция делает запрос посредством операторов Get, управляемое устройство (агент) может либо возвратить запрошенные детали, либо перечислить соответствующие ошибки. Впоследствии полученная информация хранится и отображается на управляющей станции (зачастую — в мощной системе управления базами данных). С другой стороны, при необходимости с помощью операторов Set управляющая станция может произвести конфигурационные изменения на управляемом устройстве.

В древовидной структуре объектов SNMP содержатся данные различных типов, включая числа, текст, адреса, описания назначения битовых полей и идентификаторы объектов. Для описания объектов MIB применяются две спецификации: абстрактная синтаксическая нотация версии 1 (Abstract Syntax Notation One, ASN.1) и базовые правила кодировки (Basic Encoding Rules, BER).

Абстрактная синтаксическая нотация

Абстрактная синтаксическая нотация версии 1 (ASN.1) описывает объекты при помощи текстовых описаний MIB. Она предоставляет правила для написания непротиворечивых и компилируемых баз MIB (как стандартных, так и специализированных). В ASN.1 есть базовые типы (например, целое число, восьмибитовые строки, идентификатор объекта, Null, сетевой адрес и т. д.). В листинге 28.1 показан пример объекта ASN.1 sysDescr из системной группы MIB II System Group.

Листинг 28.1. Пример описания ASN.1 объекта sysDescr MIB II

```
--the System group
sysDescr OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS mandatory
DESCRIPTION
"A textual description of the entity. This value should include the full
name and version identification of the system's hardware type, software
operating-system, and networking software. It is mandatory that this only
contain printable ASCII characters."
::= { system 1 }
```

Сингулярный объект SNMP (подобный тому, который показан в листинге 28.1) выражается как идентификатор объекта, в конце которого прибавлен адрес ".0" (OID.0). К примеру, объект sysDescr в группе MIB System Group можно выразить как 1.3.6.1.2.1.1.1.0 — это означает, что у объекта есть только один экземпляр. В обозначении расширений идентификаторов объектов SNMP для сингулярных объектов всегда применяется расширение ".0", позволяющее провести более четкое разграничение между сингулярными и колоночными объектами.

В дополнение к сингулярным объектам, ASN.1 предусматривает описание колоночных объектов, подобных таблицам или последовательностям объектов. Сингулярный объект SNMP представляет лишь одно значение. В ситуациях, когда одному типу соответствует множество записей данных (например, в случае таблицы IP-марш-

рутизации), компоновка этих значений как сингулярных может оказаться сложной или даже невыполнимой задачей (особенно тогда, когда количество записей непостоянно). В таких ситуациях данные лучше всего представлять в виде спископодобных структур или последовательностей, которые называются таблицами. Каждая строка таблицы представляет одно выражение набора объектов, содержащихся в этой таблице. В листинге 28.2 приводится таблица IP-адресов MIB II.

Листинг 28.2. Пример таблицы IP-адресов MIB II с применением SNMP

```
ipAddrTable OBJECT-TYPE
SYNTAX SEQUENCE OF IpAddrEntry
ACCESS not-accessible
STATUS mandatory
DESCRIPTION
"The table of addressing information relevant to this entity's IP ad-
dresses."
::={ip 20 }
ipAddrEntry OBJECT-TYPE
SYNTAX IpAddrEntry
ACCESS not-accessible
STATUS mandatory
DESCRIPTION
"The addressing information for one of this entity's IP addresses."
INDEX { ipAdEntAddr }
::= { ipAddrTable 1 }
IpAddrEntry ::=
SEQUENCE {
ipAdEntAddr
IpAddress,
ipAdEntIfIndex
INTEGER,
ipAdEntNetMask
IpAddress,
ipAdEntBcastAddr
INTEGER
}
```

Базовые правила кодирования

Базовые правила кодирования (BER) регламентируют преобразование значений объектов MIB в формат, обеспечивающий возможность их передачи по сети. Спецификация BER предоставляет способ выражения всех объектов ASN.1 в двоичном формате. Правила BER применяются по отношению к типам, значениям и идентификаторам объектов. Обычно формат значения, закодированного по правилам BER, содержит поле типа (1 байт), длину переменной и поля данных. Этот непротиворечивый формат позволяет разместить несколько объектов в одном пакете ответа на передающей стороне и декодировать эти данные на принимающей стороне.

Идентификаторы объектов MIB

Так как каждая ветвь дерева MIB идентифицируется с помощью числа, каждый из объектов MIB определяется уникальным адресом (называемым идентификатором объекта), который учитывает номер каждой вышестоящей ветви дерева. К примеру, спецификация ISO8824 обозначает низшие ветви дерева SNMP MIB числом 1.3.6.1, где:

- 1 = `iso`;
- 3 = `org`;
- 6 = `dod`;
- 1 = `Internet`.

Но есть множество других ветвей, которые также нужно принять во внимание. Дерево SNMP расположено в рамках поддерева `Internet`, и SNMP может пользоваться четырьмя ветвями, следующими за поддеревом `Internet`.

- Поддерево `directory` (1) зарезервировано OSI для применения в будущем.
- Поддерево `mgmt` (2) заключает в себе стандартные базы SNMP MIB I или II (RFC1156 и RFC1213).
- Поддерево `experimental` (3) зарезервировано для экспериментов с сетью Интернет.
- Поддерево `private` (4) предоставляет пространство для специализированных баз MIB отдельных производителей.

Все частные базы MIB расположены в рамках еще более низкой по иерархическому положению ветви `enterprises` (1). Таким образом, к примеру, каждый идентификатор частного объекта (OID) должен начинаться с базового адреса MIB — `1.3.6.1.4.1` (читай "`iso.org.dod.internet.private.enterprises`"). Другой пример: адрес `1.3.6.1.2.1` (читай "`iso.org.dod.internet.mgmt.mib`") является адресом стандартной базы SNMP MIB I или II в рамках дерева ISO (рис. 28.1). В рамках ветви `mib` стандартные объекты SNMP организуются ниже более высокоуровневых ветвей, называемых группами MIB. Так как количество объектов огромно (в стандарте MIB II их определяется больше двухсот), группы MIB предназначены для упрощения адресации. Группы содержат связанные объекты, подобные ICMP, TCP, EGP и т. д. Адресом объекта (его экземпляра) является путь от корневого уровня MIB до этого самого объекта. К примеру, объект `sysDescr` в группе MIB `System Group` (1.1) обладает адресом `1.3.6.1.2.1.1.1`. В SNMP существует множество стандартных групп MIB — в том числе и нижеприведенные.

- `system`. В этой группе содержится подробная информация об аппаратном обеспечении системы.
- `interfaces`. В этой группе указываются характеристики интерфейса и его ограничения.
- `at`. В этой группе содержится информация, необходимая для проведения трансляции адресов.
- `ip`. В этой группе содержатся статистические данные, необходимые при использовании протокола Интернета (IP).

- `icmp`. В этой группе содержатся статистические данные, необходимые протоколу управляющих сообщений в Интернете (ICMP).
- `tcp`. В этой группе содержится информация о соединении, необходимая при использовании протокола управления передачей (TCP).
- `udp`. В этой группе содержится статистическая информация, необходимая при использовании протокола передачи дейтаграмм пользователя (UDP).
- `egp`. В этой группе содержится информация о компонентах и состоянии, которая задействуется при использовании внешнего шлюзового протокола (EGP).
- `transmission`. В этой группе содержится информация, востребованная объектами, которые пользуются отдельными средами передачи.
- `snmp`. Эта группа имеет дело с объектами, применяемыми для сбора информации во всей сети.

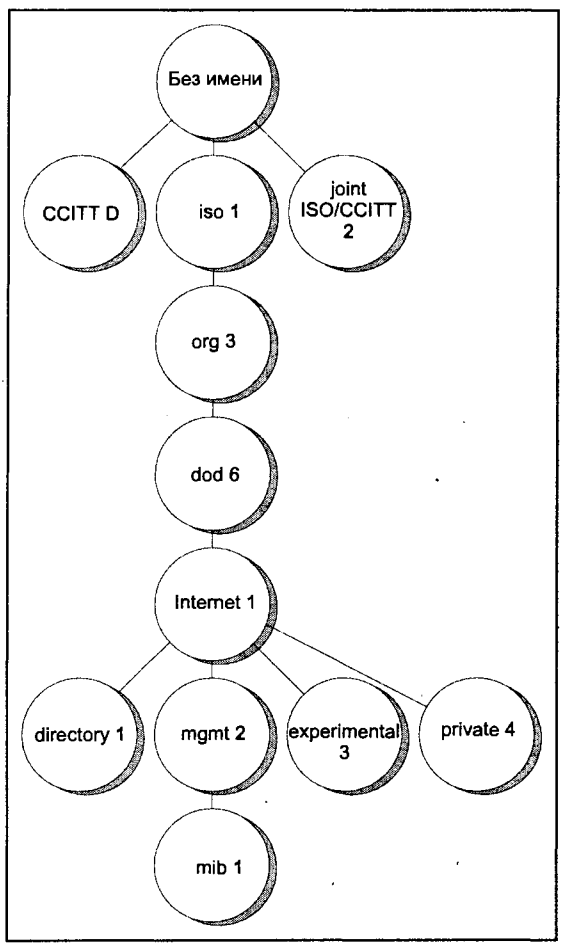


Рис. 28.1. Пример дерева идентификаторов объектов MIB (с разрешения Cisco Systems)

RMON

В SNMP применяется клиент-серверная схема, где инструментальные средства управления исполняет роль сервера, а разнообразные управляемые сетевые объекты — роль клиентов. Эта методика неплохо работает, но в некоторых случаях, когда управляющая станция систематически опрашивает своих агентов, она обуславливает появление избыточного трафика. Разработчики добились преодоления этого потенциального недостатка, создав модуль удаленного сетевого мониторинга (RMON). При наличии RMON клиент-серверная зависимость переворачивается с ног на голову — каждый агент (или зонд RMON) действует независимо, занимает место "сервера" и выполняет всю активную обработку, а управляющая станция исполняет роль их "клиента". При этом управляющей станции больше не приходится опрашивать управляемые объекты с целью сбора обновленных данных. Напротив, эту работу выполняют зонды RMON — они посылают управляющей станции ловушки и передают ей информацию, связанную с определенными событиями, когда эти события происходят. В результате объем непроизводительного трафика, генерируемого SNMP, снижается.

Объекты RMON

Так как агенты RMON зачастую более "интеллектуальны", чем стандартные объекты SNMP, они группируются совершенно по-другому. К примеру, в то время как объекты SNMP, в основном, начинаются с адреса `1.3.6.1`, объекты RMON MIB в сетях Ethernet и в маркерном кольце начинаются с адреса `1.3.6.1.2.1.16`. Большинство объектов RMON принадлежат к следующим группам MIB.

- `statistics`. Эта группа содержит подробные данные о сетевых интерфейсах — она аналогична группе `interfaces` SNMP.
- `history`. Эта группа отвечает за метод сбора данных в сети (например, она контролирует частоту выборки).
- `alarm`. Эта группа управляет аварийными сигналами, применяемыми для сигнализации об определенных событиях.
- `hostTopN`. Эта группа проводит мониторинг статистических данных, связанных с обнаруженными в сети управляемыми хостами.
- `matrix`. Эта группа осуществляет мониторинг статистических данных о трафике между сетевыми хостами.
- `filter`. Эта группа применяется для отбора отдельных пакетов, подлежащих захвату.
- `capture`. С помощью настроек группы `filter` эта группа осуществляет фактическое управление захватом отдельных пакетов.
- `event`. Эта группа управляет настройками, применяемыми для генерирования событий управляющей платформы.

Помимо этого, в современных реализациях RMON присутствует множество дополнительных групп, включая следующие:

- `NIHost`;
- `usrHistory`;
- `TokenRing`;
- `protocolDir`;

- nlMatrix;
- probeConfig;
- protocolDist;
- alHost;
- rmonConformance;
- addressMap;
- alMatrix.

В конечном счете многочисленные существующие группы и объекты RMON обеспечивают широкую функциональность SNMP. RMON предусматривает возможность сбора статистических данных со всех уровней эталонной модели OSI, включая приложения на ее высшем уровне.

Другие протоколы

SNMP (совместно с RMON) — это, безусловно, основной протокол управления, но отнюдь не единственный. Есть еще несколько протоколов, которые вы должны принимать во внимание, занимаясь планированием или внедрением управления сетью — это DMI, HTTP и WEBM.

Рабочая группа по управлению развитием настольных вычислительных систем (Desktop Management Task Force, DMTF) была сформирована в 1992 году из ведущих производителей и корпораций индустрии персональных компьютеров. Они ввели универсальный, платформонезависимый процесс управления настольным аппаратным обеспечением и программными компонентами. Группа DMTF разработала две технологии: программное обеспечение настольного интерфейса управления (Desktop Management Interface, DMI) и язык формата управляющей информации (Management Information Format, MIF). Программа DMI исполняет роль посредника между расположенными в настольной системе управляющими программами, управляемой аппаратурой и программными компонентами компьютера.

В рамках архитектуры DMI управляемые устройства содержат программный компонент, называемый уровнем обслуживания. Уровень обслуживания (и его расширения) производит мониторинг различных подсистем управляемого устройства и предоставляет эту информацию консолям управления системами. DMIv2 предусматривает новые функции, включая стандартный метод обмена информацией DMI по сети и метод обработки предупреждений. Управляющее программное обеспечение (например, Compaq Insight Manager 7) способно принимать данные DMI, которые, поступая в него, преобразуются в ловушки и связываются с устройством, их отправляющим.

Помимо этого, некоторые управляющие программы пользуются стандартным протоколом HTTP (он применяется для передачи информации во Всемирной паутине), с его помощью осуществляя передачу управляющей информации. Ведущие разработчики управляющих продуктов основывают эти работы на инициативе по системам Web-управления предприятиями (Web-based Enterprise Management, WBEM). Эту инициативу поддерживают компании Compaq, Microsoft, Intel, BMC, Cisco и еще 120 других поставщиков платформ, операционных систем и прикладного программного обеспечения.

Примечание

Ключевым моментом при оценке любой схемы управления является аппаратная совместимость. Избегайте применения инструментов управления с ограниченными

или специализированными протоколами, не поддерживающими существующие и планируемые к установке в вашей сети устройства.

Dell OpenManage

Сетевое управление позволяет администраторам выполнять инвентаризацию, сопровождение и обновление программного обеспечения и драйверов, и даже организовывать поиск неисправностей клиентских и серверных систем в сети — и все это с центральной станции управления. Теперь, когда вы ознакомились с некоторыми базовыми понятиями, связанными с управлением сетью, мы рассмотрим одну из существующих платформ управления — Dell OpenManage. В отличие от обычных приложений, управляющее программное обеспечение обычно не реализуется в виде единой универсальной программы, устанавливаемой на всех сетевых устройствах. Напротив, инструментальные средства управления обычно подразделяются на ряд функциональных модулей, направленных на реализацию отдельных функций на клиентских или серверных машинах или на других устройствах.

Примечание

Инструментальные средства управления, предлагаемые разными производителями — например, HP, Compaq, Gateway и др. — могут значительно различаться между собой. В этой части главы средства Dell OpenManage предлагаются исключительно в качестве примера.

Администрирование клиентского компьютера

Управление сетью полезно лишь в том случае, если администратор имеет возможность доступа и управления различными рабочими станциями, установленными в сети. У каждой рабочей станции должен быть собственный инструментарий — программное обеспечение, способное проверять состояние аппаратуры и настройки ПО. Кроме того, необходимо присутствие консоли управления, чья функция заключается в анализе данных, собранных на каждой рабочей станции, и составлении отчетов об этих данных. Платформа Dell OpenManage предусматривает различные функции, связанные с управлением рабочими станциями.

- *OpenManage Client Instrumentation, OMCI.* OMCI — это приложение, предназначенное для работы в системах Dell OptiPlex, Precision и Latitude. OMCI основывается на стандартных протоколах управления, таких как DMI и CIM (Customer Interaction Management — управление взаимодействием с клиентами), и предусматривает поддержку SNMP. OMCI позволяет консоли управления (отдельному приложению), соответствующей стандартам DMI, CIM или SNMP, осуществлять сбор инвентаризационной и конфигурационной информации, а также получать упреждающие оповещения о возможных сбойных ситуациях. OMCI проводит мониторинг системного аппаратного обеспечения, и в случае вскрытия системного блока или обнаружения потенциальной проблемы отправляет предупреждение. В сочетании с такими инструментальными средствами, как Dell IT Assistant, OMCI позволяет администратору производить удаленные обновления систем BIOS и изменять настройки CMOS как в отдельной системе, так и в рамках группы систем.

- *OpenManage Image Management.* В процессе развертывания рабочих станций со стандартными комплектами программного обеспечения часто обнаруживается, что проще установить предварительно составленные образы дисков, которые без труда поддаются переносу на новую станцию (вместо ручной инсталляции операционных систем и приложений). Средства управления образами Dell OpenManage реализованы в виде программы, разработанной в компании StorageSoft Corporation. Продукт StorageSoft ImageCast IC3 значительно упрощает процесс первоначального развертывания образов. На клиентских машинах Dell образы дисков могут бесплатно развертываться и обновляться в течение 30 дней. ImageCast IC3 — это недорогое инструментальное средство быстрого развертывания, поддерживающее многоадресную передачу образов по сети.
- *OpenManage IT Assistant.* Dell OpenManage IT Assistant — это средство управления рабочими группами, направленное на координацию клиентских и серверных машин. Оно не является обязательным компонентом управления клиентами Dell и представляет собой простую в использовании консоль управления на основе браузера, которая позволяет администратору оперативно проводить мониторинг степени исправности систем. В нем есть механизм обнаружения, проводящий идентификацию систем, помещающий их в надлежащую группу (например, в группу настольных или портативных компьютеров, рабочих станций или серверов) и предоставляющий весьма детальные данные о конфигурации, ОС и аппаратном составе систем.
- *OpenManage Software Management.* Средства управления программным обеспечением Dell OpenManage (выполняющие задачи наподобие инсталляции или обновления отдельных программ на сетевых компьютерах) реализованы в виде программы от компании ON Technology. Централизованные средства управления и контроля ON Command обеспечивают возможность оперативного управления приложениями и конфигурациями; они предназначены для корпоративных клиентов, которые не желают ограничиваться теми возможностями, которые предусматриваются в традиционных утилитах обслуживания. ON Command Special Edition помогает проводить первоначальную настройку и стандартизацию клиентских машин Dell, причем в течение 30 дней после приобретения это можно делать совершенно бесплатно, а по прошествии этого срока, чтобы получить возможность осуществления текущего управления программным обеспечением, — обновить до полной версии централизованной системы управления и контроля ON Command.
- *OpenManage Data/Personality Migration.* При необходимости замены персонального компьютера (для его ремонта или модернизации) перемещение существующего программного обеспечения, данных и пользовательских настроек на новую систему может стать крайне трудоемкой задачей. Personality Migration позволяет упростить процесс переноса данных старого компьютера на новый. В состав OpenManage входит продукт Miramar Desktop DNA, выполняющий роль инструмента для проведения миграции систем. Desktop DNA позволяет пользователям настольных компьютеров на свое усмотрение выбирать, сохранять и перемещать специальные настройки системы и приложений, сами приложения и файлы из системы Windows на один или несколько компьютеров — как локально, так и в масштабах всего предприятия. Результатом является уменьшение объема работы ИТ-специалистов и снижение рисков, связанных с миграцией данных.

Примечание

Помимо прочего, существуют дополнительные инструментальные средства OpenManage, предусматривающие управление массивами и кластерами.

Администрирование сервера

Кроме всего вышеперечисленного, в состав платформы OpenManage входит программное обеспечение Server Administrator. Это защищенный Web-инструментарий, предназначенный для управления отдельными серверами — например, принадлежащими к линейке Dell PowerEdge. Server Administration позволяет администратору с помощью соединения Интернет/интранет управлять сервером, находясь в любом месте и пользуясь для этого обычным Web-браузером. В дополнение к простому получению информации о состоянии, администратор может проводить поиск неисправностей, конфигурировать и обновлять сервер (рис. 28.2). В соответствии с типичным сценарием, консоль управления обнаруживает на сервере событие, требующее внимания, и отправляет администратору (или техническому специалисту) сообщение электронной почты или страничное оповещение. При поиске и устранении возникшей проблемы администратор, как правило, выполняет все действия с центральной консоли. Зачастую при необходимости проведения диагностических операций или обновлений системы технический специалист лично отправляется к нужному серверу.

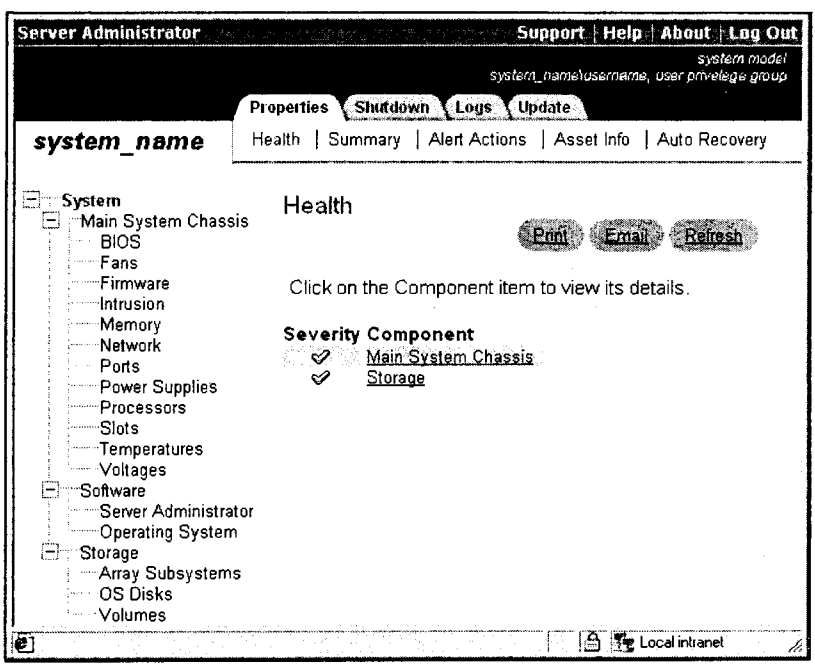


Рис. 28.2. Управление сетевыми серверами с помощью утилиты Dell OpenManage Server Administrator (с разрешения Dell Computer Corporation)

Server Administrator работает на каждом управляемом сетевом сервере. Администратор может обращаться к действующему серверу (если тот не отключен от источника питания и не заблокирован). Он может анализировать данные, связанные с аппаратной частью системы и ее конфигурацией, задействовать инструменты диагностики, настраивать BIOS и регулировать системные настройки, просматривать журнал аудита, в котором фиксируются все аппаратные события, предупреждения и команды, произошедшие на сервере, и выполнять процедуры обновления системы. Если администратор обнаруживает необходимость проведения аналогичного обновления на других серверах, он может воспользоваться дополнительным интерфейсом командной строки, запустив с его помощью сценарии автоматизации на группах серверов. Посредством Web-интерфейса и интерфейса командной строки администраторы могут выполнять следующие функции управления:

- запускать средства оперативной диагностики для поиска способов устранения проблем;
- обновлять программно-аппаратные средства и BIOS;
- вести контрольный журнал изменений, происходящих на сервере;
- выполнять мониторинг и сообщать о состоянии сервера;
- получать информацию об имуществе и размещении;
- осуществлять удаленное закрытие и перезагрузку системы.

Оперативная диагностика

Администраторы могут запускать процедуры диагностики на разных компонентах сервера (включая RAID- и SCSI-контроллеры, центральный процессор, жесткий диск, память, сетевую плату и шину PCI). Диагностические операции, не требующие вмешательства со стороны администратора, можно запланировать на более позднее время, а их результаты — послать по электронной почте на определенные почтовые ящики. К примеру, результаты можно отправить администратору или другим техническим сотрудникам, которым она поможет повысить качество сопровождения.

Обновления программно-аппаратных средств и BIOS

Эта функция позволяет системным администраторам обновлять BIOS и встроенные программно-аппаратные средства сервера, включая встроенную систему управления сервером версии 2 (Embedded Server Management 2, или ESM2) — программно-аппаратные средства серверов Dell. В последующих версиях программного обеспечения Server Management, по-видимому, будет внедрена поддержка обновлений драйверов. Обновления можно проводить как в отдельных системах (через Web-интерфейс Server Administrator), так и в группах систем (при помощи интерфейса командной строки). Функцию обновления BIOS администратор может задействовать для того, чтобы:

- знакомиться с отчетом о версиях, в котором указываются текущие версии BIOS, "зашитых" программ и операционной системы;
- выбирать пакеты обновлений BIOS или программно-аппаратных средств;
- проверять достоверность выбранного пакета обновлений;

- выполнять обновление BIOS или программно-аппаратных средств;
- распечатывать данные о BIOS и "зашитых" программах, представленные на домашней странице;
- отправлять сообщения электронной почты с отчетами о проведенных обновлениях на указанные почтовые адреса;
- кроме того, существует механизм проверки достоверности, способный подтверждать правильность выбранного пакета обновления.

Контрольные журналы

Server Administrator ведет подробнейший журнал всех аппаратных событий, предупреждений и команд, выполняемых на сервере, причем журнал этот можно просматривать через Web-интерфейс. Предусматривается возможность настройки местонахождения и размера файла, в котором он хранится. Это *циркулярный файл* — когда он достигает определенного размера, наиболее старая информация заменяется новой. Контрольный журнал оказывается полезным в ходе поиска путей устранения неисправностей. Именно к нему администратор может обратиться, чтобы просмотреть команды, исполнявшиеся на сервере в период развития проблемы. Журнал можно экспортировать в файл формата ASCII, который, в свою очередь, может собираться сценариями автоматизации в целях архивации или анализа.

Мониторинг состояния системы

Server Administrator осуществляет мониторинг работоспособности системы и предоставляет быстрый доступ к подробным данным о сбоях и производительности, собранным агентами системы. Функции генерирования отчетов и просмотра позволяют администратору проверять общее состояние всех серверных корпусов, из которых состоит система. На уровне подсистем присутствует информация о напряжениях, температурах, текущем числе оборотов вентилятора в минуту и функционировании памяти каждого из ключевых блоков системы. В сводном представлении доступна обработанная информация о стоимости владения. Администраторы имеют возможность настроить Server Administrator на вывод предупреждений при наступлении определенных условий (например, в случае, если температура центрального процессора или уровень напряжения выходят за пределы нормального диапазона). В зависимости от типа предупреждения, программа может, исходя из настроек, отвечать по-разному — например, отсылать на центральную консоль ловушку протокола SNMP, отправлять широковещательные сообщения всем пользователям, зарегистрированным на сервере, или запускать какое-либо приложение.

Информация о сетевом имуществе

На сводном экране представлена общая информация о системе — среди прочего, там указывается местонахождение сервера, его сервисная метка, имущественная метка, данные о процессоре, список свободных слотов и емкость жесткого диска. Подобные отчеты об имуществе можно экспортировать в другие программные пакеты (например, в Excel) для финансовой отчетности или выполнения описей.

Удаленное отключение и перезагрузка системы

Когда сервер находится в рабочем состоянии, он может быть отключен или перезагружен средствами Server Administrator, для этого даже не требуется карта удаленно-

го доступа (зато она необходима при перезагрузке или диагностике неисправностей на отключенном сервере).

Web-интерфейс и интерфейс командной строки

Агенты управления стандартными для индустрии системами, установленные на сервере, осуществляют сбор подробных данных о конфигурации, неисправностях и производительности. Эта информация передается посредством стандартного комплекта отчетов, доступных через Web-интерфейс. Web-интерфейс является переносимым (он работает в различных стандартных браузерах и допускает возможность удаленного доступа с систем, расположенных вне локальной сети) и высокопроизводительным. В дополнение к функциям составления отчетов, утилиты оперативной диагностики и обновления систем позволяют выполнять реальные задачи по управлению благодаря своим инструментам.

Напротив, интерфейс командной строки предназначен для применения в условиях, когда системные администраторы выполняют большинство задач с помощью сценариев, исполняемых на группах серверов. При помощи интерфейса командной строки программы Server Administrator администратор может составить сценарий конфигурации с указанием порогов предупреждения для каждого из основных компонентов системы, а также действий, которые необходимо предпринимать в случае превышения такого порога. Для критически важных компонентов в сценарии можно задать необходимость отключения питания в целях предотвращения повреждений. Такой сценарий можно распространить и исполнять на нескольких системах, входящих в группу. Возможность составления сценариев позволяет администраторам с легкостью настраивать новые системы и внедрять новые политики администрирования сразу на множестве установленных систем.

Во многих случаях интерфейс командной строки позволяет пользователю, который должен выполнить четко определенную задачу, оперативно извлечь информацию о системе. При помощи этого интерфейса производится анализ комплексных сводок обо всех компонентах системы и сохранения этих сводок в файлы для сравнения с последующими состояниями системы. Кроме того, администраторы могут составлять пакетные программы или сценарии в расчете на их исполнение в определенное время и с целью фиксации отчетов об определенных компонентах (к примеру, о числе оборотов вентилятора в минуту в периоды высокого и низкого уровней использования системы). Форматированные результаты можно сохранять в файл с целью последующего проведения его анализа. Основными командами Server Administrator являются следующие:

- `omdiag` — запуск диагностических тестов аппаратного и программного обеспечения системы с целью локализации неисправностей;
- `omupdate` — обновление версий BIOS и программно-аппаратных средств;
- `omreport` — вывод итоговых данных о компонентах, относящихся к системе в целом;
- `omconfig` — установка важнейших параметров для настраиваемых компонентов системы (значения порогов, действия, предпринимаемые в случае превышения этих порогов, имущественные данные и т. д.).

Поддержка операционной системы

При выборе инструментальных средств управления важно учитывать их совместимость с операционными системами, установленными на ваших сетевых серверах. К примеру, в полной мере возможности Serve Administrator реализуются в системах Windows NT Server 4 (Service Pack 5 или более поздняя версия пакета обслуживания) и в семействе Windows 2000 Server (включая Windows 2000 Server, Windows 2000 Advanced Server, Windows 2000 Terminal Services и Windows Small Business Server 2000). Кроме того, Dell Server Administrator работает в системах Red Hat Linux версий 7.1 и выше. Ограниченный набор функций Server Administrator реализуется в средах Novell NetWare 5.1 (Service Pack 3), 6.0 и в более поздних версиях. В операционных системах Novell функции оперативной диагностики и обновления "зашитых" программ и BIOS отсутствуют.

Приемы управления и поиск неисправностей

Dell OpenManage — это лишь один из существующих комплексов инструментальных средств, предназначенных для управления сетями; на сегодняшний день платформы управления многочисленны (среди них есть инструментальные средства от Compaq, HP, Gateway и других компаний). В условиях такого изобилия выбор оптимальных методик применения этих средств зачастую оказывается трудной задачей. В этой части главы представлены некоторые существенные предложения, связанные с управлением сетью.

Читайте документацию

Средства сетевого управления обычно состоят из нескольких мощных модулей, поэтому вы должны обратить особое внимание на анализ возможностей (и ограничений) выбранной платформы управления. Разберитесь в том, как запускать процесс первоначального обнаружения и идентификации сетевых устройств, узнайте, как подключать к системе управления дополнительные устройства. Возможно, для автоматизации обнаружения и идентификации сетевых устройств вы сможете воспользоваться мастером конфигурации (таким как мастер Initial Configuration Wizard, применяемый в Compaq Insight Manager 7).

Вникните в систему безопасности

Безопасность системы управления сетью — это серьезная задача, и администраторам следует принимать все меры предосторожности, чтобы не допустить обращения неуполномоченных пользователей к управляющей информации (в особенности через Web-инструменты наподобие Dell OpenManage Server Administrator). Даже в том случае, когда сетевые данные не являются уязвимыми, способность платформ сетевого управления регулировать параметры устройств (и, следовательно, препятствовать исполнению важных сетевых служб) делает их лакомым куском для злонамеренных пользователей. Ознакомьтесь с функциями обеспечения безопасности, предусматриваемыми определенной платформой управления, и последовательно внедряйте эти функции.

Проанализируйте обнаруженные устройства

Важной задачей администратора является обнаружение разнообразных устройств и опрос их состояния — все это делается с помощью платформы управления. После того как инструментальные средства управления обнаружили и идентифицировали сетевые устройства, вы должны выделить некоторое время на то, чтобы просмотреть результаты этих процедур. Пользуясь платформой управления, пройдитесь по серверам, рабочим станциям и другим устройствам, обнаруженным в сети, и попрактикуйтесь в формировании запросов — нахождение конкретных элементов не должно представлять для вас трудности. К примеру, вы можете, как правило, создавать запрос на вывод перечня наиболее важных сетевых устройств.

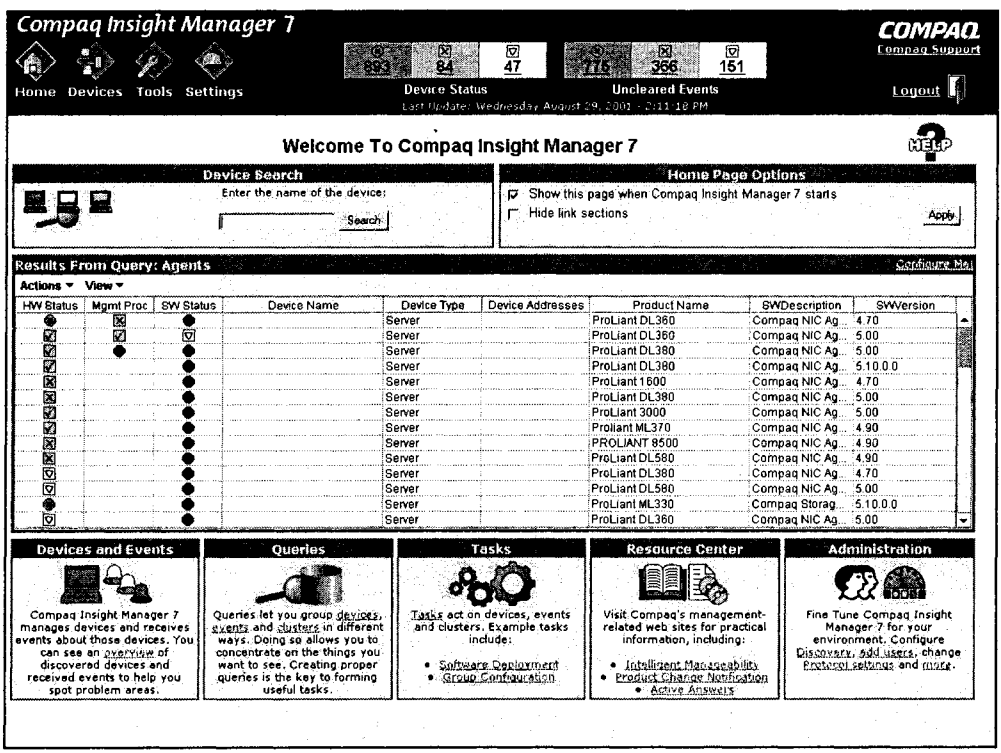


Рис. 28.3. Управление сетью с помощью Compaq Insight Manager 7 (с разрешения Compaq Computer Corporation)

Compaq Insight Manager предоставляет страницу устройств, на которой помещается весьма подробная информация об обнаруженных устройствах (рис. 28.3). От домашней страницы можно перейти на страницу устройств Compaq Insight Manager 7, а с нее дальше — к различным агентам устройств. Для просмотра подробных данных, возвращенных конкретным агентом, перейдите по ссылке на соответствующее устройство. К примеру, если речь идет об узле группы пользователей, то, чтобы получить подробную информацию об этой группе и ее участниках, перейдите по ссылке устройства **Compaq Intelligent Cluster Administrator**. Выполнив эту задачу и намерева-

ясь перейти к другим функциям, возвратитесь на страницу устройств и выберите нужные ссылки. Для того чтобы ознакомиться со сводкой текущего состояния устройств и их событий, щелкните на пиктограмме **Devices** (Устройства) на панели инструментов и выберите **Overview** (Краткий перечень).

Настройте график обнаружения

Зачастую, в соответствии со своими настройками по умолчанию, инструментальные средства управления соблюдают предустановленный график повторного обнаружения сетевых устройств. Впрочем, вам может потребоваться изменить график, установив более подходящее время, прибавить или удалить подсети, и выбрать метод(ы) обнаружения устройств. В случае интенсивного использования пропускной способности сети вы можете оптимизировать настройки SNMP и Ping, и тем самым понизить уровень трафика. Кроме того, при необходимости здесь же можно создать новые учетные записи консоли управления.

Настройте порядок опроса абонентов с учетом их важности

Инструментальные средства управления обычно опрашивают устройства непрерывно — они запускают ряд запланированных задач, принятых по умолчанию. Однако вы можете сформировать задачи опроса так, чтобы мониторинг отдельной группы устройств осуществлялся в соответствии с их собственным графиком. К примеру, на устройствах определенного типа можно сохранять статистические данные для их последующего анализа и прогнозирования. Как правило, настройки на периодический сбор данных (статистических или в виде отдельных случаев) отсутствуют. В ваших силах составить задачу, которая будет оптимально подходить именно для конкретной сети. Имейте в виду, что процедуры сбора данных могут привести к появлению постоянного сетевого трафика, поэтому планировать задачи нужно таким образом, чтобы устройства, представляющие для вас наибольший интерес, опрашивались чаще, а все прочие устройства — реже.

Настройте уведомления об ошибках

Если возникает неисправность, вы должны об этом знать. Консоль управления постоянно обновляется, информируя вас о последних критических, важных и незначительных событиях. Однако, если вы покидаете консоль, можно выполнить настройки оповещения по электронной почте или по пейджинговой связи (или, при помощи задачи "запуск приложения", настроить оригинальный метод оповещения). Степень сложности такого приложения произвольна — оно может просто воспроизводить на консоли управления звуковой сигнал, или даже напрямую взаимодействовать с устройством (например, производить автоматический перезапуск службы, работающей на этом устройстве). В случае если вы решите настроить оповещение по пейджинговой связи, не забудьте установить модем и настроить его так, как того требует производитель.

Тщательно систематизируйте устройства

Если вы управляете несколькими подсетями, то процедуры опроса могут распространяться на сотни устройств. Для достижения оптимального управления их нужно

организовать в логические группы. Платформы управления наподобие Compaq Insight Manager 7 самостоятельно приступают к сортировке, пользуясь для этого аппаратными запросами. Впрочем, эти запросы можно редактировать, удалять ненужные и создавать новые (как запросы, так и категории запросов), в соответствии с требованиями управления вашей сетью. Вы можете указывать, какие устройства нужно опрашивать, и когда это следует делать. К примеру, ничто не мешает вам создать запрос, который будет опрашивать организационную группу устройств, среди которых могут быть серверы, настольные компьютеры и принтеры. С другой стороны, процедуры опросов могут распространяться на логическую группу устройств (например, на принтеры в группе снабжения).

Организуйте доставку сообщений о событиях

Сеть, состоящая из сотен устройств, потенциально может генерировать тысячи сообщений. Некоторые из них являются исключительно информационными. С помощью механизма фильтрации вы можете отказаться от ненужных сообщений и обеспечить получение важных. Система фильтрации событий сортирует сообщения и выбирает самые важные из них. Переадресация событий позволяет указывать те пункты назначения на консоли, в которых эти сообщения действительно нужны. Платформы управления обычно предусматривают выполнение запросов и отчетов об общих событиях, но вы можете внести в эти запросы изменения, приспособив их для данной сетевой среды, или создать новые запросы, связанные с определенными устройствами и событиями. К примеру, в ваших силах избавиться от ненужных информационных сообщений или сформировать запрос для проверки статуса событий на всех серверах, которые, по вашему мнению, не должны заметно ухудшить уровень обслуживания (например, на Web-серверах).

Идентифицируйте неизвестные устройства

Нет гарантии, что система управления сможет должным образом идентифицировать все сетевые устройства. К счастью, многие системы управления позволяют вам формулировать собственные правила идентификации. К примеру, вы могли бы создать правило, направленное на идентификацию неизвестных устройств, таких как принтеры. Большинство принтеров, работающих в сети, располагают конфигурационными Web-программами. Система управления обнаруживает эти программы и создает в консоли управления ссылки на них. При помощи ссылок вы можете перемещаться по этим Web-программам и управлять своим принтером. Кроме того, у вас есть возможность зарегистрировать базы MIB других компаний, которые способны обеспечить обнаружение, идентификацию и получение ловушек SNMP на соответствующих устройствах. К примеру, можно зарегистрировать базы MIB, которые предоставят данные о маршрутизаторах. Ничто не мешает вам редактировать сообщения-ловушки SNMP — для того, чтобы они легче поддавались интерпретации.

Добавьте новые устройства

Вы можете добавить одно или несколько устройств в существующую управляемую сеть, не прибегая к автоматическому обнаружению. К примеру, если новая группа объединяется со средой управления, всех ее участников можно интегрировать одновременно с помощью диапазона IP-адресов, можно добавлять по одному устройству

за раз, а можно импортировать файл hosts. Ручное обнаружение способствует экономии сетевых ресурсов. К примеру, вы можете экспортировать файл с именами устройств и их IP-адресами, а затем импортировать его в систему управления. Во время выполнения следующего цикла обнаружения система управления собирает дополнительные идентификационные данные и помещает их в базу данных, но сам процесс обнаружения и идентификации уже свершился.

Внесение исправлений

Учитывая быстрый рост числа доступных на сегодняшний день компонентов управления, крайне сложно выполнять поиск неисправностей в средствах управления, не обращаясь к конкретным инструкциям производителя. Однако приведенные ниже советы способствуют пониманию ряда простейших проблем, о которых вы должны иметь представление.

- *Проблемы TCP/IP.* Адрес TCP/IP сетевого администратора отсутствует или неправильно настроен управляющей программой клиентского администрирования (например, Dell OpenManage Client Administrator). Проверьте установку и настройку TCP/IP в рамках операционной системы.
- *Проблемы с физическим соединением.* Компьютер (или другое устройство) не подключен к сети. Проверьте сетевое соединение (кабель, сетевую плату, концентратор/коммутатор).
- *Проблемы с логическим соединением.* Соединение с указанным клиентом недействительно. Попробуйте провести повторное подключение к клиенту (например, DMI или SNMP), управлением которого вы собираетесь заняться; перезагрузите клиента, и попробуйте подключиться еще раз.
- *Административное программное обеспечение недоступно.* Программа клиентского администрирования (например, Dell OpenManage Client Administrator) заблокирована в локальной системе. Чтобы получить возможность повторного обращения к программе клиентского администрирования, вы должны перезагрузить компьютер.
- *Несоответствие обновления BIOS.* Программе клиентского администрирования не удается провести удаленное обновление флэш-памяти BIOS (или программно-аппаратных средств), т. к. существующий файл обновления BIOS не соответствует системе BIOS, установленной в выбранной системе (системах). Новый файл BIOS не подходит для той системы (для тех систем), в которой вы пытаетесь его установить. Загрузите корректный файл BIOS и попытайтесь провести обновление еще раз.
- *Обновление BIOS блокируется по таймеру ожидания конца процедуры.* Выбранная удаленная система была отключена во время удаленного обновления ее BIOS, и программе клиентского администрирования не удалось выполнить эту процедуру. Убедитесь в том, что удаленная система подключена к источнику питания и находится в рабочем состоянии. Повторите попытку удаленного обновления флэш-памяти BIOS в удаленной системе.
- *Предупреждения при обновлении BIOS.* При проведении процедуры удаленного обновления флэш-памяти BIOS ("зашитых" программ) удаленную систему (системы) необходимо перезагрузить. Администратор должен быть уверен в том, что

обновляемые системы не используются, или отправить всем задействованным станциям широковещательное сообщение — с тем, чтобы предоставить пользователям время, достаточное для сохранения их документов и выхода из системы до начала процедуры обновления. Эти предложения действительны и при планировании удаленного обновления приложений.

- *Проблемы с программным соединением.* Программе клиентского администрирования не удается подключиться к удаленной системе, расположенной в клиентской сети. Удаленная система отключена. Обеспечьте подключение удаленной системы к источнику питания и введите ее в рабочее состояние. Если удаленной системой является портативный компьютер, проверьте состояние его аккумулятора или адаптера переменного тока, и проверьте, включен ли он. Возможно, удаленная система не настроена на участие в клиентской сети DMI/SNMP. Настройте удаленную систему на применение нужного протокола клиентской сети. Возможно, на удаленной системе не установлено необходимое клиентское программное обеспечение (например, Dell OpenManage Client). Обеспечьте наличие в удаленной системе клиентского программного обеспечения, которое требуется для достижения поставленных задач.
- *Имя устройства изменилось.* Имя локальной системы было обновлено или изменилось. Управляющий клиент не сможет обнаружить обновленное имя системы, пока данная локальная система не будет перезагружена. Перезагрузите локальную систему.
- *Неверный пароль.* Установить пароль настройки не удается: новый пароль не соответствует старому. При появлении соответствующих приглашений введите старый и новый пароли повторно.
- *Предупреждения о выключении системы.* К примеру, возможно появление сообщения о том, что некая локальная система будет выключена в течение 60 секунд. Так происходит в случае, когда программа клиентского администрирования обнаруживает в локальной системе некритическое, критическое или невосстановимое событие, которое приводит к отключению этой системы. Это — нормальная профилактика. Чтобы предотвратить потерю данных, сохраните и закройте все файлы, а затем перезагрузите систему, в которой выявлены нарушения.

Дополнительные ресурсы

Compaq: **www.compaq.com**.

Computer Associates: **www.ca.com**.

Dell: **support.dell.com**.

Gateway: **www.gateway.com**.

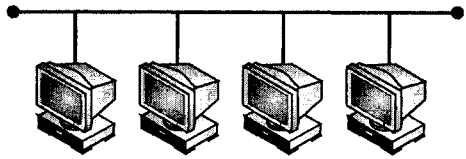
HP: **www.hp.com**.

Базы данных MIB:
www.cisco.com/univercd/cc/td/doc/product/software/ios112/mbook/mover.htm.

SNMPv3: **www.ibr.cs.tu-bs.de/projects/snmpv3/**.

Tivoli: **www.tivoli.com**.

Veritas: **www.veritas.com**.



ГЛАВА 29

Основы поиска неисправностей в сетях

Поиск неисправностей — удивительное занятие, нечто среднее между искусством и наукой. Сети крайне удобны, когда все в них исправно работает, но в случае возникновения проблем они ужасно действуют на нервы. Любой администратор или технический специалист, в задачи которого входит сопровождение и поиск неисправностей в компьютерных сетях, должен не только знать важные принципы функционирования сети и сетевые операции, но и разбираться в основных правилах и методиках поиска неисправностей. Это особенно важно при необходимости проработки многочисленных инструкций и симптомов, представленных на протяжении всей этой книги. В настоящей главе мы ставили своей задачей представить начинающим техникам основные принципы диагностики и рассмотреть некоторые наиболее популярные сервисные программы, предназначенные для проведения диагностических операций в сети. Впрочем, даже опытные технические специалисты, вероятно, сочтут эту главу удобным справочным пособием.

Общие принципы поиска неисправностей

Профессиональный специалист по сетям должен уяснить одно из основных правил бизнеса: время — деньги. Независимо от того, кто вы — предприниматель или наемный рабочий, — способность быстро и решительно выявлять и локализовывать сбои является важнейшим элементом вашего успеха. Для этого нужен острый глаз, немного здравого смысла и совсем чуть-чуть интуиции. Кроме того, необходимо иметь представление о процессе поиска неисправностей и надежный план действий.

Несмотря на то, что количество сетевых конфигураций и настроек фактически ничем не ограничено, методология, применяемая при проработке каждой проблемы, почти всегда одинакова. Эта часть главы направлена на рассмотрение основных принципов поиска неисправностей, демонстрацию методов применения ряда причинно-следственных отношений, которые способны помочь сузить проблему еще до того, как вы вскроете монтажный шкаф. Применив последовательную методику, вы можете сэкономить ценное время, какая бы восстановительная задача перед вами ни стояла.

Универсальная процедура поиска неисправностей

Независимо от сложности отдельного компьютера или сети, процедура поиска неисправностей, на которую всегда можно положиться, делится на четыре основных этапа. Они проиллюстрированы на рис. 29.1: сначала вы определяетесь с симптомами, потом выявляете и локализуете возможный источник (или местонахождение) неисправности, заменяете подозрительную подсистему, и, наконец, чтобы убедиться в исчезновении проблемы, повторно проводите полное тестирование системы. Если разрешить проблему не удалось, смело начинайте с шага № 1. Это — "универсальная" процедура, применимая к поиску любых неисправностей, причем не только тех, что связаны с оборудованием персональных компьютеров и сетями.

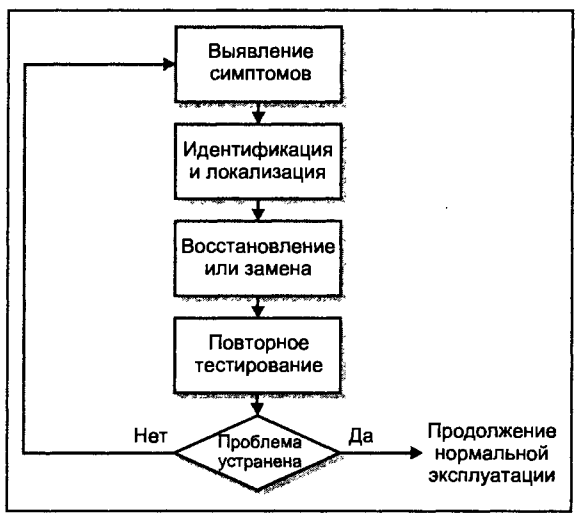


Рис. 29.1. Универсальный процесс поиска неисправностей

Определитесь с симптомами

Причина выхода сети из строя может быть как простой, например, плохо зафиксированный провод или разъем (коннектор), так и сложной, к примеру, сбой в микросхеме или в подсистеме. Прежде чем открывать ящик с инструментами, необходимо полностью уяснить все симптомы. Хорошо подумайте, в чем они заключаются. К примеру, можно задаться следующими вопросами.

- Удается ли рабочим станциям обращаться к серверу или маршрутизатору?
- Не сложилась ли ситуация, при которой Ping-запрос, отправленный на одну сторону маршрутизатора или сети, завершается успешно, а аналогичный запрос, отправленный на другую сторону, завершается ничем?
- Зажигаются ли светодиоды питания или активности?
- Не возникает ли неисправность только тогда, когда компьютер подключают к сети или удаляют?

Выявив симптомы и разобравшись в их сути, вы значительно упрощаете задачу локализации неисправности в рамках конкретного компоновочного блока или компонента. Не жалейте времени — запишите как можно больше симптомов. Сейчас это занятие, вероятно, кажется слишком утомительным, но потом, когда вы перейдете непосредственно к ремонту, письменная фиксация симптомов и обстоятельств поможет сконцентрироваться на одной задаче. Кроме того, она укрепит симптомы в вашей памяти — на случай, если впоследствии их придется разъяснять кому-то другому. В любом случае, профессиональному специалисту по устранению неисправностей зачастую приходится регистрировать имеющиеся проблемы или каким-то другим образом документировать свои действия.

Идентификация и локализация

Прежде чем пытаться изолировать проблему в рамках сети или аппаратного устройства, необходимо убедиться в том, что причиной ее возникновения послужило именно оборудование. Во многих случаях это оказывается очевидным, но бывают ситуации, допускающие двоякое толкование (например, при отсутствии питания, отсутствии командной строки DOS и т. д.). Всегда помните, что сеть функционирует благодаря тесному взаимодействию аппаратного и программного обеспечения. Неисправный или неверно настроенный программный блок может вызывать появление сбивающих с толку системных ошибок с тем же успехом, с каким это может делать вышедшее из строя аппаратное устройство. Только лишь выявив возможную проблемную область, вы сможете приступить к самому процессу ремонта — заменить подозрительную подсистему или провести повторную конфигурацию подозрительного программного обеспечения.

Замена

Так как сети замышлялись как совокупности подсистем, в большинстве случаев сразу заменить подсистему оказывается проще, чем пытаться устранить ее неполадки на компонентном уровне. В современных условиях сети часто оказываются необходимым элементом нормального функционирования предприятий, так что замена неисправного компонента (например, вышедшей из строя сетевой платы или концентратора) зачастую оказывается наиболее экономически эффективным способом возврата сети в работоспособное состояние. Производители и связанные с ними распространители часто предлагают подсистемы и оборудование в ассортименте. Имейте в виду: для того, чтобы заказать новую подсистему, вам, вероятно, придется узнать производственный шифр компонента старой подсистемы.

Другой проблемой, связанной с быстрым технологическим прогрессом, является то, что компоненты редко остаются в продаже надолго. Того 16-портового концентратора, который вы купили год назад, уже нет на прилавках, не так ли? А как насчет привода CD-ROM с автоматической сменой дисков, поставленного некоторое время назад? Сегодня уже есть что-то более новое, более быстродействующее. Когда компьютер выходит из строя, и перед вами встает задача замены неисправного устройства, вероятнее всего, вам придется проводить модернизацию — по той простой причине, что взамен старого устройства вы не сможете найти идентичное. С этой точки зрения, модернизация зачастую замещает процессы поиска неисправностей и восстановления.

Повторное тестирование

Когда ремонт наконец будет завершен, сетевые устройства придется установить заново, а после этого протестировать. Прежде чем проводить окончательные испытания, необходимо поставить на свои места всю защиту, корпуса, кабели и фильтры. Если симптомы сохранятся, придется провести их переоценку и локализовать неисправность в другой части сети. Если нормальное функционирование удастся восстановить (или значительно улучшить), нужно протестировать различные функции сети. Когда вы сможете убедиться в том, что при работе системы все симптомы исчезли, оборудование можно вновь запускать в работу. Как правило, имеет смысл позволить системе поработать, по меньшей мере, 24 часа — это позволяет удостовериться в том, что новая подсистема не выйдет из строя преждевременно. Это называется приработкой системы.

Не отчаивайтесь, обнаружив, что сеть до сих пор работает плохо. Возможно, вы забыли о каком-то соединении. Быть может, для того, чтобы система могла приспособиться к новой подсистеме, программные настройки и драйверы устройств нужно обновить. Если у вас все еще ничего не получается, отдохните, а потом на свежую голову продолжите работу, обозначив все текущие симптомы. Не бойтесь просить помощи — время от времени неудачи случаются даже у самых опытных специалистов по устранению неисправностей. Кроме того, вы должны понять, что, возможно, разбираться придется с несколькими проблемами. Помните, что сеть — это лишь некое количество систем, каждая из которых тоже состоит из некоторых компонентов. Обычно все они прекрасно работают друг с другом, но, когда одна система приходит в негодность, она может инициировать неисправности еще в одной или в нескольких взаимосвязанных системах.

Документируйте исправления

Документирование — это еще один важный прием, на который часто не обращают внимания. Выполнив успешное восстановление, вы должны выделить некоторое время на фиксацию своих находок и решений на бумаге. Для того чтобы эта привычка выработалась, нужны время и дисциплина, но она того стоит. Впоследствии, когда вам придется выполнять другие восстановительные действия, вы сможете обратиться к своим записям, и, быть может, благодаря этому вам не придется тратить битые часы на пробы и ошибки. Кроме того, заметки могут оказаться крайне ценными для других технических специалистов, столкнувшихся с теми самыми проблемами, которые вы уже научились разрешать.

Обеспечьте обратную связь

Обратная связь — это еще один важный этап, которым занятые администраторы и технические специалисты время от времени пренебрегают. Слишком часто после обращений за помощью пользователю предоставляется слишком мало информации (а иногда он остается в полном неведении). Во многих случаях в кратком сообщении пользователю просто советуется "попробовать еще раз". В других случаях проблема таинственно исчезает. Сообщать подробности предпринятых вами корректирующих действий, конечно же, необязательно, но крайне важно подтвердить получение запроса от пользователя, сообщить ему о том, что проблема устранена, и кратко объяснить пользователю причины ее возникновения. Ничего особенного

в этом нет, и если вы уложитесь в несколько предложений, этого, скорее всего, будет вполне достаточно.

Выявление изменений

Когда в сети появляется неисправность, один из первых вопросов, который вам предстоит решить, связан с изменениями — что именно изменилось с тех пор, когда сеть в последний раз работала в нормальном режиме? Изменения на компьютере происходят тогда, когда монтируется или обновляется аппаратное обеспечение, а также когда инсталлируются новые программы и когда конфигурация системы подвергается изменениям. К примеру, в результате установки на рабочей станции неверного драйвера сетевой платы это устройство может прекратить работать, таким образом, полностью лишив компьютер возможности обращения к сети. Для технического специалиста процесс поиска неисправностей часто начинается с поиска изменений, произошедших в рамках компьютера, системы кабелей, стеков протоколов, программного обеспечения или других сетевых устройств.

Спросите у пользователей

Даже те пользователи, которые действуют из лучших побуждений, могут оказаться злейшими врагами сети. Они часто стараются быстро залатать неисправность, и иногда вносят (несанкционированные) изменения в конфигурацию системы, которые приводят к появлению разного рода ошибок и к ухудшению производительности. В некоторых случаях эти проблемы способны воздействовать на функционирование всей сети. Предположим, что один из ваших пользователей установил новый браузер, потом решил отказаться от него, но забыл деинсталлировать, а на следующий день столкнулся с трудностями при обращении к внутренней сети компании. Если пользователь не расскажет вам о том, что он установил новый браузер, вы можете потратить несколько часов, пытаясь разобраться в том, что является источником проблемы. Когда проблемы выплывают на поверхность, обязательно спрашивайте у пользователей, не вносили ли они изменения в свои системы.

Примечание

Чтобы снизить частоту случайных изменений настроек, выполняемых конечными пользователями, вы должны активно препятствовать практике внесения изменений, подобных модернизации аппаратного или программного обеспечения. В каждой системе должна быть стандартная, хорошо документированная конфигурация, а исключительное право на проведение процедур сопровождения и обновления должно принадлежать уполномоченным техническим специалистам.

Проверяйте изменения, которые вносили сами

Являясь техническим специалистом, вы, вне всякого сомнения, время от времени будете вносить изменения в конфигурации систем (например, регулировать серверы и маршрутизаторы). Эти изменения могут обусловливаться необходимостью предоставления новых услуг или устранения неисправностей. К примеру, предположим, вы обнаружили, что загрузочный файл сервера IntraNetWare отказывается автоматически делать доступным один из томов, а решение этой проблемы кроется в редактировании загрузочного файла. На следующий день пользователи Windows NT начали

жаловаться на то, что часы в их системах отстают на пять часов. На первый взгляд, это проблема не кажется связанной с сервером, вполне возможно, что при редактировании серверного конфигурационного файла для обеспечения доступа к тому вы допустили погрешность. Вместо того чтобы ввести

```
SET TIME ZONE--EST5EDT
```

вы случайно отредактировали строку так, что она приняла следующую форму:

```
\SET TIME ZONE--EST5EDT
```

После сохранения отредактированного файла сервер неожиданно потерял всякое представление о том, в каком часовом поясе он расположен — он не смог интерпретировать неверную команду `\SET`.

Идея в том, что недавно выполненные изменения (даже в том случае, если они, как вам кажется, не имеют отношения к зафиксированному симптому) могут воздействовать на поведение сети. Опять же, это один из тех случаев, когда очень важна хорошая документация. Если вы сравните дату возникновения проблемы с датами изменений, указанными в журнале активности, возможные проблемные области могут сразу проясниться. Если свои обязанности в сети вы исполняете совместно с другими сотрудниками, убедитесь в том, что все ваши коллеги в полной мере документируют свои действия.

Примечание

Как правило, после внесения изменений в устройство его нужно перезагружать.

Внешнее влияние

Несмотря на то, что вы удерживаете контроль над своей внутренней локальной сетью или другой сетевой конфигурацией, работа многих сетей зависит от служб обмена информацией, предоставляемых местной телефонной компанией и поставщиком услуг Интернета (Internet Service Provider, ISP). Если внутренних изменений не зафиксировано, но службы обмена информацией работают не так, как ожидалось, имеет смысл позвонить ISP или в местную телефонную компанию — возможно, вы обнаружите, что один из внешних поставщиков услуг произвел некие изменения, которые оказали отрицательное воздействие на способность вашей сети к обмену информацией. Проблемы подобного рода часто дают о себе знать поутру в понедельник — дело в том, что большинство изменений производятся в выходные, когда уровень использования традиционно снижается.

Координируйте процедуры развертывания

В какой-то момент придет время модернизации сети путем установки в ней новой операционной системы или приложения — обычно эта процедура называется развертыванием обновления, и в условиях любой сети она предполагает внесение серьезных изменений. Проблема заключается в том, что новое программное обеспечение часто содержит ошибки. Немногие сетевые администраторы захотят проводить бета-тестирование нового продукта производителя программ, поэтому в таком случае разумно подождать около полугода, чтобы дать производителю возможность устранить дефекты своего нового продукта. Кроме того, за это время производитель мо-

жет сделать заплаты и получить первоначальный опыт поддержки новой версии (взгляните хотя бы на все пакеты обслуживания — Service Packs — для Windows NT и 2000).

Придя к выводу, что продукт обкатан, приступайте к развертыванию, но (по возможности) начинайте с небольших групп пользователей. Таким образом, вы сможете определить поведение обновления в относительно контролируемых условиях. Если обновление окажется стабильным и надежным, можно продолжать его поэтапную реализацию. Естественно, в случае появления серьезных проблем под их воздействие подпадет ограниченное количество пользователей (следовательно, при необходимости их работоспособность будет проще восстановить).

Разделяйте и властвуйте

Подобно персональным компьютерам, сети представляют собой комбинации аппаратных устройств и программных конфигураций. При возникновении проблемы выработке решения обычно способствует разделение проблемной области на более мелкие, более управляемые блоки. К примеру, предположим, что компьютер теряет возможность обращения к собственному жесткому диску. Возможно, проблема локализуется в самом жестком диске, в его контроллере, в кабеле, проведенном между диском и контроллером, или в стандартной программе CMOS Setup компьютера. Проверив варианты неисправности CMOS Setup и прокладки кабелей (проверить их проще всего) и исключив их, вы можете локализовать ошибку, заменив контроллер, а затем — жесткий диск. Этот принцип элементарно распространяется и на сеть в целом.

Предположим, в сети возникает неисправность. Принцип "разделяй и властвуй" помогает оперативно сузить область размещения неисправности со всей сети до отдельной рабочей станции или до другого устройства. Узнайте, затрагивает ли проблема одного человека (в таком случае она является локальной), или большую группу людей (в таком случае это системная проблема). Если обнаружится, что от данной неисправности лишения терпит только один человек, значит, принцип "разделяй и властвуй" в масштабах всей сети сделал свое дело, и теперь можно переходить к поиску неисправностей в рамках отдельной рабочей станции. При этом может возникнуть необходимость в дальнейшем применении принципа "разделяй и властвуй" на уровне ПК; с другой стороны, возможно, потребуется сразу заменить неисправную рабочую станцию. Если существующая неисправность влияет на работоспособность группы участников сети, приступайте к сбору дополнительной информации.

Обнаружив, какая функциональная группа пользователей находится под воздействием проблемы, и, исходя из этих данных, определите, какие области затронуты неисправностью. Определите местонахождение этих пользователей на ваших функциональных картах, и подумайте, что у них общего (и посредством чего они связаны). Вполне вероятно, что после этого ответ на вопрос о локализации неисправности станет до боли очевидным. Если плохо работают компьютеры в двух отделах, вероятно, неисправен сервер, который их обслуживает. Если на функциональной карте видно, что проблемы наблюдаются во всех группах, подключенных через определенный маршрутизатор, значит, пора проверить этот маршрутизатор. Если помощь требуется пользователям из определенного сегмента, скорее всего, проблема локализуется в этом физическом сетевом сегменте. В любом случае, идея заключается

в том, чтобы упростить задачу поиска неисправностей, сузив ее до возможной проблемной области. Если вы имеете дело с крупными сетями и с большим количеством пользователем, этот принцип становится еще более важным.

Программные решения

Подход "разделяй и властвуй", кроме прочего, применим к программному обеспечению и разрешению программных конфликтов. Когда на компьютере, без каких бы то ни было аппаратных причин, возникают проблемы с производительностью, многие технические специалисты проводят "чистку загрузки". Тем самым они добиваются уменьшения количества программ, загружаемых в память при загрузке системы, и устраняют все потенциально возможные конфликты между различными, не связанными друг с другом программами. Зачастую после этого выполняется восстановление программ — по одной за раз, что позволяет в конечном итоге выявить нарушителя. Этот ход действий применим и к сетям. К примеру, предположим, что у всех сотрудников в офисе начинаются проблемы с закрытием систем. Они все зависают на экране "Please wait while your computer shut down" (Пожалуйста, подождите, пока ваш компьютер выключится). В последнее время никто ничего не менял и не обновлял. На первый взгляд, эта проблема даже не кажется связанной с сетью. Если в офисе установлены системы Windows NT или 2000, многие программы, которые запускаются при загрузке систем, находятся в меню **Startup** (Автозагрузка). Вы избавляетесь ото всех элементов этого меню, перезагружаетесь, и вдруг обнаруживаете, что снова можете беспрепятственно выключать систему. Затем вы вновь, одну за другой, помещаете программы в каталог Startup и продолжаете перезагружаться, пока не выявите источник проблемы.

Предположим, что виновником оказалась программа почтового оповещения, однако в случае запуска исключительно этой программы отключение системы происходит в нормальном режиме. Следовательно, налицо конфликт между двумя программами. К счастью, методика "разделяй и властвуй" работает и здесь — вы можете по очереди проверить все сочетания подозрительной программы с каждой из оставшихся программ, пока не найдете другую программу, выступающую в качестве второго источника конфликта. К примеру, предположим, что трудности начинаются в случае совместной работы программы почтового оповещения и сервисной служебной антивирусной программы. Если эти две программы совместно работали в сети и ранее, дальнейший анализ может привести к выявлению факта автоматического интернет-обновления антивирусной утилиты, из чего вы сделаете вывод о том, что проблема сформирована именно этим обновлением. На самом деле, в результате непродолжительного поиска по Web-сайтам производителей вы, вероятно, найдете заплату для почтового клиента (или для антивирусной программы), и проблема, наконец, будет решена.

Проводите сравнения

Другим распространенным методом поиска неисправностей в персональных компьютерах и сетях является сравнение рабочих характеристик неисправного устройства с аналогичными характеристиками двух или нескольких идентичных устройств, работающих без ошибок. К примеру, если вам не удается заставить какой-то принтер работать через параллельный порт, но вы знаете, что через тот же самый параллель-

ный порт работает другой принтер, получается, что проблема локализуется не в параллельном порту или кабеле, а в рамках первого принтера. Тот же принцип применим к неправильно функционирующим сетевым устройствам. Если вы сможете найти идентичный работающий элемент, вполне возможно, что устранить возникшую неисправность удастся путем приведения конфигурации проблемного устройства в соответствие конфигурации работающего устройства; по меньшей мере, вы сможете предположить, что неверно функционирующее устройство вышло из строя и нуждается в замене. Аналогичный процесс подходит и к программному обеспечению (примером может быть сравнение сценариев регистрации или версий файлов); его часто называют "методом исключения".

Имейте в виду, что методика сравнения устройств прекрасно работает на низком уровне (например, в отношении концентраторов), но становится несколько более проблематичной в отношении важнейших сетевых устройств, подобных серверам и маршрутизаторам. Проблема заключается в том, что в рамках сети устройств уровня серверов или маршрутизаторов часто оказывается слишком мало, но даже когда их несколько, они редко бывают идентичными — таким образом, сравнения проводить сложно.

Кого звать на помощь

Вне зависимости от того, насколько вы опытны, нельзя исключать случай, что в конечном итоге вы встретитесь с проблемами, которые не сможете решить в данных временных условиях имеющимися инструментальными средствами и другими ресурсами. В подобной ситуации ничто не мешает вам обратиться к обширнейшей информации и опыту, накопленному различными производителями продуктов, посетителями дискуссионных форумов и независимыми организациями, занимающимися поддержкой и обладающими громадными знаниями в области организации сетей (значительная часть такой информации распространяется бесплатно). Ознакомление с чужой точкой зрения часто помогает собрать наблюдения или факты, на которые вы не обратили внимания. С другой стороны, если вы решите объяснить признаки возникшей неисправности кому-то другому, вам, возможно, придется схематически изобразить динамику проблемы, указать на важные вопросы и обсудить подходы, которые раньше вы проигнорировали.

Пользуйтесь данными, опубликованными на Web-сайтах производителей (в особенности это касается сайтов поддержки). На хороших сайтах поддержки обычно присутствует сетевая документация, руководства пользователя и руководства по установке, списки наиболее часто задаваемых вопросов, перечни замеченных трудностей и проблем, связанных с совместимостью с другими устройствами или программным обеспечением. Кроме того, в большинстве случаев на таких сайтах вы сможете найти обновленные драйверы устройств, заплаты, диагностические утилиты и другие обновления, способные разрешить проблемы, возникшие в вашей сети. Если ничего не получается, позвоните производителю. Возможно, звонок окажется платным (плата может взиматься за минуту или за неисправность), но в случаях, когда простой сети связан с потерей реальных денег, стоимость телефонной службы поддержки зачастую оказывается приемлемой.

Общедоступные форумы и новостные группы часто оказываются прекрасными источниками реального опыта работы с продуктами различных производителей (впрочем, прежде чем найти полезную информацию, вам, вероятно, придется стерпеть

огромное количество пустого трепа). Найти подходящие новостные группы не составляет труда, если для этого воспользоваться поисковой системой наподобие Google (**http://groups.google.com/**). Производители, предоставляющие комплексную техническую поддержку, содержат на своих Web-сайтах динамические форумы — они, вероятно, окажутся особенно полезными, т. к. сотрудники отдела технической поддержки компании-производителя проводят их текущий контроль.

Основы поиска неисправностей

Сколько ни читай о поиске неисправностей, а все равно, раз за разом возникает вопрос: "с чего начать?" Успешный поиск и устранение неисправности требует, чтобы локализация проблемы была выполнена как можно быстрее. Определив, в чем именно заключается проблема, вы можете предпринять меры по ее устранению — в противном случае вы будете убиты скверным настроением, потеряете много времени и сил. Эта часть настоящей главы представляет собой своеобразное практическое руководство начинающего специалиста по устранению неисправностей, прочитав которое, вы, вероятно, сможете локализовывать проблемы более оперативно.

Начало

Процесс поиска неисправности лучше всего начинать с количественного анализа — это поможет разобраться в ее сущности. Вероятно, сразу выявить причину возникновения проблемы не удастся, но понимание того, что и где происходит, поможет вам своими силами воспроизвести неисправность и определиться с тем, что нужно предпринять впоследствии. В большинстве случаев ознакомление с проблемой происходит при участии пользователей (вероятно, с ними придется говорить по телефону, или они придут к вам сами). К примеру, вполне возможно, что напуганный пользователь сообщит вам о том, что, придя на работу в 7:30 утра, ему не удалось зарегистрироваться на сервере. Помимо всего прочего, в такой ситуации вам представляется возможность получить довольно подробные данные о конкретных условиях, окружающих пользователя, его учетной записи и аппаратном обеспечении. Кроме того, для того чтобы ознакомиться с местной проводкой кабелей, узнать о наличии концентраторов/коммутаторов и смежных рабочих станций, следует обратиться к любым логическим или физическим картам сети (рис. 29.2).

Проблемы отдельного компьютера

Если неисправность поражает отдельно взятую рабочую станцию, в то время как рабочие станции, серверы и другие ресурсы функционируют в нормальном режиме, вполне возможно, что сбой локализован в данной рабочей станции, ближайших к ней элементах подключения к сети или в конфигурации ее программного обеспечения. В случае, когда неисправность наблюдается только на одном персональном компьютере, необходимо выполнить следующие действия.

- *Проверьте питание.* Возможно, это покажется слишком очевидным, но вы удивитесь, узнав, какое количество пользователей приходят на работу, предполагая, что их компьютеры включены — они даже не представляют, что их могли выключить. Если пользователь говорит, что система отключена или не желает

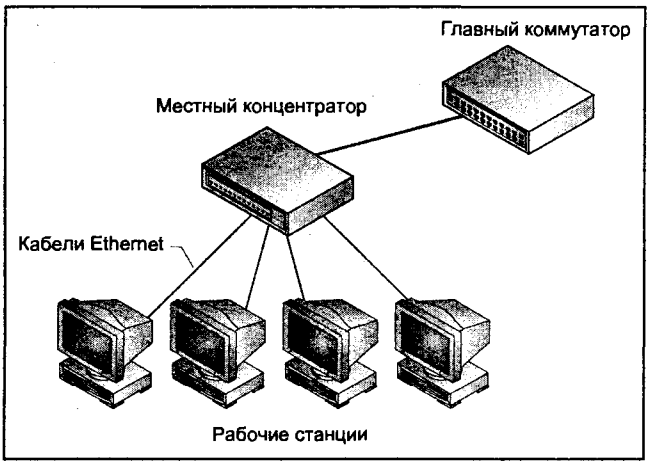


Рис. 29.2. Часть карты иерархической звездообразной сети с указанием нескольких рабочих станций

включаться, в первую очередь проверьте, подключены ли компьютер и монитор к источнику питания, и находятся ли они во включенном состоянии. Если система включена, но не может выйти из режима ожидания, попробуйте перезагрузить ее. Корректному восстановлению после нахождения в энергосберегающих режимах зачастую препятствует несовместимое аппаратное обеспечение и устаревшие драйверы. Если система включена, но ей не удается загрузиться, вам придется заменить компьютер, чтобы пользователь смог возобновить работу, а затем, находясь на своем рабочем месте, починить неисправную систему.

- *Проведите проверку на предмет вирусов.* Это стандартный этап поиска неисправностей — его необходимо проводить всякий раз при возникновении сетевых проблем. Для того чтобы проверить, насколько чист неисправный компьютер (и не воспроизводит ли он инфицированные файлы или макросы по всей сети), запустите недавно обновленную антивирусную программу. В случае обнаружения на станции вируса обязательно выполните комплексную процедуру поиска вирусов в масштабах всей сети. Более подробно тема вирусов изложена в *гл. 19.*

- *Проверьте соединение.* Взгляните на кабель, проложенный между рабочей станцией и соответствующим портом концентратора/коммутатора (возможно, для того чтобы получить данные об этом соединении, вам придется обратиться к физической карте). Проверьте, горит ли светодиод линии. Если он не работает, значит, кабель отсоединен или поврежден, и для восстановления нормального соединения, вам, вероятно, придется чинить кабельную проводку. За дополнительной информацией о кабелях обращайтесь к *гл. 8.*

- *Проверьте учетную запись.* Трудности, возникающие при попытках регистрации в сети (особенно в отдельные дни и часы), могут свидетельствовать о том, что проблема заключается в учетной записи. Возможно, ограничены часы регистрации, или в результате превышения лимита ошибок при регистрации заблокирована учетная запись (быть может, кто-то пытался выполнить несанкционированную регистрацию). Убедитесь в правильности настроек учетной записи и про-

верьте журналы безопасности сервера на предмет подозрительной активности. Кроме того, вы можете попросить пользователя попытаться зарегистрироваться с другой рабочей станции, располагающей необходимыми для этого полномочиями. Подробное изложение процедур поиска неисправностей при регистрации представлено в *гл. 26.*

- *Отправьте на станцию Ping-запрос.* Для тестирования IP-адреса проблемной станции нужно пользоваться утилитами, подобными Ping. Если станция не сможет ответить, значит, существует неисправность кабеля, порта концентратора/коммутатора, или сетевой платы, и именно в этом направлении вам предстоит копать. Если станция отвечает на Ping-запрос (и, более того, сама может отправить такие запросы другим станциям), но во всех прочих отношениях ее поведение в сети оказывается некорректным, вполне возможно, что соединение и оборудование сетевой платы работают в нормальном режиме, а проблема исходит от программного обеспечения. Еще раз проверьте настройки системы (настройки DNS, WINS, файлы autoexec.bat, Hosts и config.sys; убедитесь в отсутствии ошибок в реестре Windows), и исправьте все недочеты. Далее в этой главе мы еще поговорим о Ping.
- *Проверьте порт концентратора/коммутатора.* Если станция подключена к "управляемому" концентратору или коммутатору, вполне возможно, что ее порт отключен. Откройте служебную программу управления и проверьте состояние соответствующего данной станции порта. Если порт отключен, попытайтесь включить его. Если попытки повторного включения порта ни к чему не приведут (а также, если порт будет обозначаться как неисправный или недоступный), попытайтесь подключить рабочую станцию к другому незанятому порту (с другой стороны, вы можете полностью заменить концентратор/коммутатор). Если концентратор/коммутатор не является "управляемым", то, для того чтобы проверить исправность порта, имеет смысл перезагрузить концентратор/коммутатор или попробовать подключить рабочую станцию к другому свободному порту.

Проблемы в сегменте

Предположим, что проблема затрагивает несколько сетевых станций. Логика диктует, что проблема является общей для всех этих станций. В большинстве подобных случаев причина заключается в неисправности кабеля или концентратора/коммутатора. Для примера рассмотрим четыре станции, находящиеся в одной части офиса и подключенные к одному концентратору, который, в свою очередь, подсоединен к коммутатору, обеспечивающему работу сервера и прочих небольших групп, подключенных к локальным концентраторам по всему офису (подобная схема приводилась на рис. 29.2).

- *Проверьте питание локального концентратора.* Убедитесь в том, что небольшой концентратор, к которому подключены все четыре удаленных рабочих станции, получает питание. Можете попытаться перезагрузить этот концентратор, отключив питание на несколько секунд, а затем, возобновив его и предоставив концентратору возможность провести самотестирование. Кроме того, проверьте, светятся ли светодиоды линий, соответствующих каждой рабочей станции, подключенной к локальному концентратору. Если эти светодиоды не работают, вполне возможно, что локальный концентратор неисправен и нуждается в замене.

- *Проверьте активность и наличие конфликтов.* Необычно высокие уровни активности и избыточные конфликты способны оказать негативное воздействие на станции, расположенные в рамках отдельного сегмента. Взгляните на светодиоды активности и конфликтов, соответствующие всем затронутым рабочим станциям. Возможно, что станция Ethernet с необычно высоким уровнем активности приводит к возникновению чрезмерного количества конфликтов. Если умышленные операции передачи со станции-нарушителя не проводятся, значит, возможно, ее сетевая плата передает сбойные пакеты и требует замены. Обоснованный трафик, приводящий к возникновению избыточного количества конфликтов, возможно, свидетельствует о необходимости обеспечения более серьезной пропускной способности (например, обновления 10BaseT до 100BaseT) или своего перемещения в другой сегмент (т. е. подключения сильно занятой станции к какому-то другому концентратору).
- *Проверьте магистральный кабель.* Взгляните на кабель, проложенный между локальным портом и соответствующим ему портом коммутатора (возможно, для того, чтобы получить данные об этом соединении, вам придется обратиться к физической карте). Проверьте, светится ли светодиод канала. Если он не функционирует, значит, кабель отсоединен или поврежден — вероятно, для восстановления нормального соединения вам придется чинить кабель. Более подробная информация о кабелях представлена в *гл. 8.*
- *Отправьте Ping-запросы на локальные станции.* Пользуясь утилитой Ping, проверьте возможность передачи данных между локальными станциями. Если отправка Ping-запроса с одной локальной станции на другую не приведет к успеху, значит, концентратор неисправен и требует замены.
- *Отправьте Ping-запросы на удаленные станции.* Если локальные станции сохраняют возможность взаимной отправки Ping-запросов через концентратор, попробуйте отправить Ping-запросы на коммутатор, сервер или другие станции, являющиеся внешними по отношению к коммутатору. Если отправка Ping-запросов с любой локальной станции через коммутатор не приведет к успеху, значит, коммутатор, возможно, неисправен и требует замены. Попробуйте подключиться к другому свободному порту коммутатора. Если коммутатор является "управляемым", откройте служебную программу управления, проверьте состояние рассматриваемого порта, и, если представится такая возможность, попробуйте разблокировать его. В противном случае замените коммутатор.

Проблемы масштаба всей сети

Наиболее обременительные и серьезные типы неисправностей распространяются на всю сеть. К примеру, может сложиться ситуация, при которой ни один из пользователей не сможет зарегистрироваться на сервере домена, подключиться к сети Интернет или воспользоваться сетевым принтером. На первый взгляд, проблемы подобного рода производят впечатление крайне сложных, требующих наличия высокопрофессионального оборудования и многих лет опыта работы специалиста; как бы то ни было, самым эффективным вашим оружием является знание схемы сети и понимание причинно-следственных связей — где общая нить, а что к ней не имеет отношения.

К примеру, предположим, что на сервере домена Windows 2000 не может зарегистрироваться только один пользователь, а все остальные не сталкиваются с трудностя-

ми. Если проблема распространяется на отдельно взятую станцию, естественная логика подсказывает, что все внимание нужно обратить именно на эту станцию (начиная с качества сетевого соединения и корректности настройки учетной записи). С другой стороны, предположим, что зарегистрироваться на сервере домена не удается всем пользователям. Определить, что все эти станции сохраняют способность к передаче информации (к примеру, они обеспечивают коллективный доступ к файлам и каталогам на других серверах или персональных компьютерах), не составляет сложности. В таком случае общей нитью является сам сервер домена. Возможно, он отключен или неверно настроен; не исключено присутствие некоей аппаратной неисправности, требующей конфигурации или починки.

В качестве другого примера предположим, что ни одному из всех присутствующих пользователей не удается подключиться к сети Интернет с помощью простого маршрутизатора. Так как интернет-маршрутизатор и модуль обслуживания канала и данных CSU/DSU (например, кабельный модем или какой-то другой ресурс обмена данными) являются общими для всех вариантов доступа к Интернету, имеет смысл начать с анализа именно этих устройств. Возможно, вы обнаружите, что маршрутизатор или аппаратура модуля обслуживания канала и данных находится в выключенном или отсоединенном состоянии. После нескольких непродолжительных Ping-запросов выясняется, что маршрутизатор отвечает, но на модуле CSU/DSU не горит светодиод активности. Вероятно, в данном случае необходимо перезагрузить CSU/DSU (а может быть, и маршрутизатор) или вызвать представителя сервисной службы с целью проверки целесообразности замены CSU/DSU. В других случаях может обнаружиться, что активность присутствует, но маршрутизатор настроен некорректно.

Из всего вышесказанного можно сделать следующий вывод: в процессе устранения сетевых неисправностей здравый смысл имеет большое значение. Располагая необходимой документацией и элементарными познаниями в сфере организации сетей, технический специалист обычно может сузить область размещения большинства проблем до отдельной рабочей станции/сервера, кабеля, концентратора/коммутатора или другого сетевого устройства, причем сделать это за несколько минут при помощи минимального количества сложного испытательного оборудования, или вообще без него. Естественно, для того чтобы найти и исправить конкретную неисправность (например, обнаружить место разрыва кабеля или настроить стек TCP/IP), потребуются дополнительные усилия, но в любом случае сделать проблему решаемой — в ваших силах.

Инструментальные средства поиска неисправностей

Принципы поиска неисправностей и инструкции по их устранению, которые вы почерпнули из данной главы к настоящему моменту, представляют собой основу для выполнения процедур устранения неисправности. К счастью, поиск неисправностей — это не просто систематическая локализация; существует множество диагностических инструментальных средств, с помощью которых вы можете выявить проблемы, связанные с сетевыми операциями и производительностью. Многочисленные средства подобного рода достаются вам вместе с операционной системой, причем совершенно бесплатно. В этой части главы мы рассмотрим ассортимент ин-

струментальных средств, применяемых для подкрепления ваших усилий по поиску неисправностей.

Системные журналы

Серверы ведут несколько различных системных журналов, которые можно задействовать для отслеживания ошибок и других важных рабочих условий. В журналах обычно содержится непрерывный перечень всех ошибок и предупреждений, дата и время каждого события, а также другие существенные данные — например, имя причастного пользователя или процесса. В случае возникновения проблемы журнал может в точности сообщить вам, что и когда произошло, и какой пользователь имеет к этому отношение (если таковые имеются). Технический специалист должен знать, как обращаться к системным журналам операционных систем, подобных NetWare 5, Linux/UNIX и Windows NT/2000.

Примечание

Системные журналы — это не только важные диагностические средства; они могут быть задействованы в качестве допустимого доказательства по иску о несанкционированном вторжении или других злонамеренных деяниях.

Журналы NetWare

Novell NetWare 5.x ведет 3 системных журнала, способных предоставить помощь в диагностике неисправностей на сервере NetWare.

- *Файл console.log.* Консольный журнал регистрации (console.log) содержит архив данных по всем ошибкам и данным, выведенным на консоль сервера. Эти данные находятся в каталоге sys:\etc сервера; они создаются и сопровождаются утилитой conlog.nlm, входящей в состав операционных систем NetWare, начиная с версии 3.12. Эту утилиту необходимо загружать вручную путем введения команды `load conlog` в командной строке консоли (или размещать загрузочную команду в файле autoexec.ncf таким образом, чтобы утилита исполнялась автоматически при запуске сервера). Сразу после своей загрузки эта утилита стирает старый файл console.log и начинает регистрировать события в новом файле. Для примера, в этом журнале может присутствовать запись, обозначающая, что кто-то отредактировал файл autoexec.ncf, а затем перезагрузил сервер, что свидетельствует о серьезном изменении, произошедшем на сервере. Если бы нам пришлось искать неисправность на сервере, трудности на котором появились после недавней перезагрузки, мы заглянули бы именно сюда.
- *Файл abend.log.* Аварийное завершение (Abend — сокращение от ABnormal END) — это ситуация возникновения ошибки, которая останавливает нормальную работу сервера NetWare; в этом системном журнале регистрируются все аварийные завершения, произошедшие на сервере NetWare. Степень серьезности аварийных завершений может быть разной — не исключается блокировка сервера, но, с другой стороны, все может обойтись закрытием модуля загрузки NetWare (NLM). О том, что произошло аварийное завершение, вы можете узнать по появляющемуся на консоли сообщению об ошибке, в тексте которого содержится слово "abend". В дополнение к этому, в командной строке сервера появляется число,

заключенное в угловые скобки (например, <1>), обозначающее количество аварийных завершений сервера с момента его подключения к сети. В операционных системах NetWare, начиная с версии 4.11, есть подпрограмма, выполняющая захват выходных данных аварийного завершения на консоль и в файл abend.log (расположенный в каталоге сервера sys:system). К примеру, слова "Page Fault" ("Ошибка страницы") или "Stack" ("Стек") в этом файле регистрации могут указывать на то, что аварийное завершение произошло из-за чего-то, связанного с памятью — программа или процесс пытался занять память, которая ему не принадлежала. Когда система NetWare обнаруживает это обстоятельство, процесс-нарушитель закрывается; одновременно система выдает аварийное завершение.

- *Файл sys$log.err.* Общий серверный системный журнал (Server Log), расположенный в каталоге SYS:SYSTEM, содержит записи всех произошедших на сервере ошибок, включая аварийные завершения и ошибки NDS, а также время и дату их появления. Запись ошибки в файле sys$log.err выглядит примерно так:

```
1-07-2002 11:51:10 am: DS-7.9-17
Severity = 1 Locus = 17 Class = 19
Directory Services: Could not open local database, error: — 723
```

Серьезность проблемы выражается параметром строгости (`Severity`). Местоположение (`Locus`) указывает на то, какой компонент системы подвергся воздействию ошибки (к примеру, память, диск или сетевые платы). Класс (`Class`) обозначает тип ошибки. Сами цифры, выражающие значения строгости, местоположения и класса, могут оказаться непонятными, так что за перечнем кодов вам следует обращаться к документации по NetWare. Что касается примера, приведенного выше, `Severity = 1` обозначает предупреждение (следовательно, проблема не является серьезной), `Locus = 17` указывает на то, что ошибка относится к операционной системе (что имеет смысл, т. к. это ошибка службы каталогов), а `Class = 19` выражает связь проблемы с доменом. Таким образом, проблема определена операционной системой, но локализуется не в операционной системе.

Системные журналы Windows

В Windows NT/2000 предусмотрен обширный комплект журналов регистрации ошибок и информационных журналов. Вместо отдельных журналов для каждой программы или процесса, в продуктах компании Microsoft используется утилита Event Viewer (Просмотр событий) — она отслеживает все заметные события, происходящие на отдельно взятом компьютере Windows NT/2000. Вы должны уметь обращаться к Event Viewer и открывать все основные журналы регистрации, присутствующие в операционных системах Windows. Чтобы запустить служебную программу Event Viewer в среде Windows NT, выполните следующие действия:

1. Выберите последовательно **Start**, **Programs**, **Administrative Tools** (Пуск, Программы, Администрирование). В результате откроется диалоговое окно **Select Computer** (Выбор компьютера).
2. Введите имя компьютера, журналы регистрации событий которого вы намерены просмотреть (или двойным щелчком выберите имя этого компьютера в списке доступных систем), и нажмите кнопку **OK**.

Примечание

Если ваше соединение производится по медленному каналу, например, с помощью модема коммутируемой линии, сначала установите флажок **Low Speed Connection**, и только после этого нажимайте кнопку **OK**.

3. Чтобы просмотреть содержимое определенного файла регистрации, выберите его из представленного списка. Если вы намереваетесь просмотреть журнал, относящийся к другому компьютеру, выберите в меню **Log** команду **Select Computer**.

Для того чтобы запустить Event Viewer в операционной системе Windows 2000, выполните следующие действия:

1. Выберите последовательно **Start**, **Programs**, **Administrative Tools**, **Computer Management** (Пуск, Программы, Администрирование, Управление компьютером).
2. Разверните элемент **System Tools** (Служебные программы) и записи в **Event Viewer** (Просмотр событий) для просмотра перечня доступных журналов регистрации.
3. Чтобы ознакомиться с содержимым конкретного журнала регистрации, выберите его имя.

Типы журналов регистрации

В Windows NT/2000 существует три основных типа журналов регистрации: журналы приложений, системные журналы и журналы безопасности. Журнал приложений содержит события, зафиксированные приложениями или программами. К примеру,

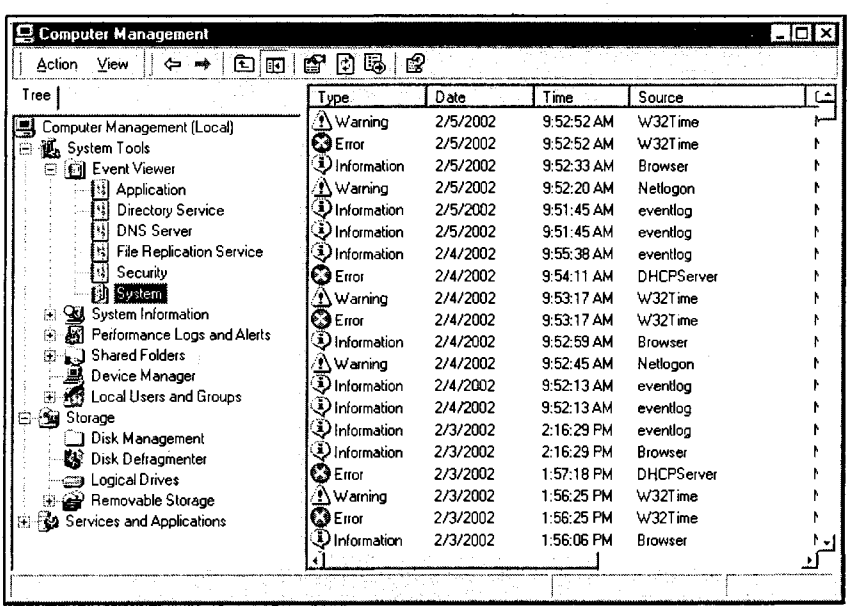


Рис. 29.3. В системном журнале могут содержаться важные сведения о событиях, приводящих к проблемам производительности системы или стабильности ее работы

может оказаться, что в журнале приложений ошибку файла зарегистрирует программа работы с базами данных. Как правило, решение, касающееся того, какие события нужно регистрировать, принимается разработчиком программы. Скажем, этот журнал может существенно помочь администраторам и техническим специалистам, если пользователи сообщат о трудностях с работой таких служб, как SQL Server. Системный журнал содержит данные о событиях, зафиксированных компонентами системы Windows NT/2000 (рис. 29.3). К примеру, невозможность загрузки драйвера или другого компонента во время запуска системы регистрируется именно в системном журнале (типы событий, регистрируемых компонентами системы, предопределены в Windows). Наконец, журнал безопасности (как вы увидели в *гл. 26*) способен фиксировать события, связанные с системой безопасности, например правомерные или неправомерные попытки регистрации, а также события, связанные с применением ресурсов, например операции создания, открытия и удаления файлов. Решение о том, какие события необходимо фиксировать в журнале безопасности, принимает администратор. К примеру, если вы включили функцию аудита регистрации, то попытки регистрации в системе заносятся в журнал безопасности.

Примечание

Запись в журналы регистрации необходимо разрешить — это делается в служебной программе Event Viewer.

Типы событий

Служебная программа Event Viewer отображает пять различных типов событий. Вы должны понимать значение и относительную важность каждого из этих событий, чтобы иметь возможность расставлять приоритеты для корректирующих действий.

- *Ошибка.* Обозначает существенный сбой в системе — например, потерю данных или функциональности. К примеру, ошибка регистрируется в том случае, если во время запуска системы не удается загрузить какую-либо службу. Ошибки могут требовать немедленного внимания и внесения исправлений.
- *Предупреждение.* Обозначает событие, которое, являясь не слишком значительным само по себе, может свидетельствовать о возможном возникновении проблемы в будущем. К примеру, предупреждение выводится в случае недостатка свободного дискового пространства. Предупреждения не требуют немедленного внимания, но должны удостаиваться проверки и конкретных действий в разумные сроки.
- *Информационное событие.* Такое событие описывает успешную работу приложения, драйвера или службы. К примеру, информационное событие регистрируется в случае успешной загрузки драйвера. Большинство информационных событий не требуют никаких ответных действий, но могут сообщать о неожиданных (или нежелательных) состояниях.
- *Проверка успешного действия.* В событии этого типа сообщается о "проверенной" попытке обращения к системе защиты, которая увенчивается успехом. К примеру, успешная попытка регистрации пользователя в системе регистрируется в качестве события проверки успешного действия.
- *Проверка неуспешного действия.* В событии этого типа сообщается о "проверенной" попытке обращения к системе защиты, которая завершилась неудачей.

К примеру, когда пользователь пытается получить доступ к сетевому диску, но не достигает успеха, эта попытка регистрируется в качестве события проверки неуспешного действия.

Примечание

При запуске Windows регистрация событий начинается автоматически. Журналы приложений и системные журналы могут просматривать все пользователи, но к журналам безопасности обращаться могут только администраторы.

Ping

Отправитель пакетов Интернета (Packet Internet Groper, Ping) — это типичное средство поиска неисправностей в линиях связи между устройствами локальной и глобальной (Интернет) сети. Ping работает в сети TCP/IP, отсылая эхо-сообщения протокола управляющих сообщений в сети Интернет (ICMP) на узел назначения. Если сеть и все ее элементы настроены корректно, узел назначения получает эхо-сообщения ICMP (ICMP Echo), и на каждое из них реагирует отсылкой сообщения эхо-ответа (ICMP Echo Response). Кроме того, в сообщении эхо-ответа отражаются все данные, представленные отправителем исходящего эхо-сообщения — при выполнении каждой операции Ping в сообщение обычно включаются 32, 56 или 64 байт данных. Если узел, породивший Ping-запрос, получает ответы в течение предопределенного периода времени, соединение признается нормальным — это значит, что все устройства IP-сети между конечным узлом и станцией, отправлявшей запросы Ping, настроены оптимально для передачи IP-трафика. Ping является компонентом всех ядер TCP/IP, включая IP-настроенные рабочие станции (например, Windows 9x/ME/2000/XP), сервер Windows NT/2000, серверы Linux и NetWare. Утилита Ping предоставляет следующий набор данных.

- Ping помещает в каждый пересылаемый пакет уникальный порядковый номер и сообщает о порядковых номерах, которые получает обратно. Таким образом, у вас есть возможность определить, не были ли пакеты выброшены, сдублированы или переупорядочены.
- Ping проверяет (вычисляет контрольные суммы) каждый пакет, которым обменивается, так что вы можете выявить некоторые разновидности поврежденных пакетов.
- Ping устанавливает в каждый пакет временную метку, которая впоследствии возвращается и может быть легко задействована при подсчете времени, ушедшего на обмен каждым пакетом, т. е. периода кругового обращения (Round Trip Time, RTT).
- Ping сообщает о других сообщениях ICMP, которые в противном случае оказались бы преданными забвению в системном программном обеспечении. К примеру, если один из маршрутизаторов объявляет о недостижимости хоста назначения, Ping сообщает об этом.

Впрочем, и у Ping есть свои ограничения, и среди тех немногих данных, которые эта утилита сообщить не сможет, есть следующие.

- Некоторые маршрутизаторы отбрасывают недоставленные пакеты, другие полагают, что пакет успешно передан, хотя это отнюдь не так. Таким образом, Ping не всегда сообщает о причинах, по которым пакеты остаются без ответов.

- Ping не знает, почему пакет был поврежден, сдублирован, а его передача — задержана. Кроме того, она не говорит, где это произошло, хотя вы, вероятно, сами сможете это вычислить.
- Ping не умеет представлять подробный анализ каждого хоста, обрабатывающего пакет.

Применение Ping

Для запуска утилиты Ping, задания опций и IP-адреса назначения применяется командная строка. В своей простейшей форме Ping представляется вместе с IP-адресом назначения (и опциями по умолчанию), например, так:

```
>ping 192.168.1.1
```

При помощи этой команды вы можете отправить Ping-запрос, скажем, на интернет-маршрутизатор. Существует несколько вариантов ответа Ping (рис. 29.4), обозначающих количество отправленных байт и период кругового обращения. Когда тестирование будет завершено, Ping выведет на экран статистику, в том числе объем потерянных данных (если они вообще были потеряны), а также минимальное, максимальное и среднее значения времени. Скорость реакции в условиях корректно настроенной сети должна приближаться к 100 процентам в отношении всех отправленных Ping-пакетов. Значение ниже 90 процентов может свидетельствовать о наличии таких проблем, как высокий уровень перегрузки сети или чрезмерное количество транзитов (маршрутизаторов) между отправителем Ping и адресом назначения.

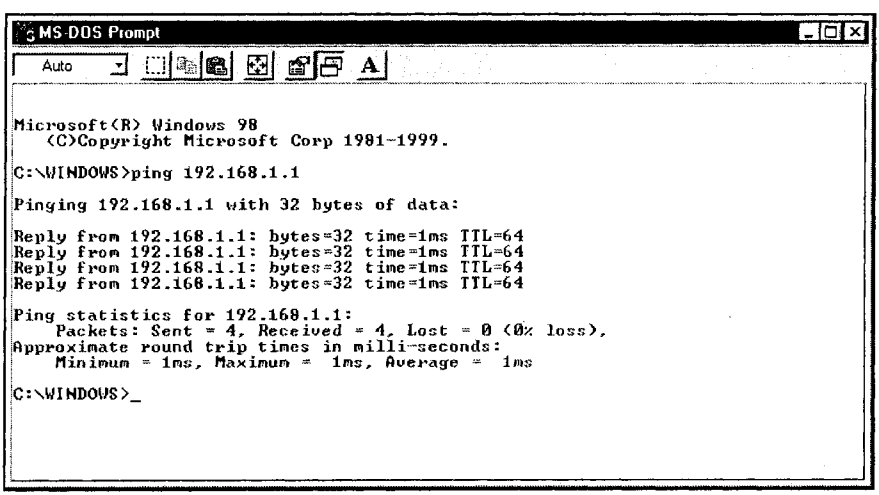


Рис. 29.4. Типичное отображение результатов работы утилиты Ping содержит временные характеристики соединения и все потери данных между двумя станциями сети

Впрочем, детали синтаксиса Ping зависят от конкретной операционной системы. Точный синтаксис для Linux выглядит следующим образом:

```
ping [-R] [-c число] [-d] [-I секунды] хост
```

Расшифровка опций представлена ниже.

- `-R`. Эта опция фиксирует маршрут, предпринятый пакетом.
- `-c`. Количество отправленных эхо-запросов ICMP.
- `-d`. Эта опция заставляет Ping отправлять пакеты настолько часто, насколько их может возвращать система назначения (до 100 раз в секунду). Результатом ее применения может быть серьезная интенсификация сетевого трафика.
- `-I`. Эта опция указывает количество секунд между пакетами. По умолчанию принимается временной промежуток, равный 1 секунде.
- `хост`. Это имя хоста назначения или его IP-адрес.

В системе Red Hat Linux 7.x принят несколько отличный синтаксис:

```
ping [-LRUbdfnqrvV] [-c подсчет] [-i интервал] [-w ожидание] [-p модель]
[-s размер_пакета] [-t время_жизни] [-I адрес_интерфейса]
[ -T опция_отметки_времени] [ -Q тип_обслуживания ] хост
```

В BSD/OS 4.x применяется следующий синтаксис:

```
ping [-dfnqRrv] [-a семейство] [-S запрос_безопасности] [-c подсчет]
[-i ожидание] [-l предварительная_загрузка] [-p модель] [-s размер_пакета]
хост
```

Синтаксис, принятый в операционных системах Windows, значительно отличается от вышеприведенных:

```
ping [-t] [-a] [-n подсчет] [-l размер] [-f] [-i время_жизни]
[-v тип_обслуживания] [-r подсчет] [-s подсчет] [[-j перечень_хостов] |
[-k перечень_хостов]] [-w лимит_времени] список_адресатов
```

Расшифровка опций представлена ниже.

- `-t`. Отправка Ping-запросов продолжается вплоть до ее явной остановки, которая производится нажатием сочетания клавиш <Ctrl>+<C>. Статистические данные выводятся на экран после остановки команды.
- `-a`. Эта опция осуществляет разрешение адресов в имена хостов.
- `-n подсчет`. Эта опция определяет количество пакетов ICMP с эхо-запросами, предназначенных для отправки.
- `-l размер`. Эта опция устанавливает объем буфера.
- `-f`. Устанавливает в пакете флаг "без фрагментации". Оказывается особенно полезной, если перед вами стоит задача узнать — не меняет ли устройство размер пакетов при их передаче между узлами.
- `-i время_жизни`. Устанавливает в пакетах значение "времени жизни" (Time to Live, TTL).
- `-v тип_обслуживания`. Устанавливает "тип обслуживания" (Type of Service, TOS).
- `-r подсчет`. Эта опция отображает маршрут по установленным транзитам.
- `-s подсчет`. Отображает временные метки всех транзитов.
- `-j перечень_хостов`. Свободная маршрутизация через узлы, заданные в перечне хостов.

- `-k перечень_хостов`. Строгая маршрутизация через перечисленные хосты.
- `-w лимит_времени`. Устанавливает значение лимита времени ожидания каждого ответа (в миллисекундах).
- `список_адресатов`. Это хост назначения или IP-адрес

Чтобы запустить Ping из командной строки консоли NetWare, введите следующую команду:

```
load ping ip_address
```

В среде NetWare параметр `ip_address` является необязательным — адрес, на который нужно отправить Ping-запрос, можно указать как в виде параметра, так и вручную в самой утилите. При использовании настроенного на разрешение имен DNS продукта NetWare 4.x, такого как NetWare NFS или Novell UNIX and Print Services, вместо IP-адреса назначения вы можете вводить имя хоста в системе DNS. Если утилита Ping загружается без параметров, появляется экран **New Target** (новый пункт назначения). Он позволяет ввести IP-адрес или хостовое имя DNS того узла, на который вы намереваетесь отправить Ping-запрос. Кроме того, вы можете указать количество секунд между Ping-запросами и размер IP-пакета (в байтах), хотя в большинстве случаев оптимальными оказываются настройки, принимаемые по умолчанию — одна секунда между Ping-запросами и 40-байтовый IP-пакет. Чтобы приступить к отправке Ping-запросов, нажмите клавишу <Esc>. На экран **Ping** в NetWare выводится следующая статистика для каждого хоста, на который вы отправляете Ping-запросы.

- **Node**. Адрес узла назначения Ping-запроса.
- **Sent**. Количество отправленных Ping-запросов.
- **Received**. Количество полученных Ping-запросов.
- **High**. Самый продолжительный период кругового обращения пакета.
- **Low**. Самый непродолжительный период кругового обращения пакета.
- **Last**. Период кругового обращения последнего Ping-пакета.
- **Average**. Средний период кругового обращения Ping-пакетов.
- **Trend**. Существующие тенденции, связанные с периодами кругового обращения.

Поиск неисправностей в конфигурациях средствами Ping

Помимо очевидных неисправностей кабельной проводки, причиной неполучения Ping-ответов может быть неверная конфигурация сетевых устройств. К примеру, на конечном узле может быть не настроен протокол IP; с другой стороны, нельзя исключать возможность неверной конфигурации самого вашего сервера. Еще один вариант — проблема с настройками маршрутизатора (конфигурацией IP или протокола маршрутизации), расположенного между двумя конечными узлами.

В случае, если на отправленные по определенному адресу Ping-запросы не поступает ответов, нужно перейти к поиску ошибок в настройках IP. Если ваш сервер установлен в сети с существующей конфигурацией TCP/IP, убедитесь в том, что параметры TCP/IP на серверах совместимы с этой конфигурацией. Проверьте соответствие применяемого вами протокола маршрутизации тому протоколу, который используется в остальных частях сети, а также действительность в данной сети

установленных IP-адресов сетевых интерфейсов сервера. Кроме того, следует проверить тип фреймов. Если ранее в сети не существовало конфигурации TCP/IP, убедитесь в том, что все устройства, расположенные в одном сегменте сети, настроены на один и тот же сетевой IP-адрес и маску подсети; не забывайте, что в рамках сегмента не должно быть двух устройств с идентичными IP-адресами. Если узел, на который вы пытаетесь отправить Ping-запрос, находится в другом сегменте, проверьте устройства маршрутизации между вашей станцией и узлом назначения. Все установленные маршрутизаторы должны пользоваться одним и тем же протоколом маршрутизации.

Убедившись в том, что все устройства, расположенные между сервером и пунктом назначения, настроены корректно (и находятся в одном и том же сегменте сети), попробуйте отправить Ping-запрос еще раз. Если сервер и пункт назначения находятся в разных сегментах, сначала попробуйте отправить Ping-запрос на маршрутизатор, находящийся в одном сегменте с сервером. Если этот запрос окажется успешным, продолжайте отправлять Ping-запросы всем прочим маршрутизаторам, находящимся между сервером и пунктом назначения. Если Ping-запрос, отправленный на первый маршрутизатор, не увенчался успехом, проверьте типы фреймов на сервере и на маршрутизаторе. Если Ping-запрос, отправленный на первый сервер, оказался успешным, а запросы, отправленные на второй или любые последующие маршрутизаторы — неуспешными, проверьте настройки протокола маршрутизации на этих маршрутизаторах и на вашем сервере — они должны быть совместимыми. Метод разделения одного Ping-запроса на несколько более мелких помогает точно локализовать проблему сетевой конфигурации. Найдя виновника, вы можете приступать к действиям, направленным на устранение проблемы.

Примечание

Если Ping-запрос, отправленный на компьютер, который расположен в том же сегменте, что и ваша рабочая станция, оказывается успешным, однако попытка отправки Ping-запроса на тот же компьютер из другого сегмента заканчивается неудачей, проверьте маску подсети последнего сегмента — она должна быть совместимой с аналогичной настройкой того сегмента, в котором расположена рабочая станция.

Tracert

Вполне возможно, что вам как техническому специалисту придется прибегать к проверке маршрута передачи пакета между источником и пунктом назначения. Утилита tracert (в операционных системах наподобие Linux она называется traceroute) отслеживает транзиты, через которые проходит пакет, и генерирует соответствующие отчеты. Эта возможность особенно полезна, если отклик приходит не сразу, а медленные ответы на Ping-запросы предполагают избыточность задержек (которые часто возникают из-за слишком большого количества транзитов). Кроме того, таким способом можно найти последний успешный транзит перед сбоем сети (и потерей пакета). Утилита tracert справляется с этой задачей, отсылая в пакете значение времени жизни (TTL) и надеясь получить сообщения ICMP time_exceeded (прошедшее время) с каждого транзита, через который проходит путь пакета данных. Значение TTL выражает допустимое количество транзитов, через которые пакет может пройти до того, как будет отвергнут. Таким образом, увеличивая это значение (начав с одного и приращивая по одному при каждой передаче), tracert имеет возможность по-

лучать сообщения time_exceeded от каждого маршрутизатора или другого устройства, через которое проходит пакет.

Примечание

Имейте в виду, что между распространенными реализациями этой утилиты — tracert и traceroute — есть различия. Утилита traceroute базируется на ICMP, а tracert использует сочетание UDP и ICMP.

Применение tracert

Для запуска утилиты tracert или traceroute, определения опций и указания пункта назначения применяется командная строка. Синтаксис tracert в Windows NT/2000 выглядит следующим образом:

```
tracert [-d] [-h максимальное_количество_транзитов] [-j перечень_хостов]
[-w лимит_времени] пункт_назначения
```

Ниже приводится расшифровка опций.

- `-d`. Возврат исключительно IP-адреса каждого транзита — разрешение имен хостов в адреса не выполняется.
- `-h максимальное_количество_транзитов`. Устанавливает максимальное количество транзитов до пункта назначения.
- `-j перечень_хостов`. Свободная маршрутизация через перечисленные хосты.
- `-w лимит_времени`. Устанавливает количество миллисекунд до блокировки по превышению лимита времени.
- `пункт_назначения`. IP-адрес или имя узла назначения.

В Red Hat Linux 7.x применяется другой синтаксис traceroute:

```
traceroute [-dFInrvx] [-g шлюз] [-i iface] [-f пер-
вое_значение_времени_жизни] [-m максимальное_время_жизни] [ -p порт]
[-q nзапросов] [-s адрес_источника] [-t тип_обслуживания]
[-w время_ожидания] хост [длина_пакета]
```

Для примера, предположим, что вы хотите проанализировать поведение Web-сервера, контролируемого службой Web-хостинга. С помощью tracert вы сможете получить сведения об имени хоста:

```
>tracert dlspubs.com
```

С другой стороны, мы можем ограничить количество хостов числом 10:

```
>tracert -h 10 dlspubs.com
```

Утилита tracert сгенерирует отчет, подобный тому, что показан на рис. 29.5. В первом столбце указывается число транзитов. В последующих трех столбцах приводятся подробные данные о периоде кругового обращения для каждого тестирования (в миллисекундах). В пятом столбце обозначается IP-адрес (и/или имя DNS) маршрутизатора или узла. Необычно продолжительные задержки или случаи блокировки по превышению лимита времени могут свидетельствовать о том, что в какой-то точке между источником и пунктом назначения трафик избыточен.

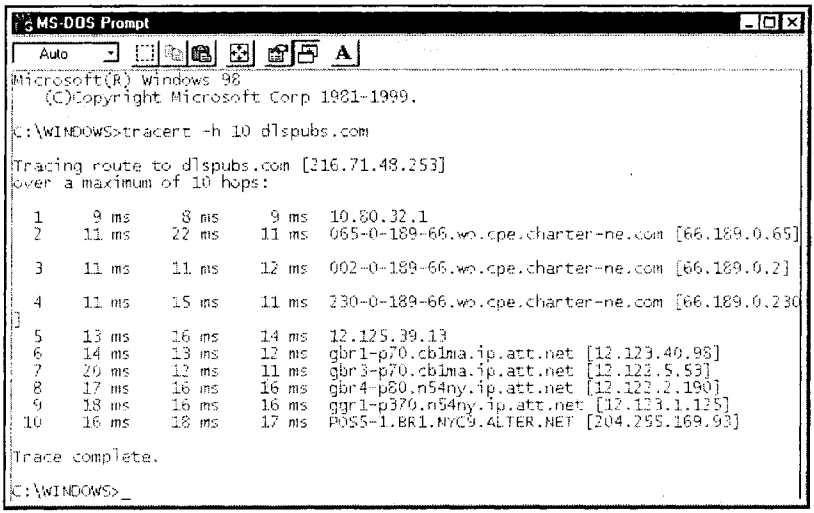


Рис. 29.5. Утилита tracert сообщает путь, по которому проходят пакеты; она способна выявлять пункт повреждения или потери трафика

Поиск неисправностей с помощью tracert

Утилита tracert может определить маршрут, по которому прошел определенный пакет. В примере, представленном ниже, пакет, направленный хосту 172.16.0.99, должен последовательно пройти через два маршрутизатора (10.0.0.1 и 192.168.0.1). Шлюзом по умолчанию хоста является 10.0.0.1, а IP-адресом маршрутизатора в сети 192.168.0.0 — 192.168.0.1.

```
>tracert 172.16.0.99 -d
Отслеживание маршрута к узлу 172.16.0.99; максимальное количество
транзитов — 30
1 2 ms 3 ms 2 ms 10.0.0.1
2 75 ms 83 ms 88 ms 192.168.0.1
3 73 ms 79 ms 93 ms 172.16.0.99
Отслеживание завершено.
```

Для того чтобы определить, в каком пункте сети пакет остановился, вы можете воспользоваться командой tracert. В следующем примере показано, как шлюз по умолчанию выявил отсутствие действительного пути к хосту 192.168.10.99. Вероятно, проблема заключается в конфигурации маршрутизатора; также возможно, что сетевой узел 192.168.10.0 не существует (т. е. указан ошибочный IP-адрес).

```
>tracert 192.168.10.99
Отслеживание маршрута к узлу 192.168.10.99; максимальное количество
транзитов — 30
1 10.0.0.1 сообщает: сеть назначения недостижима.
Отслеживание завершено.
```

Pathping

Команда pathping, присутствующая в операционной системе Windows 2000, — это инструментальное средство отслеживания маршрутов, сочетающее функции команд ping и tracert и предоставляющая дополнительные данные, отсутствующие в обеих вышеописанных утилитах. Команда pathping отправляет пакеты каждому маршрутизатору, находящемуся на пути к конечному пункту назначения, в течение определенного периода времени, а затем, исходя из полученных от каждого транзита пакетов, генерирует результаты. Так как эта команда отмечает уровень потери пакетов на любом отдельно взятом маршрутизаторе или канале, определиться с тем, какие маршрутизаторы или каналы создают имеющиеся в сети проблемы, не составляет труда.

Применение pathping

Команда pathping запускается из командной строки; в ней указывается сама команда, ее опции и пункт назначения — например, так:

```
>pathping dlspubs.com
```

Впрочем, полный синтаксис pathping в Windows 2000 выглядит следующим образом:

```
pathping [-n] [-h максимальное_количество_транзитов] [-g перечень_хостов]
[-p период] [-q запросы] [-w лимит_времени]
[-T метка] [-R]
```

Расшифровка этих опций приводится ниже.

- -n. Возврат исключительно IP-адресов каждого транзита — разрешение адресов в имена хостов не производится.
- -h максимальное_количество_транзитов. Максимальное количество транзитов до пункта назначения.
- -g перечень_хостов. Свободная маршрутизация через перечисленные хосты.
- -p период. Количество миллисекунд между Ping-запросами.
- -q запросы. Количество запросов на транзит.
- -w лимит_времени. Период времени (в миллисекундах), отводимый на ожидание каждого ответа.
- -T метка. В пакеты устанавливается приоритетная метка 2-го уровня (например, для IEEE 802.1p), и эти пакеты отсылаются по всем сетевым устройствам, через которые проходит путь. Это помогает выявить сетевые устройства с неверными настройками приоритета 2-го уровня. Ключ -T применяется для проверки качества обслуживания (QoS).
- -R. Тест RSVP помогает определить, поддерживают ли все маршрутизаторы, через которые проходит путь, протокол резервирования ресурсов (Resource Reservation Protocol, RSVP), который позволяет хост-компьютеру резервировать какую-то часть пропускной способности на прохождение потока данных. Ключ -R применяется для проверки качества обслуживания (QoS).

Поиск неисправностей с помощью pathping

Типичный отчет утилиты pathping показан в листинге 29.1. После запуска команды pathping в первую очередь появляются результаты тестирования маршрута на предмет наличия неисправностей — он очень похож на отчет, генерируемый утилитой tracert. Как бы то ни было, после этого примерно в течение двух минут (точное время зависит от числа маршрутов) pathping выводит извещение о занятости. За это время утилита собирает информацию со всех ранее перечисленных маршрутизаторов и с каналов, которые их соединяют. По окончании этого периода утилита выводит результаты тестирования. Наиболее полезные данные содержатся в столбцах **This Node/Link** (Этот узел/Соединение) **Lost/Sent=Pct** (Потеряно/Послано) и **Address** (Адрес). Как показано в листинге 29.1, канал, проходящий между 10.80.32.1 (транзит 1) и 66.189.0.65 (транзит 2) отбрасывает 13 процентов пакетов. Все остальные каналы работают нормально. Маршрутизаторы, расположенные на транзитах 2 и 4, также отбрасывают адресованные им пакеты, но эти потери не влияют на продвижение данных по заданному пути.

Листинг 29.1. Утилита pathping сочетает функции Ping и tracert, выводит подробные отчеты о прохождении пакетов между двумя станциями

```
>pathping -n aol.com
Tracing route to aol.com [64.12.187.25] over a maximum of 30 hops:
 0 192.168.168.5
 1 10.80.32.1
 2 66.189.0.65
 3 66.189.0.2
 4 66.189.0.230
 5 12.125.39.13
 6 12.123.40.98
 7 12.122.5.53
 8 12.122.2.13
 9 12.123.1.125
10 144.232.18.225
11 144.232.9.226
12 144.232.14.174
13 144.232.20.3
14 144.223.246.130
15 66.185.139.193
16 66.185.152.114
17 204.148.98.70
18 204.148.101.206
19 204.148.102.182
20 64.12.129.18
Computing statistics for 525 seconds...
                Source to Here     This Node/Link
Hop   RTT     Lost/Sent = Pct     Lost/Sent = Pct    Address
 0                                                   192.168.168.5
                                      0/ 100 =  0%      |
 1    2ms      0/ 100 = 0%           0/ 100 =  0%     10.80.32.1
                                      0/ 100 =  0%      |
```

```
 2    0ms     13/ 100 = 13%        0/ 100 =  0%    66.189.0.65
                                   0/ 100 =  0%     |
 3    0ms      0/ 100 =  0%        0/ 100 =  0%    66.189.0.2
                                   0/ 100 =  0%     |
 4    1ms      0/ 100 =  0%        0/ 100 =  0%    66.189.0.230
                                   0/ 100 =  0%     |
 5    1ms      0/ 100 =  0%        0/ 100 =  0%    12.125.39.13
                                   0/ 100 =  0%     |
 6    0ms      0/ 100 =  0%        0/ 100 =  0%    12.123.40.98
                                   0/ 100 =  0%     |
 7    1ms      0/ 100 =  0%        0/ 100 =  0%    12.122.5.53
                                   0/ 100 =  0%     |
 8    15ms     0/ 100 =  0%        0/ 100 =  0%    12.122.2.13
                                   0/ 100 =  0%     |
 9    15ms     0/ 100 =  0%        0/ 100 =  0%    12.123.1.125
                                   0/ 100 =  0%     |
10    15ms     0/ 100 =  0%        0/ 100 =  0%    144.232.18.225
                                   0/ 100 =  0%     |
11    16ms     0/ 100 =  0%        0/ 100 =  0%    144.232.9.226
                                   0/ 100 =  0%     |
12    16ms     0/ 100 =  0%        0/ 100 =  0%    144.232.14.174
                                   0/ 100 =  0%     |
13    16ms     0/ 100 =  0%        0/ 100 =  0%    144.232.20.3
                                   0/ 100 =  0%     |
14    ---    100/ 100 =100%      100/ 100 =100%    144.223.246.130
                                   0/ 100 =  0%     |
15    16ms     0/ 100 =  0%        0/ 100 =  0%    66.185.139.193
                                   0/ 100 =  0%     |
16    16ms     0/ 100 =  0%        0/ 100 =  0%    66.185.152.114
                                   0/ 100 =  0%     |
17    17ms     0/ 100 =  0%        0/ 100 =  0%    204.148.98.70
                                   0/ 100 =  0%     |
18    16ms     0/ 100 =  0%        0/ 100 =  0%    204.148.101.206
                                   0/ 100 =  0%     |
19    16ms     0/ 100 =  0%        0/ 100 =  0%    204.148.102.182
                                   0/ 100 =  0%     |
20    18ms     0/ 100 =  0%        0/ 100 =  0%    64.12.129.18
                                 100/ 100 =100%     |
21    ---    100/ 100 =100%        0/ 100 =  0%    0.0.0.0
Trace complete.
```

Коэффициенты потерь для каналов (обозначенных как "|") выражают потерю пакетов, проведенных по предложенному пути — наличие потерь свидетельствует о перегрузке канала. Коэффициенты потерь для маршрутизаторов (обозначенных их IP-адресами в крайнем правом столбце) указывают на возможность перегрузки центральных процессоров соответствующих маршрутизаторов. К примеру, похоже, что на транзитах 14 и 21 зафиксировано превышение лимита времени. Такие перегруженные маршрутизаторы, кроме того, могут оказаться источником возникновения

трудностей при сквозной передаче (особенно если пакеты перенаправляются программными маршрутизаторами).

Netstat

Утилита Netstat предоставляет техническим специалистам действенный способ вывода всесторонних статистических данных о протоколах и текущих соединениях TCP/IP. Синтаксис команды `netstat` выглядит следующим образом:

```
netstat [-a] [-e] [-n] [-s] [-p протокол] [-r] [интервал]
```

Расшифровка опций приводится ниже.

- `-a`. Показывает все соединения и прослушиваемые порты.
- `-e`. Выводит все статистические данные Ethernet.
- `-n`. Выводит все адреса и номера портов в числовой форме; разрешение имен DNS не производится.
- `-s`. Выводит статистические данные, относящиеся к каждому из следующих протоколов: TCP, IP, UDP, ICMP.
- `-p протокол`. Показывает соединения указанного протокола.
- `-r`. Выводит содержимое таблицы маршрутов.
- `интервал`. Осуществляет повторный вывод статистических данных в соответствии с указанным интервалом (в секундах).

К примеру, команда `netstat -a` выводит все соединения, а `netstat -r` — таблицу маршрутов и активные соединения. Команда `netstat -e` выводит статистические данные Ethernet, а `netstat -s` — статистику по отношению к отдельному протоколу. Если вы введете команду `netstat -n`, адреса и номера портов не будут преобразовываться в имена. Пример вывода утилиты Netstat показан в листинге 29.2.

Листинг 29.2. Утилита Netstat выводит подробный отчет о соединениях TCP/IP и состоянии указанной станции

```
>netstat -a -e -s
Interface Statistics
                           Received            Sent
Bytes                       6381673         4608428
Unicast packets               20025           19780
Non-unicast packets            3339             238
Discards                          0               0
Errors                            0               0
Unknown protocols              9780
IP Statistics
   Packets Received                   = 23121
   Received Header Errors             = 0
   Received Address Errors            = 1
   Datagrams Forwarded                = 0
   Unknown Protocols Received         = 0
```

```
    Received Packets Discarded          = 0
    Received Packets Delivered          = 23120
    Output Requests                     = 19951
    Routing Discards                    = 0
    Discarded Output Packets            = 0
    Output Packet No Route              = 0
    Reassembly Required                 = 0
    Reassembly Successful               = 0
    Reassembly Failures                 = 0
    Datagrams Successfully Fragmented   = 0
    Datagrams Failing Fragmentation     = 0
    Fragments Created                   = 0
ICMP Statistics
                            Received        Sent
    Messages                3389            3507
    Errors                  0               0
    Destination Unreachable 0               8
    Time Exceeded           40              0
    Parameter Problems      0               0
    Source Quenches         0               0
    Redirects               0               0
    Echos                   688             2811
    Echo Replies            2661            688
    Timestamps              0               0
    Timestamp Replies       0               0
    Address Masks           0               0
    Address Mask Replies    0               0
TCP Statistics
    Active Opens                        = 489
    Passive Opens                       = 487
    Failed Connection Attempts          = 0
    Reset Connections                   = 3
    Current Connections                 = 20
    Segments Received                   = 15921
    Segments Sent                       = 15658
    Segments Retransmitted              = 12
UDP Statistics
    Datagrams Received    = 1556
    No Ports              = 4955
    Receive Errors        = 0
    Datagrams Sent        = 774
```

Ipconfig

Утилита ipconfig — это удобное средство исследования конфигурации стека TCP/IP в системе Windows NT/2000 (в системах UNIX/Linux применяется утилита ifconfig). С ее помощью вы можете вывести информацию о сетевой конфигурации — данные

о каждом сетевом адаптере в отдельной системе. В подобном отчете указывается следующее:

- IP-адрес;
- маска подсети;
- шлюз по умолчанию;
- DNS-сервер(ы);
- идентификация домена.

Примечание

В клиентских системах Windows 9x вместо `ipconfig` применяется команда `winipcfg`.

Применение ipconfig

При подаче команды `ipconfig` с опцией `/all` выводится подробный отчет конфигурации всех интерфейсов, включая все настроенные последовательные порты. Помимо прочего, эти выходные данные могут использоваться для подтверждения конфигурации TCP/IP каждого компьютера в сети, а также для дальнейшего анализа проблем со стеком TCP/IP в сети. К примеру, если компьютеру присваивается IP-адрес, дублирующий существующий IP-адрес, его маска подсети представляется как 0.0.0.0. Пример, приведенный в листинге 29.3, демонстрирует выходные данные команды `ipconfig /all` на сервере домена Windows 2000.

Примечание

Если в конфигурации стека TCP/IP проблем не выявлено, следующим этапом представляется тестирование способности к соединению с другими хост-компьютерами в сети TCP/IP — это делается с помощью утилиты наподобие Ping.

Листинг 29.3. Утилита ipconfig позволяет техническим специалистам проверить и отрегулировать сетевую плату станции и логическую конфигурацию сети

```
>ipconfig /all
   Windows 2000 IP Configuration
   Host Name . . . . . . . . . . . . : SERVER01
   Primary DNS Suffix  . . . . . . . : admintration.dls.com
   Node Type . . . . . . . . . . . . : Broadcast
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : admintration.dls.com
dls.com
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : 82559 Fast Ethernet
   Physical Address. . . . . . . . . : 00-E0-18-2F-65-FC
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IP Address. . . . . . . . . . . . : 192.168.168.5
```

```
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.168.1
DHCP Server . . . . . . . . . . . : 192.168.168.1
DNS Servers . . . . . . . . . . . : 24.216.218.9
                                    24.216.218.25
                                    24.216.218.41
Lease Obtained. . . . . . . . . . : Tuesday, February 05, 2002
Lease Expires . . . . . . . . . . : Wednesday, February 06, 2002
```

Освобождение/возобновление

Осуществляя поиск сетевой неисправности, связанной с TCP/IP, начните с проверки конфигурации TCP/IP на том компьютере, где эта неисправность выявляется. Если на этом компьютере работает служба DHCP (а для получения конфигурации применяется сервер DHCP), у вас есть возможность ввести команду `ipconfig /release` для немедленного освобождения текущей DHCP-конфигурации хоста, а затем инициировать восстановление аренды при помощи команды `ipconfig /renew`. В результате подачи команды `ipconfig /renew` все сетевые адаптеры, установленные на данном компьютере и использующие DHCP (кроме тех, которые настраиваются вручную), предпринимают попытку связи с DHCP-сервером для восстановления своей существующей конфигурации или получения новой.

Другие опции ipconfig

Команда `ipconfig /flushdns` позволяет по требованию выполнить сброс на диск и установку в нулевое состояние содержимого кэша DNS-клиента Windows 2000. В ходе поиска неисправностей DNS эта команда (в случае необходимости) может пригодиться для отбрасывания безрезультатных записей из кэша, как и любых других динамически добавляемых записей. Имейте в виду, что восстановление кэша не предполагает исключения из него записей, которые были предварительно загружены из локального файла hosts.

При помощи команды `ipconfig /registerdns` в среде Windows 2000 вы можете вручную инициировать динамическую регистрацию имен DNS и IP-адресов, настроенных на данном компьютере. Эта опция может оказаться полезной в процессе поиска ошибок при неудачной регистрации имени DNS или динамическом обновлении между клиентом и DNS-сервером; при этом перезагружать клиентскую машину не нужно. По умолчанию, команда `ipconfig /registerdns` восстанавливает все аренды адресов DHCP и регистрирует все связанные с ними имена DNS, настроенные и применяемые клиентским компьютером. Чтобы найти имена адаптеров, которые можно указать в рамках команды `ipconfig`, введите только эту команду (не указывайте никаких дополнительных параметров). В результате будет выведен перечень имен всех адаптеров, которые могут использоваться в данном компьютере. После этого можно ввести команду `ipconfig /registerdns [адаптер]`. В случае поиска ошибок, связанных с неудачной динамической регистрацией DNS клиентского компьютера и его имен DNS, разумно убедиться в том, что причиной этого не является одно из следующих обстоятельств.

- Зона, в которой клиенту требуется обновление и регистрация, не способна принимать динамические обновления.

- DNS-серверы, которыми, в соответствии со своими настройками, пользуется клиент, не поддерживают или не распознают протокол динамического обновления DNS.
- Первичный (или интегрированный со службой каталогов) DNS-сервер данной зоны отказал в выполнении запроса на обновление. Вероятнее всего, причина заключается в том, что клиент не обладает правами доступа, необходимыми для обновления его собственного имени.
- Сервер или зона недоступны из-за возникновения других сетевых неисправностей — например, вследствие сбоя сети или сервера.

Для того чтобы вывести данные об идентификаторе класса DHCP на клиентском компьютере Windows 2000, введите команду `ipconfig /showclassid` — так вы сможете узнать идентификатор класса DHCP, применяемый клиентом при получении аренды от DHCP-сервера. В примере, представленном в листинге 29.4, используется принятое по умолчанию имя адаптера "Local Area Connection", а в качестве идентификатора класса DHCP, принятого в данный момент на клиентском компьютере для выполнения локального соединения в сети, указана строка ASCII ("MyNewClassId").

Листинг 29.4. Утилита ipconfig применяется для проверки и задания конфигурации DHCP на отдельной станции

```
>ipconfig /showclassid "Local Area Connection"
Windows 2000 IP Configuration
DHCP Class ID for Adapter "Local Area Connection":
DHCP ClassID Name . . . . . : Default BOOTP Class
DHCP ClassID Description . . . . : User class for BOOTP clients
DHCP ClassID Name . . . . . : Default Remote Access Class
DHCP ClassID Description . . . . : User class for remote access clients
Host Name . . . . . : SERVER01
Primary DNS Suffix . . . . . : admintration.dlspubs.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Description . . . . . : Combo PCMCIA EthernetCard
Physical Address. . . . . : 00-00-00-00-7C-DC
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.1.51
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.0.1
DHCP Class ID . . . . . : MyNewClassId
DNS servers . . . . . : 10.0.0.3
Primary WINS server . . . . . : 10.0.0.5
```

Наконец, на клиентской машине Windows 2000 установка идентификатора класса DHCP сетевого адаптера производится при помощи команды `ipconfig /setclassid`;

в ней же должно указываться имя сетевого адаптера, а также новая строка ASCII, которая будет использоваться в качестве имени класса. К примеру, команда

```
>ipconfig /setclassid "Local Area Connection" MyNewClassId
```

установит строку ASCII ("MyNewClassId") в качестве строки идентификатора класса DHCP для сетевого соединения, применяемого на данном клиентском компьютере.

ifconfig

В системах UNIX/Linux применяется команда `ifconfig`. Она не только выводит данные конфигурации IP — она способна вносить в них изменения. Команда `ifconfig` применяется во время загрузочной последовательности, выполняя функцию первоначальной конфигурации подсоединенных к системе сетевых адаптеров. После начала работы системы правом изменения конфигурации с помощью этой команды обладает только суперпользователь. В процессе поиска неисправностей в системах UNIX/Linux `ifconfig` представляет собой быстрый метод определения корректности конфигурации системы. Для того чтобы просто вывести на экран текущую конфигурационную информацию, введите команду `ifconfig` без параметров. Для изменения конфигурации суперпользователь может вводить следующие команды.

- `ifconfig arp`. Так включается протокол разрешения адресов (Address Resolution Protocol, ARP). Для отключения ARP следует ввести команду `ifconfig -arp`.
- `ifconfig dhcp`. Чтобы сетевой адаптер смог получить адрес, нужна служба DHCP. В качестве альтернативы вы можете воспользоваться командой `ifconfig auto-dhcp`.
- `ifconfig down`. Эта команда сообщает, что интерфейс не функционирует — таким образом, все сетевые соединения с участием данного адаптера закрываются.
- `ifconfig metric [значение]`. Эта команда меняет метрику маршрутизации для данного интерфейса.
- `ifconfig netmask [маска]`. Эта команда устанавливает для данного сетевого адаптера маску подсети.

Дополнительные ресурсы

ifconfig: **www.linuxdoc.org/LDP/nag2/x-087-2-iface.ifconfig.html**.

ipconfig: **www.computerhope.com/ipconfig.htm**.

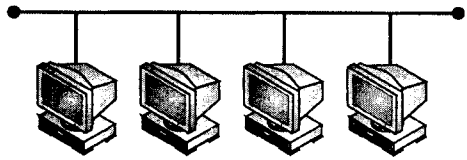
netstat: **support.morehouse.edu/winipcfg.html**.

pathping: **www.ece.villanova.edu/~kpreddy/Pathping.html**.

ping: **www.ping127001.com/pingpage.htm**.

tracert: **www.tracert.com**.

winipcfg: **support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q141698**.



ГЛАВА 30

Поиск неисправностей при помощи анализатора протоколов

Как вы понимаете, предприятиями всех размеров сети оцениваются как ценное имущество. Обеспечив возможность совместного использования ресурсов, ведения бухгалтерского учета, доступа к электронной почте и сети Интернет, компьютерные сети сократили издержки, упростили процессы и поспособствовали организации коллективного обращения к информации. Однако зачастую сети представляют собой сложные и запутанные нагромождения аппаратного и программного обеспечения, а сетевые неисправности способны оказывать негативное воздействие на продуктивность работы десятков (и даже сотен) пользователей. Технический специалист обязательно должен уметь находить причину возникновения неисправности и как можно быстрее устранять ее. Не располагая средствами отображения и интерпретации сетевого трафика, технический специалист оказывается ограниченным трудоемкими методами поиска неисправностей, предполагающими пробы и ошибки. В виде анализаторов протоколов в распоряжение технических специалистов предоставляется мощное многоцелевое инструментальное средство анализа сетевых операций и локализации слабых мест. К примеру, анализатор протоколов помогает техническим специалистам определить, какая станция генерирует чрезмерный исходящий трафик или испытывает некоторые трудности — методом проб и ошибок получить эту информацию практически невозможно. В этой главе рассмотрен ряд методов поиска неисправностей в сетях с применением программных анализаторов протоколов на сетевых компьютерах.

Примечание

Существуют и специализированные анализаторы протоколов на аппаратной основе, но в этой главе предполагается, что вы пользуетесь программным анализатором протоколов, и что он установлен на локальном компьютере — например, на подключенном к сети ноутбуке или на другой диагностической платформе.

Принципы работы анализатора протоколов

Для технических специалистов анализатор протоколов является мощным средством мониторинга сетевого трафика, а также его анализа с целью изучения данных в реальном времени или определения данных о существующих тенденциях, с помощью которых выявляется до 85 процентов всех сетевых неисправностей. Они способны

воспроизводить трафик и другие сетевые условия. К примеру, анализатор протоколов может:

- идентифицировать проблемные сетевые станции;
- фильтровать и сохранять данные, исходя из ряда критериев;
- выявлять источники и пункты назначения указанного сетевого трафика;
- измерять уровень использования сети и ее эффективность;
- вырабатывать аварийные сигналы в случае превышения заданных значений.

Не будь той информации, которую предоставляет анализатор протоколов, никто не смог бы узнать, что происходит "внутри сетевой проводки", и сетевые неисправности могли бы остаться необнаруженными и неисправленными вплоть до аппаратного сбоя. Такой ход развития событий может дорого обойтись любой организации — его цена выражается в потерянной производительности поврежденной сети и в бессчетных часах, проведенных за процедурой поиска неисправностей методом проб и ошибок. Современные сетевые анализаторы способны расшифровывать и обрабатывать захваченную информацию, определять, какие события вызывают появление определенных сбойных ситуаций, а затем выводить информацию, касающуюся возможных причин этих событий.

Впрочем, для того, чтобы пользоваться анализатором протоколов, от технического специалиста или администратора требуются некоторые знания. Так как, по существу, анализаторы протоколов занимаются захватом кадров, то для интерпретации захваченных данных нужны хорошие практические познания в области протоколов (вплоть до уровня кадров). Кроме того, для того чтобы в полной мере понимать роль захваченной информации, важно знать методы доступа, принятые в сетях Ethernet и маркерного кольца. К примеру, чтобы оценить значимость чрезмерных конфликтов в сегменте сети Ethernet, технический специалист должен разбираться в множественном доступе с контролем несущей и обнаружением коллизий (Carrier Sense Multiple Access with Collision Detection, CSMA/CD); чтобы представлять себе опасность сбойных кадров, специалист должен знать длины кадров, принятые в сетях Ethernet.

Помимо диагностики, анализатор пакетов помогает выполнить количественный анализ необходимости расширения сети; с его помощью вы можете имитировать сетевой трафик и рабочие условия. Анализатор способен фиксировать сетевые тенденции и предоставлять сетевому администратору долгосрочные данные о производительности; кроме того, он оказывает неоценимую помощь в прогнозировании необходимости роста. Анализатор даже может генерировать сетевой трафик — он делает это в случаях, когда вам необходимо оценить все возможные варианты перед выполнением обновлений (подробнее эта предметная область рассматривается в *гл. 27*).

Аппаратные и программные анализаторы

Обычно анализаторы протоколов предусматривают некую комбинацию аппаратного и программного обеспечения; за последние несколько лет они прошли долгий путь развития. Большинство ранних анализаторов представляли собой громоздкие и неповоротливые ящики, предлагавшие сравнительно простые функции аппаратного захвата и отчетности. Обеспечивая минимальную постобработку и интерпретацию,

такие анализаторы могли предоставлять необработанные данные, понятные только самым продвинутым специалистам. Кроме того, они были дороги (в пределах $30 000) и доступны только самым крупным организациям.

Программные анализаторы

Вычислительные возможности персональных компьютеров увеличивались, и для того, чтобы появились программные средства анализа протоколов, потребовалось не слишком много времени. При использовании на ПК аналитического программного обеспечения появилась возможность сделать так, чтобы сетевая плата этого компьютера захватывала все пакеты, появляющиеся в сетевой среде, вне зависимости от их адресов. Многие модели сетевых плат способны собирать любые пакеты — эта функция часто называется беспорядочным режимом. Таким образом, появилась возможность захватывать, фиксировать, обрабатывать и отображать сетевые данные на обычном персональном компьютере, а не на специализированном аппаратном устройстве (причем новые решения стоили меньше, чем аппаратные устройства). В состав программных анализаторов протоколов обычно входит компонент, отвечающий за сбор данных — он осуществляет сбор информации о данных, передающихся в рамках отдельного сегмента локальной сети. Этот элемент сбора данных отправляет данные (через операционную систему хост-компьютера) аналитическому компоненту, который расшифровывает, обрабатывает, а затем с помощью одного из нескольких представлений отображает эти данные. Переход к программному анализу значительно снизил стоимость анализаторов, но такой подход в первое время не отличался особой мобильностью (в большинстве случаев компьютер приходилось переносить из одного сегмента в другой). В современных условиях портативные компьютеры обладают вычислительными мощностями, достаточными для работы профессиональных программных анализаторов протоколов, и обеспечивают мобильность, позволяющую им работать в любом физическом местоположении в рамках компании.

Примечание

Помните, что сам по себе факт установки аналитического программного обеспечения на всех персональных компьютерах может не привести ни к чему, кроме появления сбрасываемых кадров (в случае, если буферы сетевых интерфейсных плат будут перегружены).

С другой стороны, современные программные анализаторы протоколов (например, Network Instruments Observer или Network General Sniffer) могут работать на любой рабочей станции Windows 98/ME/NT/2000/XP, подключенной к компьютерной сети. Чтобы предоставить анализатору протоколов возможность сбора данных в других областях локальной или глобальной сети (помимо отдельного сетевого сегмента), на рабочие станции, находящиеся в других сегментах, устанавливаются внешние программные компоненты (называемые зондами) — это называется распределенной средой. Такие удаленные зонды осуществляют сбор данных точно таким же образом, каким это делает локальный зонд, а затем отсылают данные на консоль анализатора протоколов с целью проведения их дальнейшего анализа. Применение зондов упрощает задачу поиска неисправностей в нескольких сегментах с единственной рабочей станции.

Новая жизнь аппаратных анализаторов

Однако с появлением программ постобработки и интерпретирования аппаратные анализаторы сделали огромный шаг вперед; в высокопроизводительных сетях они до сих пор рассматриваются как один из вариантов. В критических ситуациях анализаторы протоколов на аппаратной основе способны выполнять функции, добиться которых от программных продуктов не представляется возможным. Аппаратные средства обычно лучше справляются с высокоскоростными сетевыми средами (например, 100/1000BaseT), т. к. для получения трафика из сетевой среды программные анализаторы пользуются обычными сетевыми платами. В аппаратных анализаторах предусматриваются специальные схемы, применяемые для выполнения множества функций со скоростью, значительно превышающей быстродействие программного обеспечения; кроме того, в большинстве случаев они оказываются более надежными.

Не стоит забывать о том, что анализатор, работающий на базе персонального компьютера, может ограничиваться возможностями сетевой платы. К примеру, некоторые простые адаптерные платы содержат функцию (она зашита в их программно-аппаратные средства), которая автоматически сбрасывает определенные типы пакетов, содержащих ошибки. Следовательно, если вы пытаетесь выявить конкретные ошибки, которые приводят к появлению в сети проблем, программный продукт, работающий на базе ПК, возможно, не сможет вам помочь. Кроме того, несмотря на то, что сетевая плата способна обнаруживать практически любые проходящие в сети пакеты, нет никакой гарантии, что она сможет захватить эти данные и передать их протоколам более высокого уровня. Когда сетевая плата захватывает все кадры и передает их стеку протоколов, она работает в беспорядочном режиме. Некоторые сетевые платы (в особенности старые) не умеют действовать в беспорядочном режиме; таким образом, вы должны ознакомиться с документацией, сопровождающей сетевую плату, которую намереваетесь использовать на рабочей станции с программным анализатором протоколов.

Гибридный тип анализатора протоколов сочетает в себе лучшие черты аппаратных и программных продуктов. Гибридные анализаторы предусматривают выполнение функций захвата и фильтрации средствами специализированного аппаратного компонента, который подключается к рабочей станции (или портативному компьютеру); в свою очередь компонент, установленный на ПК, выполняет функции обработки, отображения и хранения. В составе аппаратного компонента есть специальные схемы и вычислительные возможности, достаточные для захвата данных непосредственно из кабеля; впоследствии эти данные фильтруются, обрабатываются и выводятся на экран программным приложением, установленным на персональном компьютере. Анализатор этого типа дороже, чем исключительно программные решения, однако он способен проводить анализ на значительно более высоких скоростях передачи данных и оказывается крайне полезным в средах с высокой пропускной способностью (например, в оптоволоконных сетях).

Основные функции

Проще говоря, назначением анализатора протоколов является захват и отображение данных, проходящих по сетевым проводам. По существу, анализатор подключается к сети в качестве записывающего устройства, осуществляет мониторинг трафика, но

при этом (иногда) в незначительных объемах генерирует собственный трафик. Каждый кадр данных, проходящий по проводам, сохраняется в буферной памяти анализатора (хотя с помощью фильтров можно предотвратить захват трафика определенных типов). Рассмотрим базовые функции анализатора протоколов.

Захват данных

Анализатор протоколов захватывает пакеты данных, когда они проходят через локальный сегмент сети, и ставит на каждый пакет отметку времени. Многие анализаторы используются для фиксации следов (ряда кадров) в течение предопределенного периода времени или в ответ на определенное событие (рис. 30.1). Анализатор получает данные через собственный буфер; обычно в нем предусматриваются компоненты, позволяющие сохранять содержимое буфера в файл на гибком или жестком диске, в отношении которого впоследствии проводятся аналитические или сравнительные операции.

Анализатор захватывает данные в буфер ограниченного размера, так что в случае заполнения буфера анализатор начинает записывать новые данные поверх старых — тех, что записаны в начале буфера. К примеру, если оставить анализатор подключенным к сети в течение всего дня, то данные, собранные утром, могут быть потеряны, т. е. заменены данными, собранными вечером. Следовательно, рекомендуется либо настроить объемный буфер захвата (это относится к программным анализаторам), либо приобрести столько памяти и дискового пространства, сколько вы можете себе позволить (в отношении аппаратных анализаторов). Чем больше пространства выделяется для хранения захвата, тем больше данных вы впоследствии сможете проанализировать.

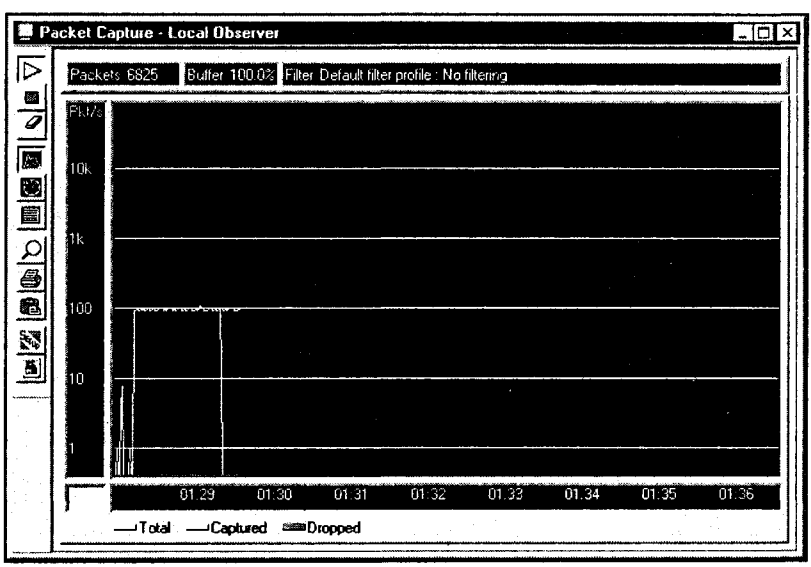


Рис. 30.1. Применение функции захвата анализатора пакетов для фиксации сетевого трафика с целью последующего анализа

Фильтрация данных

Информация, которую вы получите в результате фиксации каждого пакета данных, передаваемого по сети, скорее всего, окажется избыточной по сравнению с тем, что вам нужно для устранения конкретной проблемы (кроме того, она заполнит даже самый большой буфер). Практически во всех типах анализаторов протоколов предусматривается ряд фильтров захвата, которые способны препятствовать захвату всего трафика, кроме того, который вам нужен (рис. 30.2). Возможна фильтрация по узлу, серверу, протоколу, классу назначения или сетевому событию. К примеру, если вам известно, что данная проблема связана с протоколом IPX, вы можете настроить фильтр на захват исключительно пакетов IPX — таким образом, данные всех прочих протоколов захватываться не будут, а в буфере останется больше свободного пространства. С другой стороны, если вы знаете, что проблема связана с конкретным узлом, вы можете настроить фильтр захвата на анализ всех исходящих и входящих пакетов этого узла. Фильтрация может проводиться во время захвата или отображения. Скажем, вы можете захватить все кадры, прошедшие в течение заданного временного интервала, но, исходя из задач по поиску неисправностей, просмотреть только определенные кадры.

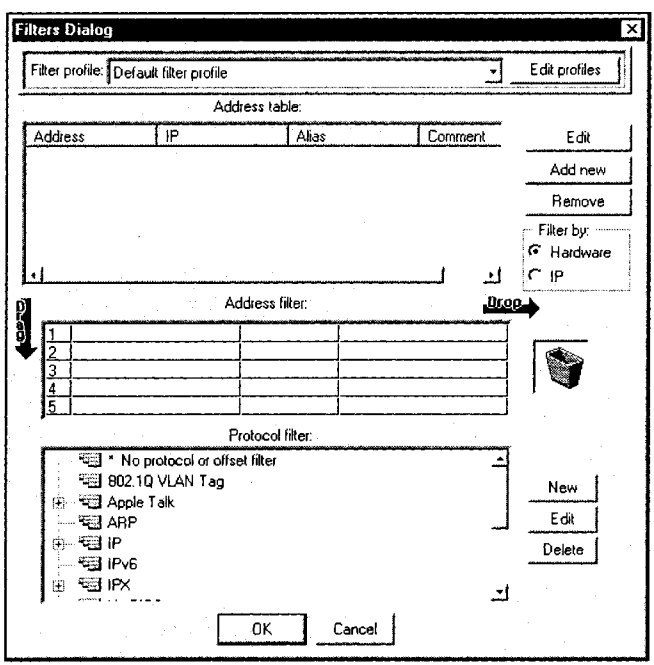


Рис. 30.2. Фильтры захвата позволяют анализатору сфокусироваться на захвате только интересующих вас пакетов, обеспечивая большее время захвата при меньшем объеме потребляемой памяти

Расшифровка данных

После захвата пакетов анализатор может провести их расшифровку — для этого используется интерпретатор протоколов. Некоторые анализаторы протоколов способ-

ны расшифровывать только данные какого-то одного протокола; в других же есть несколько интерпретаторов протоколов, которые можно приобрести по отдельности (с другой стороны, при покупке продукта они могут поставляться в качестве пакета дополнений). Процесс расшифровки подразумевает последовательную разбивку каждого захваченного пакета с последующим декодированием присутствующих в нем уровней различных протоколов. Эти данные обычно выводятся в виде сводки, составленной из простого текста (рис. 30.3). Именно эта информация позволяет "заглянуть внутрь" отдельного кадра.

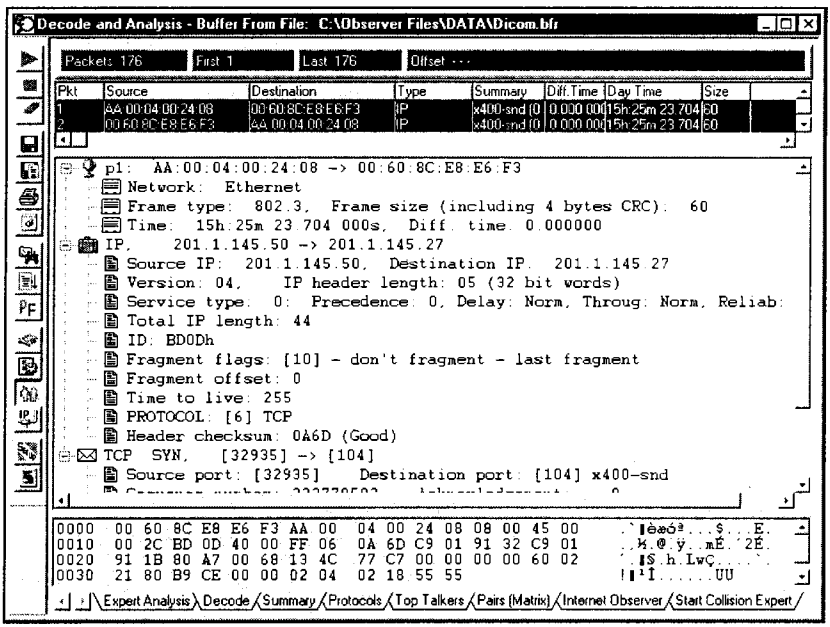


Рис. 30.3. После захвата данных у вас есть возможность расшифровки отдельных пакетов для их проверки на предмет повреждений или других проблем

Как правило, анализаторы протоколов не осуществляют расшифровку пакетов и их сравнение с моделью OSI по отдельным уровням. На практике анализаторы часто смешивают уровни. К примеру, три верхних уровня модели OSI (прикладной, представления и сеансовый) часто сводятся к одному уровню расшифровки, который также называется прикладным уровнем — дело в том, что обычно на сеансовом уровне и уровне представления работает ограниченное количество протоколов (подобных NetBIOS). На этом уровне анализатору важно то, как два узла, участвующих в соединении, настраиваются приложением, и как эти два конечных узла взаимодействуют через приложение. При этом возможно выявление таких элементов, как медленные передачи файлов.

Анализаторы часто обозначают транспортный уровень модели OSI как уровень соединений; они анализируют эффективность сквозной передачи и устранения ошибок. Сетевой уровень модели OSI некоторыми анализаторами называется уровнем сетевых станций — он связан с сетевыми адресами и вопросами маршрутизации. Дублированные сетевые адреса выявляются именно на этом уровне расшифровки.

На канальном и физическом уровнях OSI (некоторыми анализаторами они сводятся к одному и называются уровнем станций) анализатор работает с реально передаваемыми данными и физическими ошибками, возникающими по пути их передачи. Кроме того, на этом уровне расшифровывается пропускная способность, широковещательные кадры и ошибки контроля при помощи циклического избыточного кода (Cyclic Redundancy Check, CRC).

Отображение данных

Естественно, анализатор протоколов был бы совершенно бесполезным приспособлением, если бы не мог выводить расшифрованную информацию на экран — для ее просмотра администратором. Отображение может отделяться от захвата, т. е. выполняться на отдельном этапе (при этом сначала производится захват, а затем — просмотр файла данных), или производиться одновременно с захватом. Зачастую этот одновременный метод оказывается более полезным — он позволяет администратору переключаться между экранами, анализируя происходящее в режиме реального времени. Большинство анализаторов предусматривают графическое отображение таких параметров, как уровень использования сети, уровни использования протоколов и т. д. Как только кадр проходит через фильтр отображения, его можно представлять в сводном и подробном режимах, в шестнадцатеричном представлении, сочетаемом с режимом ASCII, и т. д. Некоторые анализаторы предусматривают возможность вывода на экран всех этих трех представлений одновременно (хотя это иногда сбивает с толку).

Прочие функции

Несомненно, современными анализаторами протоколов предлагается множество дополнительных функций и возможностей; функции, описанные ниже, нетрудно встретить в новейших программных анализаторах протоколов наподобие Observer. Определяясь с выбором анализатора, примите их во внимание.

Аварийные сигналы

Аварийные сигналы предоставляют сетевому администратору возможность проведения профилактического мониторинга сети. Некоторые анализаторы позволяют администраторам устанавливать пороги, при превышении которых происходит выдача аварийных сигналов. К примеру, установив 25-процентный порог уровня использования в сети Ethernet, вы сможете узнать, когда сеть войдет в переполненное состояние — таким образом, администратор может приступить к планированию модернизации или оптимизации еще до того, как переполнение сети перейдет в критическую фазу. Обычно анализаторы поставляются с порогами, принимаемыми по умолчанию — они устанавливаются на уровнях, которые в большинстве случаев являются приемлемыми; впрочем, вы можете установить пороги самостоятельно (рис. 30.4).

Триггеры и действия

Администратор может без труда настроить анализатор на выявление определенного сетевого события и выполнение тех или иных действий. К примеру, когда анализа-

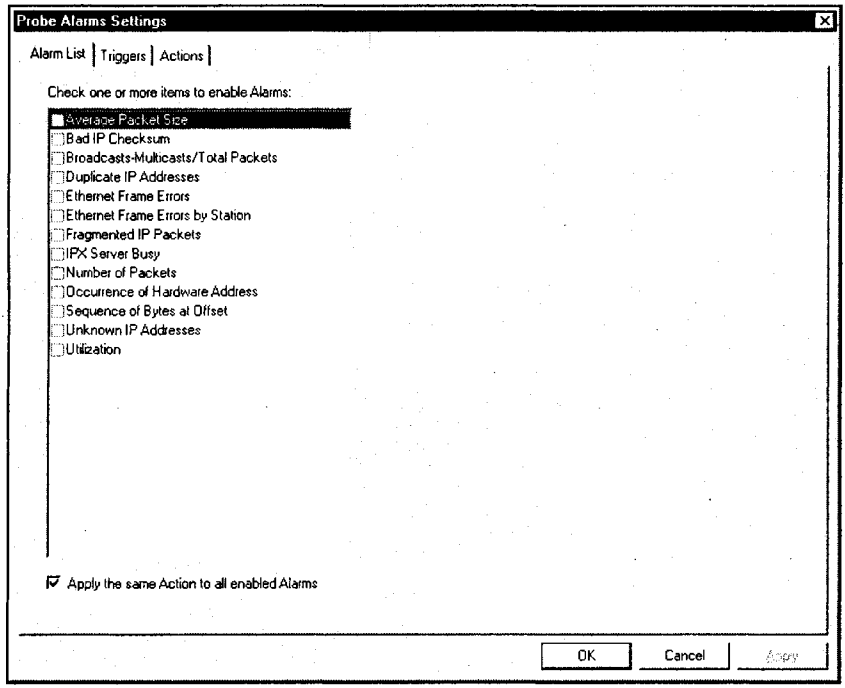


Рис. 30.4. Аварийные сигналы можно использовать для оповещения о потенциальных проблемах еще до того, как они станут серьезными и смогут ухудшить работу сети

тор обнаруживает заданное (триггерное) событие (например, дублированный сетевой адрес), он начинает запись или захват данных на диск, но факультативно может прекратить захват после того, как это событие произойдет. Эта функция оказывается чрезвычайно полезной в тех ситуациях, когда вы знаете, какие события хотите захватить, но вам неизвестно, когда они произойдут. Вместо того чтобы производить беспорядочный захват и тратить время на анализ данных, надеясь выявить нужное событие, вы можете запрограммировать анализатор на выполнение захвата только в том случае, если нужное событие произойдет.

Рассмотрим пример использования программного анализатора, подобного Observer. Предположим, что вы хотите настроить анализатор на принятие мер в отношении ошибок кадров Ethernet. В первую очередь нужно открыть вкладку **Alarm List** (Список аварийных сигналов) (рис. 30.4) и пометить флажок **Ethernet Frame Errors** (Ошибки кадров сети Ethernet). Чтобы настроить запуск аварийного сигнала, перейдите на вкладку **Triggers** (Триггеры) (рис. 30.5). В данном случае доступен только один триггер, однако для него вы можете настроить процентное отношение ошибочных кадров, минимальное количество пакетов и период усреднения. Задействовав настройки триггера, перейдите на вкладку **Actions** (Действия) (рис. 30.6) — с ее помощью вы сможете определить, каким образом анализатор будет реагировать. Установите флажки, соответствующие нужным действиям, и примените эти настройки. Таким образом вы сможете организовать точный, автоматический мониторинг сетевых параметров.

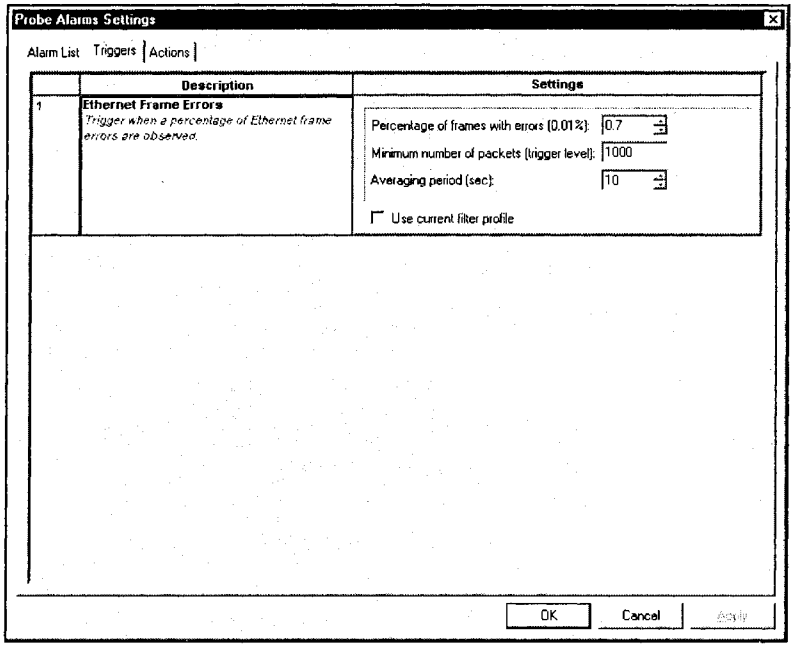


Рис. 30.5. Конфигурирование аварийных сигналов путем настройки характеристик триггера

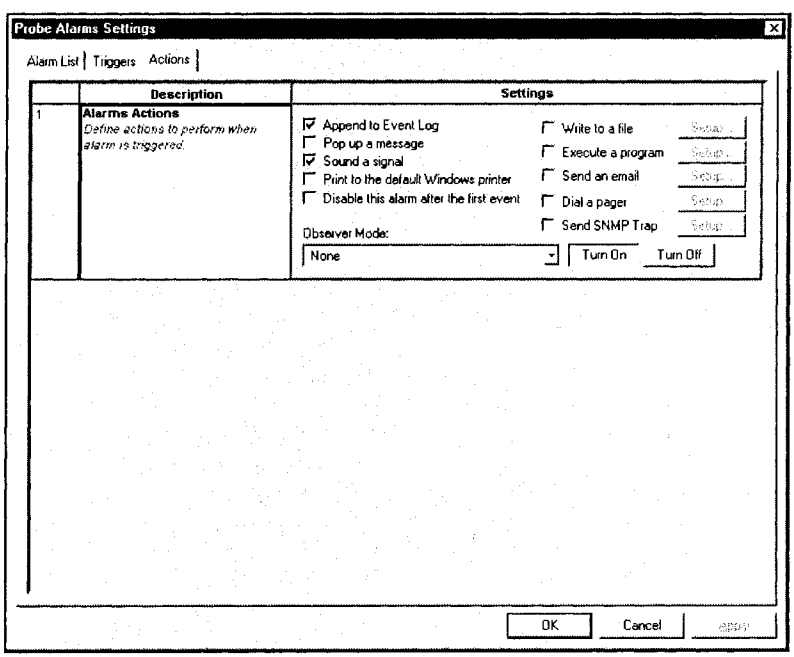


Рис. 30.6. После настройки аварийных настроек вы можете указать действия, которые анализатор должен будет выполнять автоматически

Установление базиса

Некоторые анализаторы протоколов, в том числе Observer, предусматривают возможность отслеживания сетевой активности и производительности во время работы в нормальном режиме — таким способом устанавливаются "нормальные" уровни сетевой активности. Впоследствии эти данные используются в качестве базиса (Baseline) для сравнения с проблемными ситуациями в сети. В некоторых случаях возможно сохранение фиксированных данных, которые впоследствии можно использовать для воспроизведения конкретной ошибки, или ее имитации при исправной сети для целей, связанных с анализом. Более подробная информация о выявлении базиса сети содержится в *гл. 27.*

Псевдонимы

Одна из трудностей, связанных с анализом протоколов, заключается в том, что результаты иногда бывает трудно связать с конкретной станцией или пользователем. К примеру, не представляет проблемы определить, что основным источником сообщений является IP-адрес 192.168.1.4, или, скажем, с MAC-адресом 03:FD:3E:44:A5:50 связано чрезмерное количество ошибок Ethernet, но совсем другое дело, если бы мы знали, что речь идет о рабочей станции John или сервере R&D. Многие анализаторы протоколов содержат таблицу адресов, связываемую с пользователями (они называются псевдонимами). Анализатор может делать это автоматически, но, с другой стороны, он позволяет вам загрузить заранее составленный перечень псевдонимов.

Генерирование трафика

Анализаторы протоколов (наподобие Observer) предусматривают функцию генератора трафика, которая поддерживает целый ряд протоколов (рис. 30.7) — иногда ее называют имитатором. Генератор трафика способен формировать пакеты заданных размеров с определенной частотой и в указанных количествах, включать в них нужные заголовки. Эта функция может оказаться предельно полезной для администратора, который желает поэкспериментировать с возможными вариантами развития событий в определенных ситуациях. Имитации позволяют сетевому администратору узнать, как будет себя вести сеть, поставленная в определенные условия трафика.

Анализ сетевого аппаратного обеспечения

Несмотря на то, что наиболее полезные функции анализаторов связаны с анализом пакетов, отправляемых по сети, некоторые анализаторы (подобные Observer) могут проводить более непосредственную оценку сетевого аппаратного обеспечения и принимать решения о том, как оно работает.

- Функции, подобные наблюдению за маршрутизаторами (**Router Observer**), позволяют вам в реальном времени увидеть, как работает маршрутизатор (или группа маршрутизаторов), оценить уровень его использования. Возможно, вы очень быстро убедитесь в том, что маршрутизатор создает узкое место, и сможете определить, какие пакеты препятствуют его нормальной работе: входящие или исходящие (может быть, и те, и другие). Ознакомившись со статистическими данными за прошлые периоды, вы сможете выяснить, является ли зафиксированная проблема хронической (что, вероятно, свидетельствует о необходимости организации более скоростного соединения) или острой (в последнем случае она, видимо, свидетельствует о каком-либо сбое).

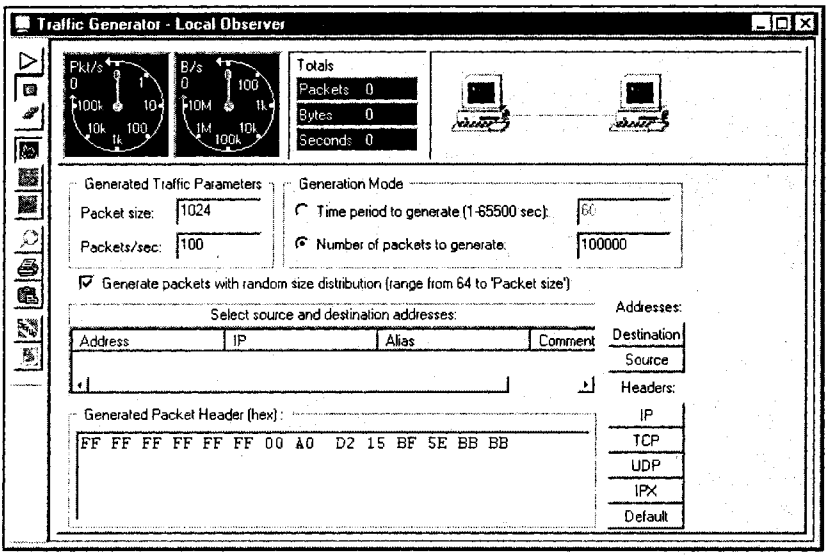


Рис. 30.7. Функция генерации трафика способна имитировать широкий спектр условий сетевого трафика в целях проведения нагрузочных испытаний и проверки возможных вариантов развития событий в заданных ситуациях

- Если Observer установлен на рабочей станции с поддерживаемой им сетевой платой и предназначенным для нее драйвером ErrorTrak от компании Network Instruments, у вас появляется возможность отслеживать сетевые ошибки, связанные именно с данной станцией. Этот режим позволяет акцентировать ошибки, допускаемые отправляющей станцией, и тип этих ошибок. Кроме того, работая за данной станцией и просматривая коэффициенты ошибок, вы можете оценивать серьезность потока сообщений об ошибках. Традиционно для получения таких данных требовались дорогостоящие аппаратные анализаторы. Однако такой тип анализа на базе персональных компьютеров требует наличия определенных моделей сетевых плат и драйверов, так что реализация этой функции может ограничить возможности вашей платформы.
- Анализаторы могут помочь вам корректно настроить новый коммутатор, отображая данные о распределении сетевой нагрузки между устройствами. Кроме того, инструментальные средства, подобные Observer, помогают определить причины, по которым существующий коммутатор демонстрирует неприемлемую производительность.
- Режим показа предыстории производительности позволяет узнать, в какой момент времени изменение или реконфигурация сети оказала негативное воздействие на пропускную способность сети, для чего производится ранжирование пропускной способности сегмента. Эта возможность полезна и перед обновлением, и после него.
- Анализатор помогает найти поврежденный концентратор или сетевую плату, выявляя те сетевые станции, которые характеризуются избыточными повторными передачами.

Подключение автономного анализатора

На первом этапе использования портативного анализатора протоколов его нужно физически подключить к сети, которую вы намерены тестировать, и корректно выполнить настройку этого соединения. Анализатор можно подключить к сети в качестве узла или сделать так, чтобы он осуществлял мониторинг трафика между узлами. Соединение и конфигурация, которую вы выберете, зависит не только от того, какие тесты вы собираетесь проводить, но и от физического окружения (концентраторы или коммутаторы). Концентратор (Hub) передает любой пакет, прибывающий на один из его портов, во все другие свои порты. Это означает, что все узлы, подключенные к концентратору, могут прослушивать друг друга. Для сравнения, коммутаторы способны определять местоположение узлов в сети путем связывания физических адресов узлов и сегментов сети, где они установлены, а затем перенаправлять или фильтровать пакеты, в зависимости от адреса назначения. Когда пакет поступает на коммутатор, тот сравнивает физические адреса источника и приемника, участвующие в диалоге, и изолирует этот диалог от остальных портов коммутатора.

Следовательно, управление коммутаторами (Switch) и их мониторинг часто связан с трудностями. Одна из наиболее серьезных проблем при тестировании коммутируемой сети заключается в динамическом изменении моделей трафика — коммутатор открывает и закрывает порты в зависимости от трафика. При подключении анализатора к сети вы должны принимать во внимание это обстоятельство. К примеру, если вы подключаете и настраиваете анализатор в качестве узла в коммутируемой среде, вы не сможете просматривать весь трафик, хотя в других условиях вы могли бы на это рассчитывать. Так как все остальные элементы сети не будут подозревать о существовании анализатора, ему не будет приходить никакого специального трафика, а коммутатор будет блокировать физический порт, к которому анализатор будет подключен. Единственным видом трафика, который такой анализатор сможет захватывать, является широковещательный трафик.

Прежде чем подключать анализатор, нужно принять во внимание окружение, в котором он будет установлен — среда может быть построена вокруг концентратора или вокруг коммутатора. При подключении анализатора к коммутируемой среде его разумно установить и настроить в качестве монитора — так анализатор сможет фиксировать весь трафик, проходящий между определенным коммутатором и сервером/рабочей станцией. При подключении анализатора к среде концентратора его имеет смысл установить и настроить в качестве узла — в результате анализатор сможет фиксировать весь трафик, направленный во все порты концентратора.

Подключение в качестве узла

Узловое соединение (иногда его называют двухточечным) предполагает простое подключение порта анализатора к свободному порту на концентраторе или коммутаторе, но применяется оно, в основном, в окружении концентратора. Такое соединение позволяет анализатору выполнять функцию узла — независимой точки сети. В этом случае анализатор рассматривает трафик, проходящий через концентратор, точно таким же образом, каким его рассматривает любой другой узел сети Ethernet. При этом соединении анализатор подключен непосредственно к порту концентратора, причем это подключение производится через кабель RJ-45 100BaseT (его макси-

мальная длина составляет 100 метров). Анализатор осуществляет мониторинг трафика всех станций, подключенных к тому же самому концентратору (и проблемному домену). Помимо прочего, такая схема позволяет анализатору генерировать сетевой трафик. Узловые соединения предоставляют анализатору возможность работать в полудуплексном или полнодуплексном режиме. Полудуплексный режим обычно используется в 10-мегабитовых средах Ethernet, где узел анализатора выполняет операции отправки и получения разновременно. Полнодуплексный режим чаще всего используется в средах Fast Ethernet, в которых каналы отправки и получения имеют возможность одновременной передачи — результирующая пропускная способность при этом равна 200 Мбит/с.

Подключение в качестве монитора

Режим монитора (иногда его также называют линейным, или проходным режимом) обычно используется в коммутируемой среде, когда анализатор устанавливается в линию между портом коммутатора и сервером (или сегментом сервера). На практике, коммутатор обычно подключают напрямую к серверу через кроссоверный (Crossover) кабель. Чтобы установить анализатор между сервером и коммутатором, отключите этот кабель от сервера и подключите сервер к узловому порту анализатора[1]. Затем подключите кроссоверный кабель, отходящий от коммутатора, к коммутационному порту анализатора. Данный режим подходит как для Ethernet с пропускной способностью 10 Мбит/с, так и для Fast Ethernet с пропускной способностью 100 Мбит/с. Имейте в виду, что вариант применения анализатора в режиме монитора связан со следующими ограничениями.

- Режим монитора обычно не позволяет анализатору генерировать трафик.
- Режим монитора предусматривает полнодуплексный мониторинг с захватом трафика, проходящего с коммутатора на сервер и с сервера на коммутатор.
- Всегда пользуйтесь существующим кабелем, проведенным между сервером и коммутатором. Этот кабель может быть как кроссоверным, так и проходным — в зависимости от конкретного оборудования. В дополнение к существующему кабелю всегда должен присутствовать второй кабель, причем обязательно проходной — это делается для того, чтобы сигналы не подвергались случайному инвертированию.
- При работе в режиме монитора анализатор не осуществляет регенерацию сигнала — таким образом, суммарная длина обоих кабелей не должна превышать 100 м.
- В случаях, когда питание анализатора отключено, соединение между коммутатором и сервером, как правило, сохраняется.

В коммутируемой оптоволоконной среде коммутатор обычно подключается напрямую к серверу, причем для этого используется оптоволоконный кабель. Тем не менее вам все равно придется установить анализатор на линии, соединяющей сервер с коммутатором. Как и в случае с кабелями RJ-45, в такой ситуации вы должны отключить оптоволоконный кабель от сервера и подключить его к узловому порту анализатора. Иногда встречаются устройства с коннекторами типа ST или SC, так

[1] С помощью другого кабеля. — *Ред.*

что вы должны быть уверены в том, что модуль вашего анализатора можно подключить к проведенному кабелю.

Применение анализатора

Теперь, когда вы имеете некоторое представление о том, что такое анализаторы протоколов и как они работают, самое время рассмотреть вопросы их практического применения в ситуациях, требующих проведения базовых процедур поиска неисправностей. В этой главе мы будем работать с многофункциональным продуктом Observer Suite от компании Network Instruments. Не забывайте, что разные анализаторы протоколов значительно отличаются друг от друга по своим функциям и производительности, так что за дополнительными подробностями и методами эксплуатации вы должны обращаться к документации по конкретному продукту.

Диагностика в реальном времени

Естественно, вы можете сразу приступить к захвату пакетов и их анализу, однако в большинстве анализаторов протоколов предусмотрены специальные комплекты инструментов, которые применяются для диагностики сетевых проблем в режиме реального времени. Во многих случаях разумно начать именно с этих инструментальных средств — они помогают получить представление о комплексном воздействии существующей проблемы, а затем, при необходимости, приступить к захвату пакетов и их анализу, выделению конкретных проблем, исходя из блоков трафика.

Обнаружение сетевых имен

Режим обнаружения сетевых имен (**Discover Network Names**) предусматривает захват всех сетевых адресов, расположенных в локальном сегменте, их сохранение в таблице фильтрации и последующее присвоение им псевдонимов. Эта функция позволяет вам в точности определить, какие станции присутствуют в данной сети, и оказывается полезной в ситуациях, когда какая-то одна станция становится недоступной, а также когда вы проверяете, способна ли недавно подключенная станция отвечать. Сетевому адресу можно присвоить имя; с другой стороны, вы можете пользоваться IP-адресами, именами DNS, именами регистрации NetWare или именами сетевой регистрации Microsoft. После сохранения сетевых имен их можно задействовать во всех совершаемых запросах. Знание сетевых имен часто помогает техническим специалистам в деле выявления проблемных рабочих станций или других сетевых устройств. Если вам не удается напрямую обнаружить группу сетевых имен, имейте в виду, что Observer позволяет импортировать в таблицу адресов список этих адресов. Для этого вы должны щелкнуть на пиктограмме **Discover Network Names** (Обнаружение сетевых имен) на панели инструментов Observer — в результате на экране появится диалоговое окно, показанное на рис. 30.8. Запустите процесс обнаружения и не препятствуйте его выполнению. В это время вы увидите, как таблица будет заполняться, а цикл — продолжаться. Как только режим **Discover Network Names** завершит процесс активного обнаружения, Observer перейдет к пассивному "прослушиванию" локальной сети, в ходе которого он будет записывать все зафиксированные сетевые адреса.

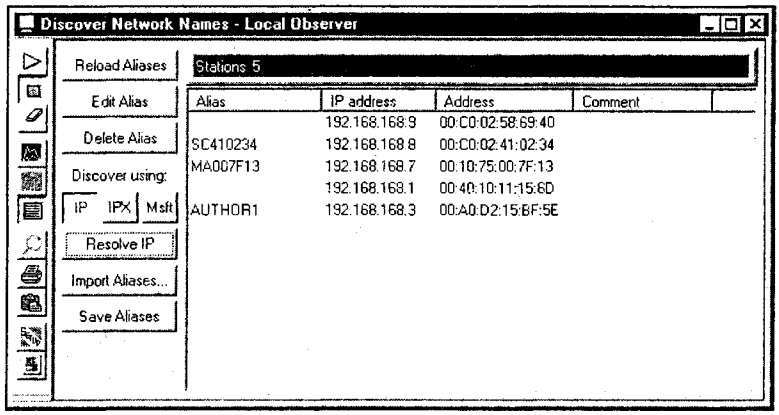


Рис. 30.8. Обнаружение сетевых имен с целью нахождения сетевых станций, а также соответствующих им обозначений IP, MAC и псевдонимов

Режим **Discover Network Names** автоматически присваивает найденным сетевым адресам псевдонимы; для этого есть три метода: **IP**, **IPX** и **Microsoft** (**Msft**). Режимом по умолчанию является **IP**. В этом режиме Observer сначала дважды пытается средствами ARP провести разрешение всех адресов в рамках указанного вами IP-адреса, а затем приступает к прослушиванию на предмет любых дополнительных аппаратных адресов, которые могут обнаружиться с течением времени. Находясь в режиме **IPX**, Observer запрашивает все локальные серверы NetWare и запрашивает у сервера регистрационное имя NetWare, соответствующее каждому аппаратному адресу, обнаруженному в пределах локального сегмента. Это делается путем создания пакетов IPX и регистрации на сервере в качестве администратора. Прежде чем Observer приступит к опросу сервера, вы должны будете вести административный пароль NetWare. При нахождении в режиме **Microsoft** (**Msft**) Observer осуществляет пассивное прослушивание на предмет прохождения пакетов; при этом он может обнаруживать исключительно имена NetBIOS/NetBEUI в ходе их широковещания в локальной сети. Для того чтобы сформировать псевдонимы для всех имен в локальной сети, может потребоваться от пяти минут до многих часов.

Уровень использования пропускной способности

Если вы хотите измерить объем пропускной способности, потребляемый данным сегментом сети, воспользуйтесь функцией **Bandwidth Utilization** (уровень использования пропускной способности). Неожиданная нехватка пропускной способности может свидетельствовать об избыточном трафике (в этом случае требуется модернизация) и приводить к выполнению сетевой платой повторных передач. Уровень использования пропускной способности подсчитывается путем фиксации количества байт, отправленных анализатором Observer (или проверочной станцией) за период времени продолжительностью в 1 секунду. Затем это значение корректируется путем прибавления к размерам данных соответствующих заголовков и завершителей MAC. После этого получившийся объем данных сравнивается с теоретической максимальной пропускной способностью, поддерживаемой драйвером сетевой платы (она может равняться 10/100/1000 Мбит/с — в зависимости от того, о какой величине со-

общает сама сетевая плата); наконец, на график выводятся статистические данные, выражающие процентное отношение.

Чтобы измерить уровень использования пропускной способности, нажмите кнопку **Bandwidth Utilization (BU)**, расположенную на панели инструментов Observer. В результате на экране появится диалоговое окно **Bandwidth Utilization** (рис. 30.9). На представленном в этом окне графике будет показан текущий уровень использования пропускной способности, а также максимальное, среднее и последнее значения этого показателя.

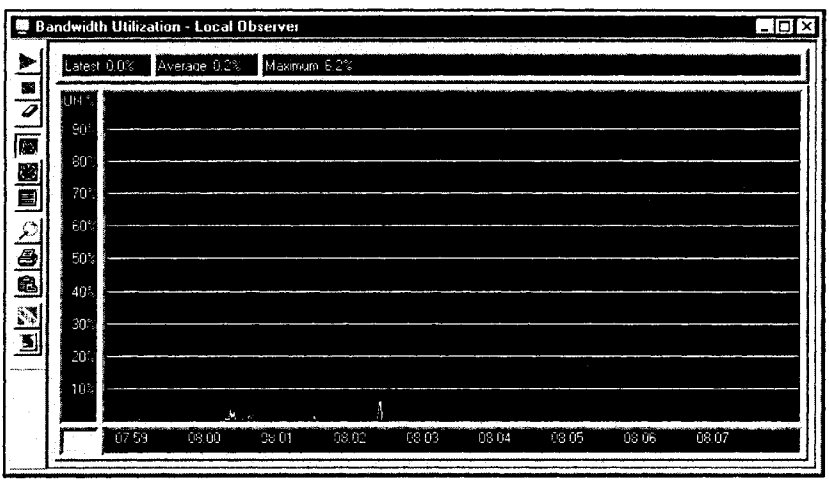


Рис. 30.9. Уровень использования пропускной способности может свидетельствовать об избыточности трафика — этот показатель заблаговременно предупреждает о сетевых проблемах и необходимости модернизации

Сетевая активность

Индикатор **Network Activity Display** (индикатор сетевой активности) демонстрирует критический уровень использования сети и данные о широковещании в виде графика трафика (пакетов/с) и процентного показателя уровня использования. Из этого индикатора можно почерпнуть данные об общем состоянии локальной сети; кроме того, на нем могут появляться предупреждения о предстоящих замедлениях в результате широковещательных или многоадресных штормов. Для того чтобы проверить сетевую активность, нажмите кнопку **Network Activity Display (NAD)**, расположенную на панели инструментов Observer; в результате на экране появится диалоговое окно **Network Activity Display** (рис. 30.10). На графике демонстрируется уровень широковещания и многоадресного вещания, средний и максимальный уровни использования. Чрезмерный объем широковещания может свидетельствовать о неисправности сетевой интерфейсной платы одной из станций.

Основные показатели сети

Режим **Network Vital Signs** (Основные показатели сети) анализатора Observer демонстрирует текущую активность локальной сети (пакеты в секунду и процентный по-

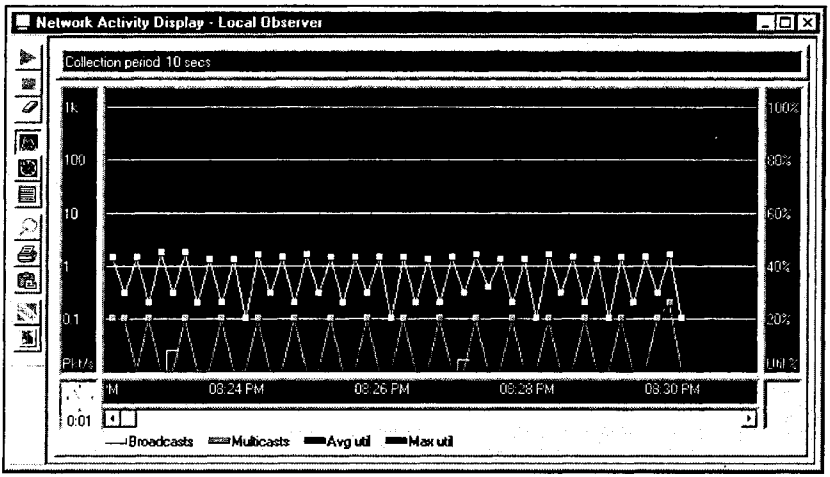


Рис. 30.10. Индикатор сетевой активности оперативно отчитывается об уровне использования сети и широковещательной/многоадресной активности

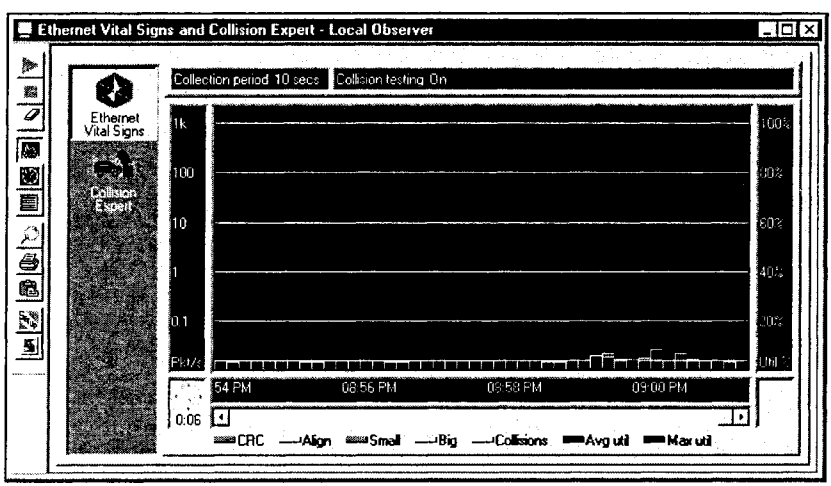


Рис. 30.11. В режиме основных показателей сети оперативно обозначаются простые сбойные ситуации, возникающие во время прохождения сетевого трафика

казатель уровня использования), отображаемую по отношению к текущему состоянию ошибок — например, ошибок CRC, выравнивания, слишком малых и слишком крупных кадров, конфликтам, среднему и высокому уровням использования. Чтобы перейти в режим **Network Vital Signs** (NVS), щелкните на соответствующей пиктограмме, расположенной на панели инструментов Observer, — в результате на экране появится график основных показателей сети (рис. 30.11). На этом индикаторе выводится комплексный снимок сбойных состояний, а также уровень этих состояний в сравнении с текущей активностью локальной сети. Уровень сбойных ситуаций

важен с точки зрения определения строгости конкретной ошибки. К примеру, 50-процентный уровень пакетных ошибок, выявленный посредством контроля CRC, не является проблемой, если численность выборки (общая активность) составляет всего два пакета. С другой стороны, 10-процентный уровень пакетных ошибок во время загруженного трафиком периода свидетельствует о критической проблеме.

Сетевые ошибки на станциях

Если индикатор **Network Vital Signs** указывает на наличие ошибок, переходите в режим сетевых ошибок по станциям (**Network Errors by Station**) — он позволяет классифицировать ошибочные пакеты Ethernet по источникам (станциям) ошибок, а также по типам ошибочных пакетов. Чтобы просмотреть сетевые ошибки, щелкните на пиктограмме **Network Errors by Station (NES)** — в результате на экране появится диалоговое окно **Network Errors by Station** (за помощью о методах исправления каждого из возможных типов ошибок обращайтесь к разделу, посвященному *поиску неисправностей, далее в этой главе*). В этом диалоговом окне содержится подробный отчет о каждой станции-нарушителе; в числе прочих в нем указываются следующие характеристики станции:

- **Alias** (псевдоним);
- **IP Address** (IP-адрес);
- **Address** (адрес);
- **Errors** (ошибки);
- **CRC** (ошибки контроля при помощи циклического избыточного кода);
- **Alignment** (выравнивание);
- **Too Small** (слишком малый размер);
- **Packets** (пакеты);
- **% Errors** (процент ошибок);
- **Errors/sec** (количество ошибок в секунду);
- **CRC/sec** (количество ошибок контроля CRC в секунду);
- **Alignment/sec** (выравниваний в секунду);
- **Too Small/sec** (пакетов слишком малого размера в секунду);
- **Packets/sec** (пакетов в секунду).

Примечание

Способность Observer к отслеживанию ошибок Ethernet по отдельным станциям предполагает применение драйвера Network Instruments ErrorTrak и сертифицированной сетевой интерфейсной платы. Другие анализаторы протоколов могут налагать другие ограничения.

Распределение по протоколам

Режим распределения по протоколам (**Protocol Distribution**) отражает разделение данных в локальной сети по отдельным протоколам, которые могут быть представ-

лены в виде списка или графика. Обследование протоколов дает вам возможность сформировать представление о различных задействованных серверах и приложениях и понять, есть ли в локальной сети какие-либо неизвестные или неверно настроенные протоколы. Для того чтобы ознакомиться с распределением по протоколам, щелкните на пиктограмме **Protocol Distribution (PD)**, расположенной на панели инструментов Observer — в результате на экране появится диалоговое окно **Protocol Distribution** (рис. 30.12). В режиме **All** это диалоговое окно содержит перечисление всех протоколов, чьи данные проходят через сеть; в то же время, у вас есть возможность выбрать только протоколы **IP** или **IPX**.

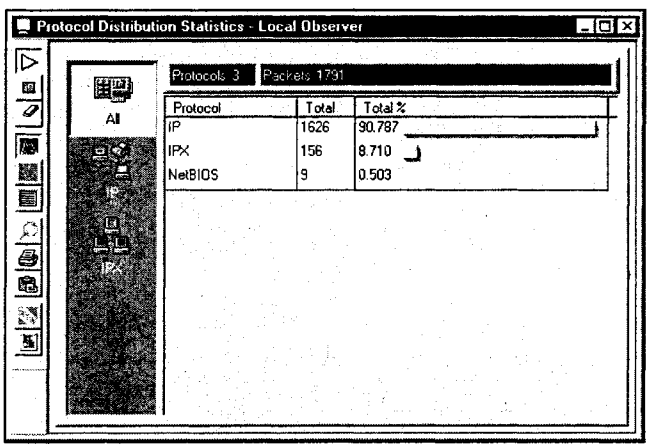
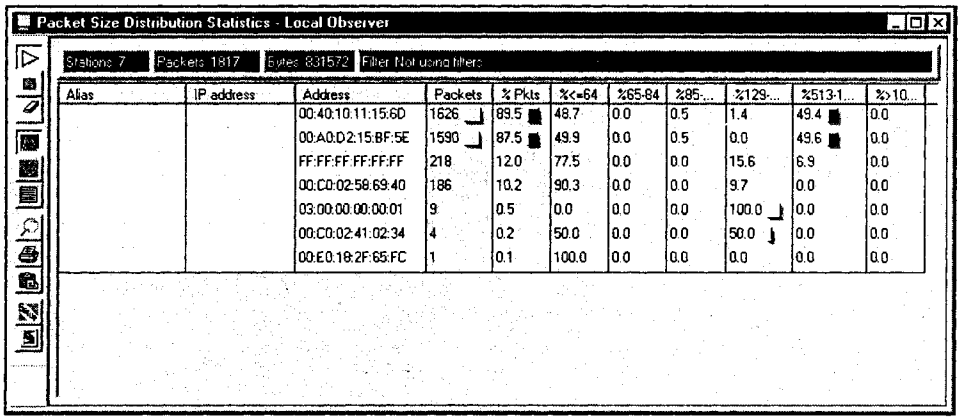


Рис. 30.12. Исходя из распределения по протоколам, вы можете быстро определить, какие сетевые станции настроены некорректно (т. е. пользуются неверным протоколом)

Распределение по размеру пакетов

Статистические данные, связанные с распределением по размеру пакетов (**Packet Size Distribution Statistics**), отражают модели трафика каждой станции локальной сети, классифицированные по размеру пакетов. Подобного рода информация помогает выявить проблемы, имеющие отношение к сетевому потоку. К примеру, вы можете без труда определить станции или маршрутизаторы, отправляющие по преимуществу небольшие пакеты, и, напротив, станции или маршрутизаторы, которые, в основном, отправляют крупные пакеты. По умолчанию здесь приводятся все станции, которые расположены в пределах локальной сети (это нефильтрованный трафик), но для того чтобы выделить размеры пакетов, относящиеся к определенным станциям источника или назначения, вы можете задействовать фильтры. Чтобы открыть диалоговое окно со статистическими данными, нужно щелкнуть на пиктограмме **Packet Size Distribution Statistics (SDS)**, расположенной на панели инструментов Observer (рис. 30.13). На этом индикаторе указано процентное распределение пакетов, попадающих в каждый из диапазонов — эти данные выводятся в виде списка или графика. Первая запись на рис. 30.13 гласит, что станция с MAC-адресом 00:40:10:11:15:6D отправила 1626 пакетов, причем размер 48,7% этих пакетов меньше 64 байт, а размер 49,4% находится в диапазоне от 512 до 1024 байт.



Alias	IP address	Address	Packets	% Pkts	%<=64	%65-84	%85-...	%129-...	%513-1...	%>10...
		00:40:10:11:15:6D	1626	89.5	48.7	0.0	0.5	1.4	49.4	0.0
		00:A0:D2:15:BF:5E	1590	87.5	49.9	0.0	0.5	0.0	49.6	0.0
		FF:FF:FF:FF:FF:FF	218	12.0	77.5	0.0	0.0	15.6	6.9	0.0
		00:C0:02:58:69:40	186	10.2	90.3	0.0	0.0	9.7	0.0	0.0
		03:00:00:00:00:01	9	0.5	0.0	0.0	0.0	100.0	0.0	0.0
		00:C0:02:41:02:34	4	0.2	50.0	0.0	0.0	50.0	0.0	0.0
		00:E0:18:2F:65:FC	1	0.1	100.0	0.0	0.0	0.0	0.0	0.0

Рис. 30.13. Исходя из распределения по размеру пакетов, вы можете быстро определить, какие станции генерируют пакеты неверного размера

Захват и анализ пакетов

Теперь, когда вы ознакомились с некоторыми диагностическими средствами, которые присутствуют во многих анализаторах, самое время рассмотреть основную функцию анализатора пакетов — захват и анализ пакетов. Режим **Packet Capture** (Захват пакетов) обеспечивает захват трафика локальной сети и хранит данные для их последующего просмотра в окне расшифровки. Кроме того, режим захвата пакетов можно задействовать для просмотра отдельных пакетов в ходе сетевого диалога (но вы должны отдавать себе отчет в том, какие аспекты безопасности связаны с просмотром отдельных пакетов данных). Как правило, изучив отправленную информацию и конкретный ответ, вы формируете четкое представление о сущности проблемы или неверного обмена данными.

После захвата пакетов их можно просматривать и анализировать — для этого существуют формы списка и графика. Функции анализа применимы к действующим операциям захвата (к захватам в реальном времени, когда Observer захватывает и сохраняет трафик, проходящий в локальном сегменте, или пользуется зондом для захвата и сохранения данных в удаленном сегменте). Кроме того, возможен анализ сохраненных буферных файлов (когда локальная копия Observer применяется для исследования и анализа пакетов, захваченных любой другой копией Observer). Чтобы перейти в режим захвата и анализа пакетов, щелкните на пиктограмме **Packet Capture (PC)**, расположенной на панели инструментов Observer. В результате на экране появится диалоговое окно **Packet Capture**. Для указания параметров захвата (например, размера буфера или других опций) воспользуйтесь функцией Setup; после этого запустите захват (см. рис. 30.1). В диалоговом окне будут приведены данные о количестве захваченных пакетов и объеме занятого буферного пространства. Кроме того, в этом графике отслеживается общее количество пакетов, количество захваченных и выброшенных пакетов. Захват прекращается в момент заполнения буфера — впрочем, вы можете остановить его вручную.

Примечание

Не забывайте, что выброшенные пакеты знаменуют сбойную ситуацию. В случае наблюдения выброшенных пакетов вам следует обследовать сетевое оборудование на предмет наличия неисправностей, а также проверить, соответствуют ли вычислительные возможности хост-компьютера минимальным требованиям, которые предъявляет ваш анализатор протоколов.

Расшифровка буфера с захваченными пакетами, исследование и подробный анализ пакетных диалогов — все это производится в рамках компонента **Decode and Analysis** (Расшифровка и анализ) режима **Packet Capture** (Захват пакетов). Observer позволяет анализировать содержимое буфера захвата на предмет протоколов, основных источников сообщений, парных диалогов и т. п. Компонент **Collision Expert** (Эксперт коллизий) позволяет знакомиться с основными показателями сети Ethernet, а также проводить испытания на предмет коллизий, которые могут обуславливаться наличием в каком-либо пункте сети некорректно работающей сетевой платы. Для того чтобы запустить анализ, щелкните на пиктограмме **View** (просмотр), расположенной в диалоговом окне **Capture** (Захват) — так вы сможете вызвать окно анализа.

Поиск неисправностей с помощью экспертного анализа

Одно из ограничений, связанных со старыми моделями анализаторов протоколов, заключается в том, что в них необработанные данные почти (или совсем) не интерпретировались. Однако современные анализаторы протоколов, подобные Observer от компании Network Instruments, имеют возможность вывода сводки, содержащей анализ ошибок и отчет. Чтобы вывести список ошибок (если таковые зафиксированы), перейдите на вкладку **Expert Analysis** (Экспертный анализ). В этой части главы объясняются ошибки, которые фиксируются анализаторами протоколов чаще всего, и выдвигаются некоторые предложения по корректирующим действиям.

Ошибки выравнивания

Ошибки выравнивания (Alignment Errors) (которые иногда называют ошибками выравнивания Ethernet) проявляются в том случае, если пакет не выровнен по границе периода передачи. В целях синхронизации сетевая плата формирует и отправляет преамбулу, предваряющую пакеты Ethernet. Таймеры отправляющего и принимающего адаптеров синхронизируют фазы тактирования и вычисляют положение фазы для выдачи начала фактического пакета. Положение фазы задействуется для того, чтобы принимающий адаптер смог узнать, когда пакет начинается и каким образом он должен согласовываться с фактическим сигналом.

Появление ошибок выравнивания обуславливается несколькими факторами. Как правило, они являются результатом предшествующих коллизий. Если коллизия происходит во время передачи (после преамбулы), то положение результирующего сигнала относительно периода этого сигнала оказывается неправильным — принимающая сетевая плата подтверждает это обстоятельство, и пакет отбрасывается. Кроме того, к ошибкам выравнивания может приводить дефект кабеля, соединяющего станцию с концентратором/коммутатором, его чрезмерная протяженность (или электрические помехи, оказывающие воздействие на кабель), а также дефект сетевой платы Ethernet или соединения с маршрутизатором.

Неверная контрольная сумма IP

Контрольные суммы (Checksum) и контроль при помощи циклического избыточного кода (CRC) — это методы проверки целостности данных, суть которых заключается в вычислении дополнительных разрядов и их передаче вместе с данными. Получатель задействует аналогичный алгоритм для перевычисления этой дополнительной информации, и проверяет ее правильность. Неверная контрольная сумма IP получается в такой ситуации, когда пакет, сгенерированный сетевой платой, кажется верным, но его секция протокола оказывается поврежденной. Контрольная сумма MAC-уровня предусматривает отвержение пакета; в то же время неверная контрольная сумма IP обрабатывается стеком и передается соответствующему приложению IP. Причины формирования неверных контрольных сумм IP разнообразны — это может быть неисправная сетевая плата источника передачи, поврежденный кабель или коннектор, через который проходит маршрут передачи, или дефектный драйвер TCP/IP, или программа обработки протоколов на источнике. Отключите станцию-нарушителя от сети, проверьте кабель и сетевую плату (если она неисправна, замените ее), переустановите драйверы протоколов или программное обеспечение, предназначенное для их обработки.

Широковещательный/многоадресный шторм

Широковещательным штормом (Broadcast Storm) (или штормом данных) называется избыточная сетевая передача широковещательного трафика. Это происходит тогда, когда широковещательное сообщение, проходящее по сети, инициирует большое количество ответов, каждый из которых, в свою очередь, вызывает появление еще большего количества ответов — в результате получается эффект снежного кома. Если сетевой трафик приближается к 100 процентам возможной пропускной способности, он полностью блокируется. Широковещательные штормы часто обуславливаются повреждениями сетевых плат или кабеля; такая плата (кабель) наводняет сеть пакетами. К примеру, если сетевая плата повторяет один и тот же ARP-запрос при частоте несколько сотен раз в секунду, существует вероятность, что эти запросы будут распространяться по сети другими устройствами. Чтобы оперативно избавиться от подобного рода трудности, необходимо выявить и отключить компьютер-нарушитель от сети, заменить его плату Ethernet, или проверить сетевой кабель на предмет разрывов, загибов, неплотно зафиксированных коннекторов, и при необходимости внести все необходимые исправления. Помимо этого, появление широковещательных штормов может быть вызвано неверно настроенными серверами или устройствами NetBIOS/NetBEUI. Кроме того, широковещательный шторм может возникнуть между маршрутизаторами в том случае, если широковещательный пакет перенаправляется большее число раз, чем должен. Широковещательное сообщение будет отброшено, когда счетчик числа его транзитов достигнет нуля, но может переполнять каналы глобальной сети, пока этого не случится.

Коллизии

Сети Ethernet работают по принципу множественного доступа с контролем несущей и обнаружением коллизий (CSMA/CD), и поэтому, прежде чем произвести операцию отправки, станция прослушивает кабель на предмет наличия другого трафика. В случае, если другие станции не занимаются отправкой, данная станция получает возможность отправить свой пакет. В противном случае она должна подождать, и через некоторое время выполнить операцию контроля несущей частоты повторно.

В периоды интенсивного трафика в ожидании возможности отправки данных может находиться несколько станций. Если две (или несколько) таких станций проведут операцию контроля несущей одновременно, они могут в одно и то же время принять решения об отправке данных. В таком случае произойдет коллизия (Collision) (при этом может произойти ошибка выравнивания, ошибка контроля CRC, или и то и другое — в зависимости от временных характеристик).

При относительно низких уровнях использования сети (обычно — при 5 процентах сетевого трафика) конфликты представляются естественным и приемлемым элементом любой сети Ethernet. Чем интенсивнее трафик в сети, тем больше может возникнуть коллизий, но избыточные коллизии способны ввести сеть в состояние бездействия. Конфликты часто обуславливаются неисправностью сетевого адаптера или перегрузкой сегмента сети. В случае их возникновения следует отключить от линии станции-нарушители и протестировать их сетевые платы. Неисправные сетевые платы необходимо заменить. Если же плата работает без ошибок, обычно лучшим выходом является ее замена на более производительную плату (например, с 10BaseT до 100BaseT), или проведение сегментации сети.

Дублирование IP-адресов

Такая ошибка появляется в том случае, если два устройства обладают идентичными IP-адресами, но видны как разные аппаратные устройства (MAC-адреса) сети. Дублированные IP-адреса часто встречаются при сочетании статических IP-адресов с применением службы DHCP без ограничения диапазона таблицы адресов DHCP-сервера. К примеру, может случиться так, что пользователь назначит себе IP-адрес, не связавшись с администратором. В таком случае одну из станций-нарушителей нужно будет перенастроить на применение незанятого IP-адреса (или DHCP). В других случаях причина может заключаться в том, что новое устройство установлено в локальную сеть без должной настройки — соответственно, настройку следует провести.

Ошибки контроля CRC в сетях Ethernet

Есть два типа ошибок Ethernet CRC, о которых вы должны знать, — это ошибки CRC кадров MAC и ошибки CRC внутренних протоколов. Ошибки CRC кадров MAC распространены в наибольшей степени — именно их имеют в виду большинство устройств и анализаторов, сообщая о выявлении ошибки CRC. Пакеты Ethernet инкапсулируются в кадр MAC, содержащий преамбулу и данные проверки CRC после упаковки. Сетевая плата Ethernet отправляющей станции несет ответственность за создание преамбулы, размещение данных пакета (включая адресацию, протокол, данные и т. д.), подсчет контрольной суммы CRC и ее вставку в конец пакета. Принимающая станция проверяет контрольную сумму и определяет, остался ли пакет в неизменном состоянии. Если контрольная сумма некорректна, пакет, скорее всего, поврежден и отбрасывается.

Появление ошибок кадров MAC обуславливается несколькими факторами. Обычно они возникают в результате повреждения кабеля или коллизии. Если кабельное соединение сетевой платы Ethernet или концентратора повреждено, электрический контакт вибрирует, многократно замыкаясь и размыкаясь в ходе передачи — это "дрожание" может оборвать части передачи и повредить сигнал. Если коллизия происходит во время передачи пакета, сигнал, соответствующий этому пакету, прерыва-

ется, и получаемый результирующий пакет оказывается поврежденным. Если во время передачи сигнал прерывается частично, то контрольная сумма CRC, вычисляемая сетевой платой, оказывается недействительной, пакет маркируется флагом ошибки CRC и отвергается. Имейте в виду, что в загруженных сетях ошибки CRC не являются редкостью, и лишь незначительная часть из них не свидетельствует о возникновении какой-либо сетевой проблемы. Если процентный показатель ошибок CRC высок, или если одна из станций демонстрирует особо большое количество ошибок CRC, то в кабеле, сетевой плате или порте концентратора/коммутатора может существовать проблема, на которую вам следует обратить внимание.

Другой тип ошибок CRC, который нужно иметь в виду, — это ошибки CRC внутренних протоколов. Некоторые протоколы (например, TCP/IP) предполагают наличие второй контрольной суммы, которая используется для обеспечения целостности данных (в дополнение к контрольной сумме CRC MAC-кадра). Эта вторая контрольная сумма вычисляется для части внутренних данных каждого пакета — с ее помощью выполняется вторая, независимая проверка целостности пакета. Анализатор протоколов подсчитывает эту контрольную сумму самостоятельно и выводит результаты на индикатор анализа протоколов. Ошибки CRC подобного рода крайне редки — они могут быть вызваны некорректно функционирующим программным обеспечением или драйверами протокола.

Недостижимость пункта назначения ICMP

Если сеть, обозначенная в поле пункта назначения дейтаграммы Интернета, недостижима на основе содержимого таблиц маршрутов маршрутизатора или шлюза (т. е. расстояние до сети назначения приравнивается к бесконечности), маршрутизатор или шлюз могут отправить интернет-источнику данной дейтаграммы сообщение о том, что "пункт назначения недостижим" (Destination Unreachable). В некоторых сетях маршрутизатор или шлюз способны определять факт недостижимости пункта назначения Интернета — в таком случае эти устройства могут отсылать источнику сообщение о том, что "хост назначения недостижим". Кроме того, хост назначения отсылает хосту источника сообщение о "недостижимости пункта назначения" в том случае, если IP-модуль пункта назначения не может доставить дейтаграмму по причине неактивности указанного модуля протокола (или порта процесса). Другая возможная причина — для перенаправления дейтаграммы шлюзом ее необходимо фрагментировать, но при этом в дейтаграмме установлен флаг **Don't Fragment** (Запрет на фрагментацию). В таком случае шлюз вынужден отбросить дейтаграмму, сопроводив это действие возвратом сообщения о "недостижимости пункта назначения".

Такие ошибки происходят, если таблицы маршрутов маршрутизатора настроены неверно, пункт назначения не существует, пункт назначения не признан в качестве возможно действительного адреса (т. е. запрещен), или служба, запрошенная в системе назначения, недоступна. Убедитесь в том, что пункт назначения существует и признается действительным адресом; после этого проверьте таблицы маршрутов и, в случае необходимости, обновите их.

Ошибка параметра ICMP

Если маршрутизатор, шлюз или хост, обрабатывающий дейтаграмму, обнаруживает проблему, связанную с параметрами заголовка (и ему не удается завершить обработку дейтаграммы), он вынужден отбросить ее. Часто это обуславливается наличием

в опции неверных параметров. При этом маршрутизатор, шлюз или хост оповещают источник при помощи сообщения "ошибки параметра" (Parameter Problem) — это сообщение отсылается лишь в том случае, если возникшая ошибка привела к сбрасыванию дейтаграммы. Помимо всего прочего, эта ошибка может возникнуть при неисправности стека TCP, сетевой платы или сетевого соединения отправляющей станции. Кроме того, ее можно отнести к сетевому соединению, организуемому поврежденным маршрутизатором или шлюзом (или устройством с неисправным стеком TCP).

Ошибка ICMP "время жизни истекло"

Если маршрутизатор или шлюз, обрабатывающий дейтаграмму, обнаруживает ноль в поле TTL (время жизни), он вынужден сбросить ее. При этом маршрутизатор или шлюз может оповестить источник об ошибке, отправив сообщение об "истечении времени жизни" (Time to Live Exceeded). Если хосту, выполняющему повторную сборку фрагментированной дейтаграммы, из-за отсутствия некоторых фрагментов не удается за определенный срок завершить эту операцию, он также сбрасывает дейтаграмму и (в некоторых случаях) отправляет сообщение об "истечении времени жизни". Такая ошибка часто возникает при наличии проблем с маршрутизацией, когда в таблице маршрутов выявляется неверный маршрут или маршрут, проходящий через такое число транзитов, которое превышает принятое данным хостом максимальное значение. Кроме того, эту проблему можно связать с потерей пакета по вине некорректно функционирующего маршрутизатора, перегруженной сети, или неисправной сетевой платы на хосте или маршрутизаторе.

Ошибка локальной маршрутизации

Трудности в рамках локальной маршрутизации обычно возникают тогда, когда станция, не являющаяся маршрутизатором, пользуется неверной сетевой маской IP и отправляет локальный трафик на маршрутизатор по умолчанию. В таком случае вам следует задействовать на станции, не являющейся маршрутизатором, нужную сетевую маску IP. Кроме того, возможно, проблема заключается в том, что две станции (не маршрутизаторы) пользуются одним и тем же IP-адресом, или в том, что настройки станции, не являющейся маршрутизатором, указывают на неверный шлюз по умолчанию.

Максимальный уровень использования превышен

Эта ошибка может свидетельствовать (а может и не свидетельствовать) о наличии проблемы в сети — возможно, она заключается в том, что уровень использования сети нормален, но высок. Если показатели времени отклика хуже, чем предполагалось, или вам удалось выявить чрезмерный уровень использования, попытайтесь определить источник высокой нагрузки на сеть. Как правило, в качестве источников выступают следующие факторы:

- отдельная станция осуществляет повторную отправку ошибочных пакетов, или ее заклинило на непрекращающемся цикле отправки;
- маршрутизатор или мост ошибочно осуществляет непрерывную отправку данных;
- в рамках одного проблемного домена находится слишком много станций;
- станция или ряд станций осуществляют передачу данных в значительных объемах.

Слишком малые/большие размеры пакетов

В соответствии со спецификацией Ethernet размер всех пакетов должен быть не меньше 64 байт, но не больше чем 1518 байт (включая контрольную сумму). Любой пакет размером менее 64 байт, отправляемый по кабелю, признается "слишком малым" (Too Small), а пакеты, чей размер превышает 1518 байт, маркируются как ошибочные и сбрасываются — иногда их называют сбойными кадрами. И в том и в другом случае проблемы с размером пакетов обычно обуславливаются неисправностями аппаратного обеспечения. Сетевая плата, установленная на станции с высокими показателями ошибок пакетов, подлежит проверке и замене.

Ошибка маршрутизации

Ошибка маршрутизации обычно происходит в случаях, когда станции, не являющиеся маршрутизаторами (их IP-адреса указываются в ошибках), настраиваются на применение неверного шлюза по умолчанию. При необходимости вы должны проверить станцию-нарушителя и перенастроить ее.

Избыточность повторных передач TCP/UDP

Такие ошибки происходят тогда, когда порядковый номер TCP оказывается идентичным предыдущему или меньше него. Это говорит о том, что данный пакет дублирует другой пакет, отправленный ранее. К примеру, это может быть вызвано тем, что станция-отправитель не получила подтверждения приема предыдущего пакета, пакет был утерян, сброшен, или поврежден каким-либо другим образом. Повторные передачи TCP могут обуславливаться тем, что принимающая станция была слишком занята, чтобы ответить отправляющей станции, или тем, что сетевой трафик был настолько высок, что первоначальный пакет оказался утерянным (или, вследствие высокого уровня использования сети, подтверждение не было получено). С другой стороны, маршрутизатор может сбрасывать пакеты (или не переадресовывать их) вследствие собственной занятости или неисправности. Наконец, вполне возможно, вы обнаружите, что перемежающиеся сетевые сбои вызываются дефектом кабеля или повреждением коммутатора/концентратора, результатом чего являются избыточные повторные передачи.

Избыток нулевых окон TCP

Когда станция TCP обменивается информацией с другой станцией, отправка "величины окна" (Window Value) указывает на тот объем данных, который отправляющая станция готова переправить следующим пакетом. Если отправляющая станция объявляет *нулевое окно* (Zero Window), это значит, что в настоящий момент она не может заниматься обработкой дополнительных данных. Нулевые окна появляются тогда, когда система (объявляющая их) оказывается слишком загруженной, не имеющей возможности обрабатывать больше данных. Кроме того, возможен вариант серьезного несоответствия обрабатывающих способностей отправляющей и принимающей станций (например, когда станция 100BaseT пытается подать данные на станцию 10BaseT). В ряде случаев приложение оказывается настолько медленным, что не справляется с потоком данных, приходящих из сети, или пребывает в ожидании другого события. Поинтересуйтесь, нет ли каких-то обновлений или заплат для сетевых приложений, которые могли бы повысить производительность.

Медленное установление соединения TCP/медленная реакция TCP

Медленность соединения или реакции может обуславливаться высокой нагрузкой на сеть. С другой стороны, возможно, что занята или перегружена система, с которой производится соединение, или же само это соединение производится по перегруженному каналу (т. е. перенаправление пакетов тормозится маршрутизатором).

Расшифровка

Страница расшифровки **Decode** (рис. 30.14) позволяет вам перемещаться по буферу захвата и "заглядывать внутрь" каждого содержащегося в нем пакета. Окно **Decode** программы Observer делится на три основных области: область заголовков, область расшифровки и область необработанных данных. В области заголовков приводятся данные об источнике, пункте назначения, типе, сводке, отметке времени и размере каждого пакета. У вас есть возможность быстро прокрутить длинный список захваченных пакетов и выбрать тот, который вам интересен. К примеру, стоит указать на пакет 4, и в окне **Decode** появится его содержимое. Необработанные данные выбранного пакета представлены в нижней части окна. Окно **Decode** интерпретирует пакет и представляет его содержимое в "удобочитаемой" форме. Что касается пакета 4, показанного на рис. 30.14, то в нем содержится преамбула, уровень IP и записи уровня TCP; вы можете развернуть интересующую вас запись (например, **TCP**), и при помощи прокрутки просмотреть ее полное интерпретированное содержимое. Таким способом можно исследовать каждый пакет и провести поиск на предмет

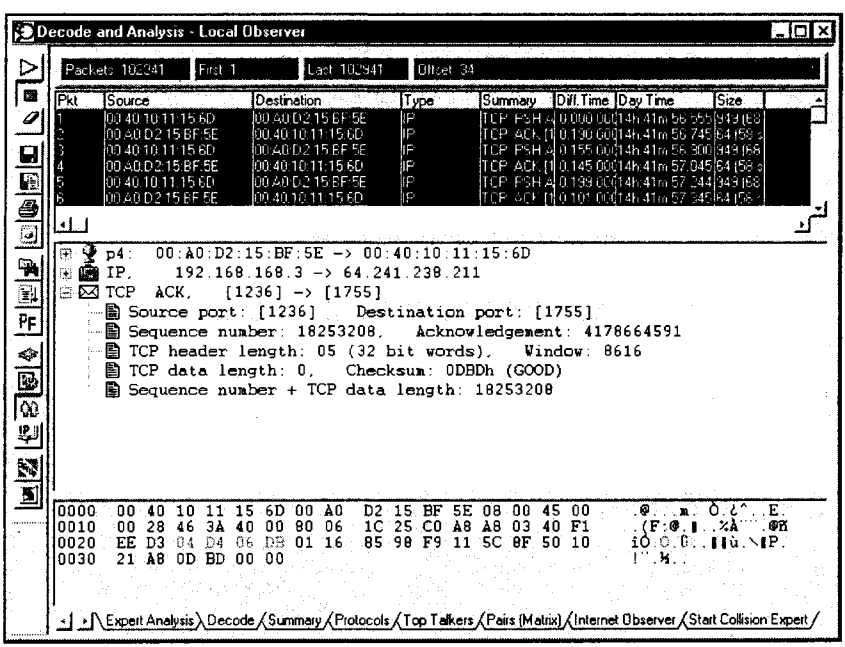


Рис. 30.14. На странице **Decode** отображается подробная информация о каждом пакете, находящемся в буфере захвата

существования каких-либо проблем между станциями или другими сетевыми устройствами. В расшифровке, представленной на рис. 30.14, мы видим, что контрольная сумма TCP 0DBDh является нормальной, а значит, можем утверждать, что данный кадр прибыл в пункт назначения в неповрежденном состоянии.

Эксперт по коллизиям

Анализ коллизий производится в режиме **Collision Expert** (Эксперт по коллизиям) (рис. 30.15). С его помощью выполняется исследование всех станций, находившихся в активном состоянии непосредственно перед, во время и сразу после коллизии. Станции-нарушители (станции, постоянно присутствующие или выполняющие повторную передачу во время коллизии) маркируются и отслеживаются. Здесь демонстрируются десять самых активных инициаторов коллизий в сети, количество пакетов и зафиксированных коллизий, а также процентный показатель коллизий, произошедших по вине десяти наиболее активных инициаторов. Когда одна или несколько станций демонстрируют устойчиво высокие показатели повторных передач примерно в то время, когда происходят коллизии, в логике этих станций обнаруживаются конфликтные события; при этом в итоговой статистике эти станции демонстрируют необычно высокие показатели частоты конфликтов. В области сводки, в которой выводятся эти показатели, также даются рекомендации относительно проверки определенных станций на предмет неисправностей аппаратного обеспечения. Разрешить конфликты помогает замена сетевой платы на станциях-нарушителях; еще один вариант действий — проверка кабелей.

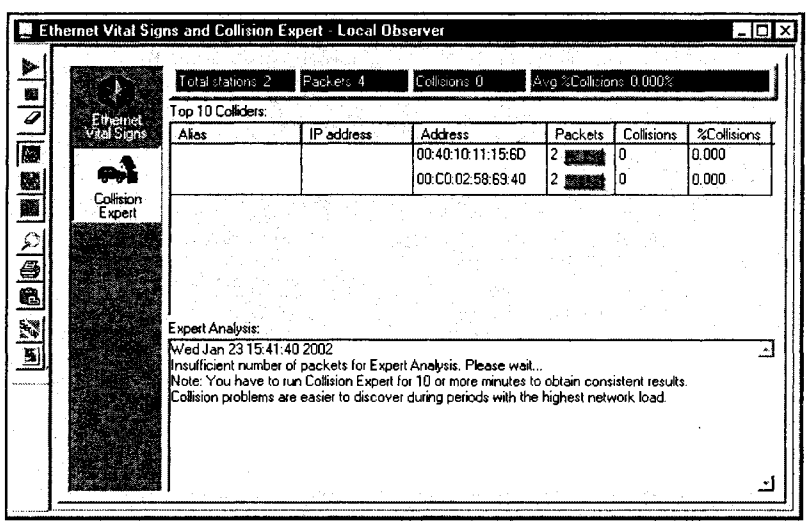


Рис. 30.15. Режим **Collision Expert** анализатора Observer помогает выявить источник избыточных сетевых конфликтов

Динамика соединений

На странице **Connection Dynamics** (Динамика соединений) (рис. 30.16) выводится выбранный диалог с графическим представлением межпакетной задержки (обозна-

чается расстоянием между пакетами). Временные задержки между пакетами даются в графическом представлении, которое позволяет мгновенно выявить длительную задержку и избыточные показатели времени реакции. На индикаторе пакетов может содержаться либо краткое, либо подробное представление содержимого каждого пакета, причем в целях обеспечения оперативной идентификации повторные передачи и случаи потерянных пакетов отмечаются красным цветом. Для того чтобы открыть страницу **Connection Dynamics**, щелкните правой кнопкой мыши на диалоге, показанном в диалоговом окне **TCP Events** (События TCP) или **UDP Events** (События UDP), и выберите пункт меню **Connection Dynamics**. После этого появляется страница **Connection Dynamics**, а в ней выводится весь диалог.

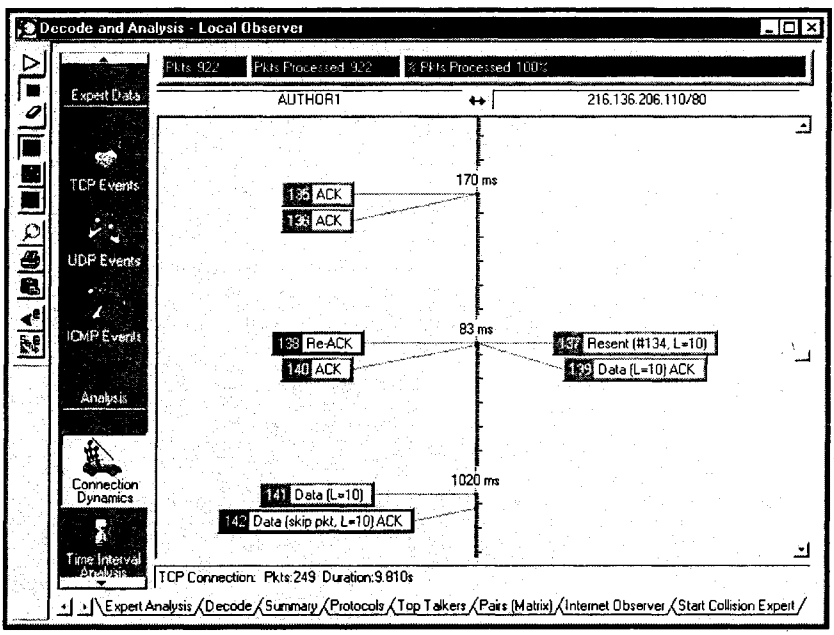


Рис. 30.16. Режим **Connection Dynamics** демонстрирует диалог во всей его полноте; при этом в качестве параметров могут выступать время и состояние пакета

В зависимости от того, какие манипуляции мышью вы проводите, на этой странице может выводиться огромное количество информации. Когда мышь не указывает ни на один пакет, в строке состояния выводится тип диалога, показанного на дисплее (TCP или UDP), продолжительного этого диалога (в секундах) и количество пакетов. Если в программе Observer вы установите указатель мыши на каком-то пакете, этот пакет будет выделен синим цветом. Когда пакет не находится под курсором мыши, его цвет выражает некоторую информацию о пакете. Смысловая нагрузка той или иной окраски пакетов представлена ниже.

- *Серый цвет*. Время отклика является нормальным — с пакетом не связано никаких ошибок.
- *Фиолетовый цвет*. Возможна ошибка. Проблема не обязательно связана с данным соединением, но оно нуждается в дальнейшем исследовании на предмет на-

личия других, более серьезных ошибок — последнее замечание особенно актуально, если фиолетовых пакетов несколько.

- *Красный цвет.* Пакет явно проблемный (возможно, проблема связана с временем реакции, ошибкой CRC, пропущенными пакетами, избыточным количеством повторных передач, или с чем-то другим). После того как анализатор протоколов выявил наличие ошибки, связанной с данным пакетом, администратор должен провести дальнейшее исследование и определить, является ли ошибка временной и случайной, или же она свидетельствует о наличии в сети более серьезной проблемы.

В примере, приведенном на рис. 30.16, пакет 137 (красный) представляет собой повторно отправленный пакет 134. Расшифровав пакет 134, вы обнаружите, что контрольная сумма этого пакета неверна. Тем не менее сводка **Expert Analysis** не содержит указаний на наличие сколько-нибудь серьезных сбойных ситуаций — таким образом, мы можем сделать вывод о том, что дефектный кадр является обычным компонентом функционирования сети Ethernet.

Анализ временных интервалов

Функция **Time Interval Analysis** (Анализ временных интервалов) отображает диалоги **TCP Event** или **UDP Event** в табличном формате, при этом демонстрируемый диалог разделен на временные промежутки, длительность которых задается пользователем.

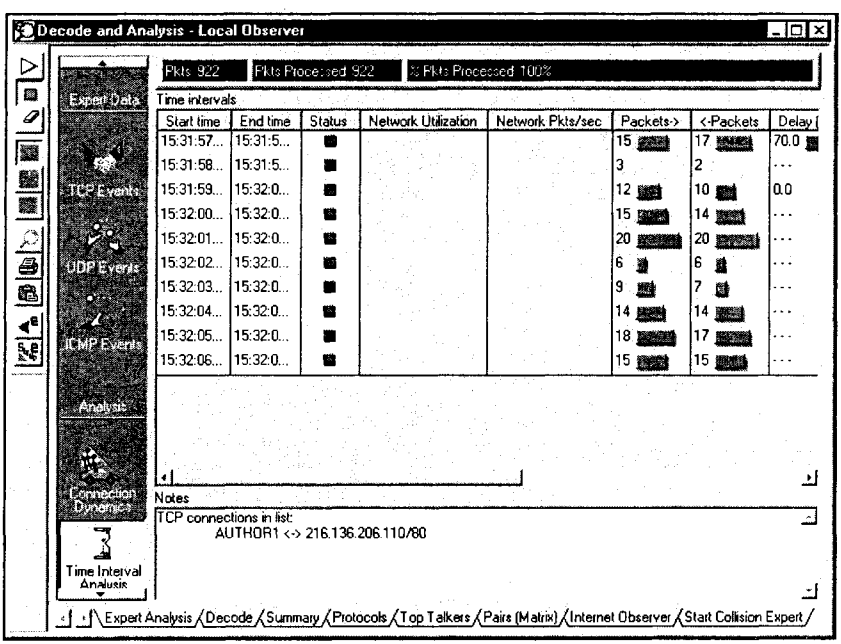


Рис. 30.17. Анализ временных интервалов позволяет вам знакомиться с временной статистикой пакетов, находящихся в буфере захвата, применительно к конкретным диалогам

Чтобы перейти к окну **Time Interval Analysis**, щелкните правой кнопкой на одном из выбранных диалоговых окон **TCP Events** или **UDP Events**, а затем выберите пункт меню **Time Interval Analysis** (рис. 30.17). Для того чтобы определить временной период, щелкните в окне правой кнопкой мыши и выберите пункт **Properties** (Свойства). Среди столбцов таблицы есть **Network Utilization** (Уровень использования сети) и **Network Packets/sec** (Количество сетевых пакетов в секунду), (кроме них, в таблице приводятся данные о количестве пакетов и условиях задержки) — эти параметры помогают определить общие сетевые параметры и наличие ошибок.

Другие индикаторы анализатора

Режим **Analysis** (Анализ) программы Observer позволяет вам получить и другую информацию, связанную с захваченными данными.

- *Сводка.* Страница **Summary** содержит обзор параметров захвата, статистику пакетов и ошибок. Зачастую, прежде чем искать проблемные пакеты, имеет смысл обратиться именно к сводке.
- *Протоколы.* Страница **Protocols** по своему назначению и внешнему виду аналогична статистической функции **Protocol Distribution**, о которой мы говорили ранее. На этой странице присутствует перечень протоколов, применяемых в пакетах, находящихся в буфере захвата, количество отправленных пакетов, а также относительный, процентный показатель их использования. Это позволяет вам быстро выявить случаи неожиданного или неверного применения протоколов.
- *Основные источники сообщений.* По своему внешнему виду и назначению страница **Top Talkers** аналогична функции **Top Talkers**, речь о которой шла ранее. Основные источники сообщений, находящихся в буфере захвата, приводятся вместе с соответствующей статистикой трафика. Таким образом, вы можете без труда выявить станции, испытывающие потребность в более высокой пропускной способности.
- *Пары.* На странице **Pairs (Matrix)** выводится статистика, связанная с тем, как сетевые станции взаимодействуют друг с другом. На индикаторе с круговой шкалой представлена таблица всех диалогов, где толщина линий представляет относительный объем данных, передающихся между каждой из пар. Эта функция обеспечивает графическое представление станций, обменивающихся необычно большими объемами трафика, а также станций, с трудом (или вообще не) взаимодействующих с другими компьютерами сети.
- *Интернет-наблюдатель.* Страница **Internet Observer** позволяет вам изучать интернет-трафик, захваченный в данной локальной сети. Таким способом можно проводить мониторинг общего уровня использования Интернета и сосредоточить свое внимание на отдельной станции или станциях. Кроме того, показатели использования Интернета можно разбить по протоколам (для того, например, чтобы определить, в каких пропорциях интернет-трафик разделяется между Web-доступом и средствами POP-почты). Этот инструмент помогает выявить случаи несанкционированного обращения к Web, а также сформулировать необходимость в дополнительной пропускной способности.

Поиск неисправностей при помощи анализатора

В инфраструктуру сети входят кабели, коннекторы и сетевые платы. В равной степени важен уровень протоколов, который обеспечивает возможность взаимодействия между физическим уровнем, с одной стороны, и более высокоуровневыми приложениями, с другой — он называется канальным уровнем. Большинство проблем, возникающих в сетях (от 80 до 90 процентов), зарождаются на физическом уровне, в рамках интерфейса между физическим и канальным уровнем, или на самом канальном уровне. Многие случаи неэффективной работы сети, обусловленные проблемами на уровнях 1 и 2, маскируются за счет большой пропускной способности, присутствующей в большинстве современных сетей Ethernet (100/1000 Мбит/с). Такие случаи неэффективности, конечно, оказывают не слишком сильное влияние на производительность сети, однако по мере роста сети и внедрения новых служб они начинают приводить к проблемам. Эти проблемы лучше всего найти и устранить до того, как они приведут к сбоям и простою сети. В нижеследующей части главы будут представлены некоторые инструкции по поиску неисправностей средствами анализатора протоколов.

Общие проблемы сетей Ethernet

Если вы установили базис сетевой производительности, обнаружение проблемных условий становится намного более простой задачей — в вашем распоряжении имеется "нормальная" область, с которой можно сравнивать результаты текущего тестирования. Тем не менее ошибки не всегда бросаются в глаза. Рассматривая данные, полученные при захвате и анализе сетевых тенденций, вы должны пытаться выявить некоторые распространенные проблемы, перечисленные ниже.

- Ищите необычные модели трафика (например, FTP со средним размером пакета, равным 100 байт). Когда узел отсылает файл при помощи протокола передачи файлов (FTP), намного эффективнее формировать крупные пакеты, а не мелкие. Наибольшим размером пакета Ethernet является 1518 байт — это намного больше, чем 100 байт. Такое обстоятельство может свидетельствовать о неверно настроенной станции.
- Ищите случаи устойчивого использования сети на одном уровне. Уровни использования, превышающие 35 процентов, свидетельствуют о перегруженности сети. Иногда уровень использования может подскакивать до 80 или 90 процентов, но такие случаи должны быть непродолжительными. Когда уровень использования постоянно высок, вероятность возникновения сетевых конфликтов возрастает, в результате чего появляются нежелательные передачи.
- Частота коллизий не должна превышать 5% от частоты передачи пакетов. К примеру, если в данной сети в течение одной секунды передается 100 пакетов, то за тот же промежуток времени коллизий должно быть не более пяти. Коллизии являются компонентом метода CSMA/CD. Они необходимы, но большое их количество свидетельствует о наличии проблем.
- Обратите внимание на коэффициент ошибок. Небольшое количество ошибок — это норма, однако коэффициент ошибок не должен превышать 5% от частоты передачи пакетов.

- Проверьте физические сегменты локальной сети. В каждом отдельно взятом сегменте Ethernet должно находиться не более 200 активных станций, иначе потребность в ресурсах сети может оказаться на высоком уровне, а физические ограничения сети могут быть легко превышены.
- Уровни широковещательного и многоадресного трафика, превышающие примерно 20 пакетов в секунду (packets per second, pps), также создают проблемы, т. к. широковещание приводит к замедлению работы центрального процессора узла. В результате производительность компьютеров сети уменьшается.
- В качестве основных источников сообщений в нормальных ситуациях выступают маршрутизаторы и серверы. Любое другое сетевое устройство, характеризующееся высокими уровнями использования, заслуживает более подробного рассмотрения.
- С течением времени показатель времени ответа не должен изменяться более чем на 10 процентов. Если время ответа колеблется сильнее, вероятно, дело в том, что на сеть оказывают воздействие новые пользователи или приложения. Кроме того, возможны какие-то физические дефекты (связанные с кабелем или сетевой платой) или ошибки протоколов.
- Показатель распределения по протоколам должен согласовываться с программными протоколами. Если речь идет о сети Novell, использующей главным образом протокол IPX, и в ней самым востребованным оказывается IP, проблемы могут заключаться в инкапсуляции или неверной конфигурации.

Тестирование на физическом уровне

В большинстве случаев процесс поиска неисправностей в сетях начинается с попытки выявления возможных физических дефектов, например, неверных контактов, плохо зафиксированных кабелей, поврежденных сетевых плат. Подтверждение работоспособности сетевого кабеля и интерфейсных плат — это необходимый этап проверки качества работы сети. Проблемы, возникшие на физическом уровне, обычно заявляют о себе сами, благодаря множеству симптомов, поэтому используйте анализатор протоколов для измерения и отображения следующих статистических данных:

- неоправданно высокий уровень использования;
- избыточные коллизии;
- неверные контрольные последовательности кадров (Frame Check Sequence, FCS);
- ошибки выравнивания;
- маломерные пакеты (мелкие кадры, Runts);
- сбойные (крупные) кадры (Jabbers);
- режим широковещательных/многоадресных сообщений.

Примечание

Анализаторы протоколов, подобные Observer, предусматривают наличие сводной страницы захвата и анализа пакетов, на которой в удобной форме перечисляются разнообразные пакетные ошибки, обнаруженные в буфере захвата.

Уровень использования

Один из первых показателей, на которые надо обратить внимание, — это уровни использования. Зафиксируйте максимальный уровень использования, а также длительность временного периода, в течение которого он наблюдался. В исправной сети Ethernet постоянный уровень использования не должен превышать 35—40 процентов. Если фиксируемые уровни использования устойчиво превышают этот порог, время ответа увеличивается, количество коллизий повышается, а общая производительность падает.

Коллизии

Другим важным параметром физического уровня является частота коллизий. Коллизии являются нормальным компонентом операций, проходящих в сетях Ethernet, однако чрезмерное их количество сильно уменьшает пропускную способность сети и предполагает наличие проблем на физическом уровне. Если частота появления коллизий (или ошибок) в коаксиальной сети находится на очень высоком уровне, сразу обратите внимание на такие возможные проблемы кабеля, как выход из строя или отсутствие оконечной нагрузки (терминатора), неплотная фиксация цилиндрического или Т-образного коннектора или раздавливание кабеля.

Для того чтобы выявить причины избыточных коллизий, вы должны определить, являются ли эти коллизии *нормальными* или запаздывающими. *Запаздывающие коллизии* возникают после прохождения окна нормальной коллизии с размером кадра 512 байт (8 байт преамбулы плюс 56 байт самого кадра). Они обуславливаются чрезмерно длительным временем прохождения сигнала от узла к узлу (т. е. общим временем прохождения сигнала по всем сегментам кабеля и повторителям/концентраторам). Кроме того, появление таких коллизий могут вызывать сетевые платы, чьи схемы контроля несущей работают неверно. Так как многие сети Ethernet имеют тенденцию к постепенному росту, дополнительный отрезок кабеля и очередной повторитель могут привести к тому, что время распространения сигнала превысит проектные нормы Ethernet. В большинстве случаев эта ситуация разрешается путем перекомпоновки сетевой топологии. Избыточные "нормальные коллизии" могут быть вызваны, к примеру, следующими причинами.

- Рассогласование сопротивления: дефектные оконечные нагрузки, неплотно зафиксированные цилиндрические и Т-образные коннекторы, избыток коннекторов в рамках отдельного сегмента, загибы кабеля, наличие сегментов кабеля с сопротивлением, превышающим 50 Ом (в эту категорию попадает, к примеру, шнур для подключения дисплея).
- Неправильное заземление часто приводит к появлению помех в кабеле. Чтобы не допустить появления контуров заземления, сеть должна заземляться только в одном месте.
- Плохие или неустойчивые соединения.

Удаленные запаздывающие коллизии происходят в тех случаях, когда полученная коллизия с большой долей вероятности является результатом запаздывающей коллизии в другом сегменте сети. Фрагмент признается удаленной запаздывающей коллизией, если его длина превышает 64 байт, у него нарушена контрольная последовательность кадров (FCS), и в нем содержится беспорядочная комбинация чередующихся единиц и нулей. В сетях 10BaseT практически все запаздывающие конфликты ока-

зываются удаленными. В коаксиальных сетях такие конфликты становятся обычными, если в сети наблюдается интенсивный трафик и присутствуют повторители.

В нормальной сети удаленные запаздывающие конфликты могут возникать лишь изредка, а если они редки, то практически не причиняют ущерба. Устойчивая фиксация удаленных запаздывающих конфликтов свидетельствует о том, что физическая протяженность сети слишком велика, что повторители и мосты создают слишком серьезные задержки, или что сеть крайне восприимчива к шумовым помехам. Если удаленные запаздывающие конфликты постоянно фиксируются в коаксиальной сети, попробуйте перенести анализатор в другие сегменты и узнайте, в каком из них наблюдаются локальные запаздывающие коллизии, и копайте от него. В ситуации, когда наблюдается небольшое количество коллизий, но относительно много ошибок, причина может крыться в чрезмерных помехах в кабеле (или, может быть, в дефекте сетевой платы).

Ошибки

Другими признаками коллизий или неисправностей на физическом уровне являются ошибки наподобие маломерных пакетов (кадров с длиной менее 64 байт), сбойных пакетов (кадров с длиной более 1518 байт) и нарушенных контрольных последовательностей кадров (FCS). Описание этих сбойных ситуаций дается ниже.

- *Маломерный пакет* (Rant) чаще всего представляет собой фрагмент кадра, сформированного в результате конфликта двух других кадров. Это нормальное сетевое состояние, причем в небольших коаксиальных сетях маломерные пакеты практически отсутствуют, т. к. фактические коллизии в них происходят в рамках преамбул кадров. Наблюдение маломерных пакетов более вероятно в крупных сетях, или в 10/100BaseT. В относительно крупных сетях появление коллизий в рамках передаваемого кадра вызывается большими значениями времени сквозного прохождения сигнала. В сетях 10/100BaseT коллизии происходят в рамках концентратора. Связанные с ним задержки приводят к тому, что многие фрагменты кадров (т. е. маломерные пакеты) распространяются по сети.
- Нарушенные *контрольные последовательности кадров* вызываются различными причинами: коллизиями, помехами в кабеле, дефектными сетевыми платами и плохими соединениями. Систематическое выявление источников возникновения ошибок подобного рода крайне важно. Если они являются результатом коллизий, частота которых не слишком высока, тогда опасаться нечего.
- *Сбойные пакеты* — это ненормальное состояние сети, которое обычно свидетельствует о возникновении серьезной проблемы. Сбойные пакеты (иногда они называются гигантскими кадрами) представляют собой кадры, длина которых превышает 1518 байт; обычно их генерирует узел, не соблюдающий спецификации Ethernet, или неисправный приемопередатчик. Среди других возможных причин появления сбойных пакетов можно упомянуть контуры заземления, дефектные сетевые платы или модули доступа к среде.

Тестирование на канальном уровне

После проведения проверки на физическом уровне следует переходить к анализу канального уровня (уровня протоколов) и изучению структуры протоколов и паке-

тов. Естественно, оценить целостность на канальном уровне значительно сложнее, чем физическую инфраструктуру, т. к. в данном случае необходимо учитывать множество переменных. Наиболее важными моментами, которые нужно учесть, — это назначение рассматриваемого сегмента (например, магистрали), типы подключенных к нему узлов и местоположение блочных устройств (в число которых входят повторители, мосты, маршрутизаторы и коммутаторы). Среди факторов, которые необходимо учесть, — уровень использования, широковещательный трафик и сочетание протоколов. Ниже приведено несколько общих рекомендаций, которые имеет смысл принять во внимание.

- Работая с мостом/маршрутизатором, имейте в виду, что с этими устройствами связывается более высокий процентный показатель широковещательных и многоадресных пакетов (широковещательные и многоадресные пакеты передаются через мостовые сети, поскольку они всегда ретранслируются). Кроме того, средний размер кадра у них меньше.
- Обращайте особое внимание на объем широковещательного трафика. В идеале, его частота не должна превышать 20 пакетов в секунду. Все узлы, вне зависимости от применяемых стеков протоколов, обязаны обрабатывать широковещательный трафик. Широковещательный трафик влияет на производительность всех сетевых узлов.
- Уровень использования канала очень сильно зависит от применяемых приложений (например, от передач файлов и интерактивных процессов).

Рассмотрим пример. Предположим, что пользователи сети начали жаловаться на замедление доступа к совместно используемым сетевым устройствам. Во время проведения в сети ряда диагностических тестов вы обнаруживаете, что частота коллизий избыточна. Довольно часто для решения таких проблем задействуется подход "разделяй и властвуй" — при этом сеть последовательно делится на две физических части, и, в конце концов, методом исключения сегмент, инициирующий появление проблемы, обнаруживается. Подобным же образом этот метод применяется к самому сегменту — он постоянно делится пополам на все меньшие физические части, и происходит это до тех пор, пока проблемная станция не выявляется. Этот метод эффективен, но медленен и недостаточен. С помощью анализатора протоколов процесс обнаружения проблемного объекта значительно упрощается, а анализ буфера захвата пакетов свидетельствует о том, что частота конфликтов в сети действительно высока.

В сети Ethernet нормальным является частота коллизий, составляющая 5 процентов общего уровня использования сети (измеряемого в кадрах в секунду). Статистические данные, свидетельствующие о превышении этого порога, при расшифровке обычно обозначаются как ошибки. Узнав тип проблемы, вы должны найти ее источник. Просматривайте захваченный трафик, пока не найдете кадр с обозначенной ошибкой. Обратите внимание на то, что в записях адресов кадров, участвовавших в конфликтах, ставятся шестнадцатеричные отметки FF, 55, AA, A5 или 5A.

Теперь, когда вам удалось обнаружить кадры, участвующие в конфликтах, необходимо установить, откуда они появляются. Как правило, кадр, следующий сразу за поврежденным кадром, исходит от одной из двух станций, инициирующих коллизию. Чтобы убедиться в этом, взгляните на временную метку. Если разница во времени между дефектным кадром и кадром, следующим непосредственно за ним, не

превышает 150 мс (в зависимости от местоположения станции в сети и длины сегмента), значит, это действительно один из конфликтных кадров. Если уровень трафика в сети высок, значит, кадр, исходящий со станции-нарушителя, мог быть опережен кадром с другой станции. Имеет смысл проверить кадры, следующие за несколькими другими дефектными кадрами. Если показатель частоты коллизий высок, вполне возможно, что ошибок много. Одна из станций, приводящих к появлению коллизий, должна устойчиво фиксироваться вслед за дефектными кадрами. Выявив станцию-нарушителя, вы можете предпринять корректирующие действия. После этого тестирование сети разумно повторить — просто чтобы убедиться, что показатель частоты коллизий вернулся в допустимые рамки.

Примечание

Инструментальные средства, подобные Observer, предусматривают функцию **Collision Expert** (Эксперт по конфликтам), предназначенную для автоматической идентификации источников конфликтов.

Дублированные IP-адреса

Дублированный IP-адрес (адрес протокола Интернет) — это конфликт между логическими адресами, который возникает тогда, когда два физических MAC-адреса по ошибке начинают пользоваться одним и тем же логическим IP-адресом. Иногда, когда в сети происходят изменения, или когда сетевой администратор не располагает жестким контролем над назначенными IP-адресами, ошибки конфигурации могут приводить к подобному дублированию. Среди симптомов дублирования IP-адресов можно выделить жалобы пользователей на ошибочные потери соединения TCP или предупредительные сообщения ICMP, исходящие от сетевых маршрутизаторов.

Убедиться в том, что IP-адреса дублируются, проще всего с помощью ARP — этот протокол показывает, действительно ли подозрительным IP-адресом пользуются несколько MAC-станций в сети. Обычно это делается путем отправки с сетевой рабочей станции на подозрительный IP-адрес Ping-запросов — с помощью команд Ping утилиты Ping анализатора. Как правило, оповещения о дублировании IP-адресов генерируются в ходе анализа буфера захвата (например, на странице **Expert Analysis** программы Observer). При этом в отчете обозначается сетевой IP-адрес, конфликтующие MAC-адреса, а также номера (назначенные анализатором) двух захваченных кадров. Когда анализатор идентифицирует маршрутизаторы, они исключаются из отчета по дублированию IP-адресов. Впрочем, если маршрутизатор еще не идентифицирован, на протяжении непродолжительного времени ошибочный дублированный IP-адрес может фигурировать в отчете. MAC-адреса маршрутизаторов не признаются источниками дублирования.

Поиск неисправностей в сетях типа маркерного кольца

Помимо прочего, анализаторы протоколов, подобные Observer, помогают искать ошибки уровня управления доступом к среде в сетях типа маркерного кольца (Token Ring). Ошибки в кольцеобразных сетях обычно делятся на постоянные и случайные. Постоянные ошибки обычно выводят из строя всю кольцеобразную сеть, причем устранить их средствами анализатора протоколов крайне сложно — для того чтобы анализатор протоколов мог помочь в процессе поиска неисправностей, сеть должна

функционировать хотя бы частично. Среди постоянных ошибок встречаются нижеследующие.

- *Потоковые ошибки.* Они обычно связаны с неисправностью адаптера, который начинает выполнять операции, не соблюдая последовательность и перезаписывая (или уничтожая) кадры и маркеры. В наиболее сложных случаях (они называются потоками кадров) адаптер осуществляет непрерывную передачу кадров, маркеров и шумовых сигналов.
- *Частотные ошибки.* Такие ошибки могут возникать в случаях, когда частота сигнала входящих кадров выходит за пределы стандартного диапазона более чем на 0,6%. К счастью, конструктивные решения современных устройств маркерного кольца делает такие ошибки довольно редкими.
- *Ошибки потери сигнала.* Они обычно связываются с неисправной (или не соответствующей спецификациям) проводкой, в некоторых случаях — с дефектными модулями доступа к среде и повторителями. Как правило, эта проблема является аппаратной и не имеет отношения к программному обеспечению или драйверам.
- *Внутренние ошибки.* Это ошибки аппаратуры адаптера, они настолько серьезные, что приводят адаптер (установленный в кольце) к самопроизвольному удалению из сети.
- *Ошибки, связанные с аппаратной несовместимостью.* Эти ошибки обуславливаются аппаратными конфликтами между адаптером и другим аппаратным устройством, установленным на локальной станции (это может быть конфликт прерываний или DMA). В большинстве случаев такой адаптер просто не присоединяется к кольцу.

Есть четыре типа случайных ошибок, которые нужно иметь в виду. Ошибками 1-го типа являются простые некритические ошибки, которые, как правило, не требуют восстановительных действий. Ошибки 2-го типа несколько более серьезны, они подразумевают проведение чистки кольца. Ошибки 3-го типа еще более трудны, они требуют проведения состязания между мониторами. Последний тип случайных ошибок — это сигналы (сигнальные кадры). В свою очередь, ошибки 1-го типа подразделяются на следующие категории.

- *Ошибки линии.* В кольцеобразной сети эти ошибки эквивалентны ошибкам CRC в Ethernet. По отношению к входящим кадрам каждая станция выполняет проверку при помощи CRC. Если станция обнаруживает несоответствие между числом, выражающим контрольную сумму, и результатами вычисления контрольной суммы, она отчитывается об ошибке. Ошибки канала обычно наблюдаются в загруженных сетях. Впрочем, если станция постоянно оповещает о формировании ошибок канала, это, как правило, означает, что сетевая плата, установленная на вышестоящем соседнем узле, неисправна.
- *Внутренние ошибки.* Ошибки такого рода происходят, когда станция обнаруживает присутствие восстановимого аппаратного сбоя. Если адаптер постоянно отчитывается о внутренних ошибках, это, вероятно, означает, что он начинает выходить из строя. Прежде чем менять сетевую плату, еще раз проверьте все соединения.
- *Ошибка значения бита ARI/FCI.* Сообщение об этой ошибке появляется тогда, когда во время кольцевого опроса станция обнаруживает два кадра с "наличием

резервного монитора", у которых бит ARI/FCI установлен на ноль (без вмешательства активного монитора). Такая ошибка встречается редко.

- *Ошибки переполнения при приеме.* Станция сообщает об этой ошибке, когда свободного буферного пространства недостаточно для копирования пакетов, которые ей адресованы. Если адаптер постоянно сообщает об ошибках переполнения при приеме, это свидетельствует либо об аппаратной или программной неисправности принимающей станции, либо о дефектном (сопровождающемся помехами) соединении с вышестоящим по отношению к данной станции модулем доступа к среде (принимающие схемы адаптера могут быть переполнены).
- *Ошибки копированных кадров.* Сообщения о таких ошибках появляются в тех случаях, когда в кадре, направленном данной станции, уже установлен бит ARI/FCI. Это свидетельствует о существовании в сети двух сетевых плат с идентичными адресами. Такая ситуация возможна в условиях мостовых многокольцевых сетей, в которых адреса маркерного кольца назначаются локально.

Существует ряд случайных ошибок 2-го типа, которые при поиске неисправностей заслуживают более пристального внимания.

- *Пакетные ошибки.* Сообщения о таких ошибках появляются в тех случаях, когда станция обнаруживает потерю сигнала в течение полубайтовых циклов и более. В работе кольцеобразных сетей пакетные ошибки встречаются довольно часто, причем, в основном, они происходят тогда, когда станция присоединяется к кольцу или покидает его. Постоянная фиксация такой ошибки может свидетельствовать об аппаратной неисправности вышестоящего по отношению к оповещающему адаптеру соседнего узла (или его ретрансляторов MAU). Пакетные ошибки обычно сопровождаются ошибками канала, потери кадров или маркера.
- *Ошибка передачи прерывающего разграничителя.* Сообщение об этой ошибке появляется в том случае, если станция осуществляет передачу прерывающего разграничителя, вне зависимости от причины, по которой это делается. В таком случае активный монитор обнаруживает вмешательство в маркерный протокол и чистит кольцо.
- *Ошибки потерянных кадров.* Когда станция передает завершитель кадра, она устанавливает таймер, тем самым определяя временной промежуток, в течение которого этот завершитель должен возвратиться с вышестоящей станции. Когда кадр возвращается, станция извлекает его из сети и выполняет действие, зависящее от того, установлен ли бит FCI или нет. Если же станция не получает завершитель до истечения таймера, она считает кадр потерянным, и увеличивает значение своего счетчика потерянных кадров.
- *Ошибки маркера.* Активный монитор генерирует сообщение о такой ошибке, если он обнаруживает поврежденный маркер или кадр, потерянный маркер, циркулирующий кадр или приоритетный маркер.

Ошибки 3-го типа — одни из самых серьезных; в случае их возникновения технический специалист должен немедленно приступать к действиям.

- *Ошибки потерянного монитора.* Эти ошибки фиксируются в тот момент, когда активный монитор покидает кольцо или перестает работать. Сообщение о такой ошибке генерирует резервный монитор, обнаруживший отсутствие активного монитора. После этого оставшиеся резервные мониторы приступают к состяза-

тельному процессу, направленному на выбор новой станции, которая будет исполнять роль активного монитора.

- *Частотные ошибки.* Появление такой ошибки является результатом неверной схемы тактирования активного монитора. Обычно она разрешается с помощью состязания между мониторами, в ходе которого активным становится другой резервный монитор.

Наконец, вы должны понимать, что делать с сигналами-маяками (Beacons). Передача сигнальных кадров производится сетевой платой в том случае, если она обнаруживает молчание кабеля (не получая от вышестоящего соседнего узла ни маркеров, ни кадров данных). Адаптер отправляет сигналы по нисходящей, извещая все остальные устройства. Если вышестоящий соседний узел получает сигнал от своего нижестоящего соседа (а сигнальное состояние было вызвано временным аппаратным сбоем), последний в конечном итоге получает сигнал от первого. В противном случае оба адаптера удаляются из кольца и пытаются провести повторное подключение. В случае неисправности кабеля или аппаратного обеспечения поврежденная станция не сможет провести повторное подключение, и работа сети будет возобновлена (это называется "разрешенным сигнальным состоянием"). Если попытка автоматического разрешения сигнального состояния не увенчивается успехом, может потребоваться прямое вмешательство технического специалиста.

Дополнительные ресурсы

Network Instruments: **www.networkinstruments.com**.

Agilent: **www.agilent.com**.

Hewlett-Packard: **www.hp.com**.

Protocol.com: **www.protocols.com**.

ПРИЛОЖЕНИЕ 1

Дополнительные интернет-ресурсы

В заключительной части каждой главы этого издания приводятся многочисленные интернет-источники, однако существуют и более общие с тематической точки зрения ресурсы, к которым могут свободно обращаться технические специалисты, имеющие доступ к сети Интернет. Некоторые ресурсы, приведенные ниже, предоставлены производителями, другие обслуживаются независимыми группами или организациями.

Web-сайты

База знаний 3Com: **knowledgebase.3com.com**.

Служба поддержки 3Com: **support.3com.com**.

Национальный институт стандартизации США (ANSI, American National Standards Institute): **www.ansi.org**.

Форум по технологии ATM: **www.atmforum.com**.

Прокладка/техническое обслуживание кабелей: **cim.pennnet.com/home.cfm**.

Поиск неисправностей продукции Cisco: **www.cisco.com/public/technotes/serv_tips.shtml**.

Руководства пользователя по продукции Compaq: **www.compaq.com/support/techpubs/maintenance_guides/index.html**.

Служба поддержки Dell: **support.dell.com/us/en/home.asp**.

Поиск неисправностей DUN: **www.webcom.com/~llarrow/trouble.html**.

Руководство по сетям Ethernet: **wwwhost.ots.utexas.edu/ethernet/ethernet.html**.

Форум по технологии ретрансляции кадров: **www.frforum.com**.

Общая техническая документация (Global Engineering Documents): **www.global.ihs.com**.

Служба поддержки Hewlett-Packard: **www.hp.com/cposupport/eschome.html**.

Служба поддержки IBM по сетевым продуктам: **www.networking.ibm.com/netsupt.html**.

Стандарт IEEE 802.3: **grouper.ieee.org/groups/802/3/index.html**.

Стандарт IEEE 802.5: **www.8025.org**.

Уникальные идентификаторы IEEE:
standards.ieee.org/regauth/oui/tutorials/lanman.html.

Информационный центр сети Интернет (Internet Network Information Center, InterNIC): **www.internic.net**.

Международный союз электросвязи (International Telecommunications Union, ITU):
www.itu.int/home/index.html.

Служба поддержки Microsoft: **support.microsoft.com**.

Сетевые компьютерные технологии:
www.networkcomputing.com/netdesign/troubleintro.html.

Поиск неисправностей в сетях: **www.k12.hi.us/~network/1999/41200nettrbleshoot/**.

Поиск неисправностей в сетях: **www.networktroubleshooting.com**.

Поиск неисправностей в сетях:
www2.ucsc.edu/cats/sc/tools/network-troubleshoot/index.shtml.

Североамериканский форум пользователей ISDN: **www.niuf.nist.gov/**.

Служба поддержки Novell: **support.novell.com**.

База знаний Sun: **www.sun.com/service/support/**.

Telcordia: **www.telcordia.com/pssindex.html**.

TroubleTree: **www.troubletree.com/**.

Поиск неисправностей устройств беспроводной связи:
www.practicallynetworked.com/support/troubleshoot_wireless.htm.

Новостные группы

comp.dcom.cabling.

comp.dcom.lans.ethernet.

comp.dcom.lans.fddi.

comp.dcom.lans.misc.

comp.dcom.lans.token-ring.

comp.dcom.moderns.cable.

comp.dcom.sys.cisco.

comp.dcom.xdsl.

comp.dcorn.modems.

comp.os.linux.networking.

comp.os.linux.setup.

comp.os.ms-windows.networking.misc.

comp.os.ms-windows.networking.tcp-ip.

comp.os.ms-windows.networking.win95.

comp.os.ms-windows.nt.admin.misc.

comp.os.ms-windows.nt.admin.networking.

comp.os.ms-windows.nt.misc.

comp.protocols.tcp-ip.

comp.sys.mac.misc.

comp.unix.solaris.

han.cornp.os.linux.

han.cornp.os.winnt.

microsoft.public.win95.networking.

microsoft.public.win98.networking.

microsoft.public.win98.performance.

microsoft.public.win98.setup.

microsoft.public.windowsnt.protocol.tcpip.

ПРИЛОЖЕНИЕ 2

Общие сведения о сертификатах Net+ и Server+

Если вы собираетесь сменить род деятельности, перейти на другое место работы или надеетесь на повышение, самая сложная для вас задача будет заключаться в том, чтобы продемонстрировать будущему работодателю свою квалификацию и убедить его, что вы действительно настолько компетентны, что можете претендовать на желаемую должность в компании. Один из простейших способов продемонстрировать свои знания — это пройти сертификацию по программе, относящейся к соответствующей технологии. Сертификат, признанный производителем, свидетельствует о том, что вы прошли образовательный этап и владеете базовыми знаниями, необходимыми для работы на заданном уровне. Сегодня практически каждый технический специалист выигрывает от получения с умом выбранного сертификата. Факт сертификации поднимает уровень вашей заработной платы, улучшает навыки, обеспечивает наиболее оптимальное соответствие вашей работы вашим ожиданиям.

В компьютерной индустрии существует множество различных сертификатов, причем у большинства производителей есть специальные сертификаты для работы с их продукцией. Тем не менее некоторые наиболее популярные и уважаемые сертификаты нейтральны по отношению к представителям индустрии (в том числе A+, Network+ и Server+, спонсором которых является CompTIA, а управляющими организациями — Prometric и VUE). Такой сертификат охватывает распространенные методики и часто используемое оборудование. Сертификация обеспечивает разнообразные и безусловные преимущества как для работников, так и для работодателей.

- *Объективность при найме.* Требование соответствующего нейтрального сертификата обеспечивает минимальный уровень знаний, которым должны обладать все соискатели. Это упрощает отбор соискателей и содействует карьерному росту только квалифицированного персонала.
- *Более обширные знания.* Сертификаты производителей, несомненно, полезны, однако нейтральные сертификаты обычно охватывают более широкую область знаний и оборудования, подготавливая более универсальных специалистов. В условиях быстро изменяющегося рынка технологий подобная гибкость является значительным преимуществом.
- *Более высокий престиж и доверие.* На рынке технологий в его современном виде сертификация предоставляет значительное конкурентное преимущество. Такое

доверие к сертификату помогает как его владельцу, так и компании, которая предоставляет ему работу.

- *Более обширные возможности трудоустройства.* Введение сертификации сотрудников компании позволяет более точно определить для сертифицированного специалиста круг выполняемых задач, а также выявить новые/альтернативные сертификаты, которые могут помочь повысить профессиональную базу компании. В результате специалистам предоставляются больше перспектив с точки зрения трудоустройства и образования.
- *Улучшение условий труда.* Так как сертификаты определяют профессиональные навыки сотрудника, на основании сертификатов можно объективно устанавливать уровень оплаты труда сотрудника.

Примечание

Более подробную информацию о сертификатах, предлагаемых CompTIA, можно получить на Web-сайте компании по адресу **www.comptia.com**. Составить расписание экзаменов и заплатить за них можно через Prometric (**www.2test.com/index.jsp**) и VUE (**www.vue.com/comptia**).

Server+

Экзамен "Специалист по серверному аппаратному обеспечению" (Server Hardware Specialist, Server+) — это сравнительно новая сертификация CompTIA, целью которой является обучение работе с аппаратным обеспечением персональных компьютеров типа RAID, SCSI, различными процессорами и т. д. Курс обучения специалиста по серверному аппаратному обеспечению включает изучение комплексных проблем и работ, связанных с конфигурированием, сопровождением и ремонтом серверов. Предполагается, что специалист Server+ должен обладать глубокими знаниями в области планирования, установки и сопровождения серверов, в том числе разбираться в аппаратуре сервера, системах хранения и восстановления данных, а также в подсистемах ввода/вывода. Технический специалист по серверам должен уметь предсказать работу всех компонентов серверной системы, иметь представление о вариантах выполняемых ими операций. Специалист Server+ обычно работает независимо, решает сложные проблемы, однако в особых случаях он может обратиться за помощью к сотрудникам службы системной поддержки. Соискателю на получение этого сертификата рекомендуется обладать следующим опытом:

- минимум 18—24 месяца работы в индустрии серверных технологий (организации сетей);
- непосредственный опыт монтажа, конфигурирования, диагностирования и поиска неисправностей серверного аппаратного обеспечения и сетевых операционных систем;
- наличие по крайней мере одного сертификата по информационным технологиям типа CompTIA A+, Compaq ACT, Novell CAN, Microsoft MCP, HP STAR, SCO или Banyan;
- способность к эффективному взаимодействию и документированию.

Темы экзамена Server+

Для сдачи экзамена Server+ от кандидатов требуется знание тематических областей, перечисленных в табл. П2.1. Их подробное описание приведено ниже.

Таблица П2.1. *Темы экзамена Server+*

Тема	Процентное содержание
Монтаж	17
Конфигурирование	18
Модернизация	12
Профилактическое обслуживание	9
Окружающая среда	5
Поиск неисправностей	27
Аварийное восстановление	12

Нижеследующий перечень характеризует стандартный план экзамена Server+.

Монтаж

- ❒ Проведите предустановочное планирование.
  - Спланируйте схему монтажа.
  - Проверьте план монтажа.
  - Проверьте аппаратную совместимость с операционной системой.
  - Проверьте источники питания, место размещения, наличие источника бесперебойного питания и возможность подключения к сети.
  - Проверьте наличие всех необходимых компонентов и кабелей.
- ❒ Установите аппаратное обеспечение (платы, дисководы, процессоры, память, внутренние кабели и т. д.).
  - Установите стойку.
  - Нарежьте и обожмите сетевые кабели.
  - Установите источник бесперебойного питания.
  - Проверьте конфигурацию идентификаторов SCSI и оконечную нагрузку.
  - Установите внешние устройства (клавиатуры, мониторы, подсистемы, модемный пул и т. д.).
  - Проверьте подачу напряжения, включив питание.

Конфигурирование

- ❒ Проверьте и обновите состояние BIOS/микропрограммного обеспечения (на материнской плате, RAID, контроллере, жестком диске и т. д.).

- ☐ Настройте массив RAID.
- ☐ Установите сетевую операционную систему.
  - Настройте сеть.
  - Проверьте возможность подключения к сети.
- ☐ Настройте внешние периферийные устройства (источник бесперебойного питания, внешние диски и т. д.). Установите обновления сетевой операционной системы.
- ☐ Обновите драйверы, поставляемые производителем.
- ☐ Установите служебные инструментальные средства (программу резервирования, агенты системного мониторинга, журналы регистрации событий и т. д.).
- ☐ Установите базис сервера.
- ☐ Задокументируйте конфигурацию.

Модернизация

- ☐ Выполните операции резервирования/восстановления.
  - Проверьте резервную копию.
- ☐ Установите дополнительные процессоры.
  - При модернизации единственного процессора в системе проверьте его совместимость.
  - Проверьте совместимость версий процессоров.
  - Проверьте соответствие скорости и параметров кэшей.
  - Проведите обновление BIOS.
  - Проведите обновление операционной системы в расчете на поддержку многопроцессорной обработки.
  - Найдите/получите самые свежие драйверы, обновления операционной системы, программное обеспечение.
- ☐ Установите дополнительные жесткие диски.
  - Проверьте соответствие типа жестких дисков.
  - Проверьте оконечные нагрузки и кабельные соединения.
  - Для дисководов ATA/IDE проверьте кабельные соединения, отношения главного/подчиненного устройства, потенциальную совместимость между моделями устройств.
  - Проведите модернизацию запоминающих устройств.
  - Добавьте в массив RAID новые диски.
  - Замените существующие диски.
  - Объедините диски в систему хранения и сделайте их доступными для операционной системы.

- ❒ Увеличьте объем памяти.
  - Проверьте наличие поддержки наращивания емкости памяти со стороны аппаратного обеспечения и операционной системы.
  - Проверьте наличие модуля памяти в списке совместимого оборудования/совместимых производителей.
  - Проверьте совместимость памяти.
  - Убедитесь в том, что сервер и операционная система способны идентифицировать добавленную память.
  - Проведите оптимизацию сервера, направленную на активизацию дополнительной оперативной памяти.
- ❒ Обновите BIOS/микропрограммное обеспечение.
- ❒ Проведите модернизацию ключевых адаптеров (сетевых адаптеров, плат SCSI, RAID и т. д.).
- ❒ Проведите модернизацию внутренних и внешних периферийных устройств.
  - Проверьте соответствующие системные ресурсы (слоты расширения, IRQ, DMA и т. д.).
- ❒ Проведите обновление программ системного мониторинга.
- ❒ Проведите обновление служебных инструментальных средств (диагностических средств, диагностического разделения, утилиты настройки системы и т. д.).
- ❒ Проведите модернизацию источника бесперебойного питания.

Профилактическое обслуживание

- ❒ Проводите регулярное резервирование.
- ❒ Установите базис и сравнивайте с ним показатели текущей производительности.
- ❒ Настройте пороги SNMP.
- ❒ Проводите обслуживание физических компонентов.
- ❒ Проводите контроль состояния аппаратного обеспечения.
- ❒ Организуйте удаленное оповещение.

Окружающая среда

- ❒ Выявите проблемные области физической защиты и составьте соответствующий отчет.
  - Ограничьте доступ к помещению, в котором располагается сервер, а также к резервным копиям.
  - Убедитесь в наличии на дверях замков.
  - Установите средства защиты аппаратного обеспечения (заблокируйте стойки сервера).
- ❒ Выявите проблемные области, связанные с помещением, где находится сервер, и составьте соответствующий отчет.

Поиск неисправностей

- ❒ Выявите неисправность.
  - Научитесь, как выявлять неисправности.
  - Установите, какие лица ответственны за устранение неисправностей.
  - Научитесь определять характер неисправности по внешним признакам.
- ❒ Используйте диагностическую аппаратуру, программные средства и утилиты.
  - Составьте представление о распространенных диагностических средствах.
  - Попрактикуйтесь в завершении работы операционной системы.
  - Выберите подходящее инструментальное средство.
  - Придерживайтесь эффективных методов применения выбранного инструментального средства.
  - Замените неисправные аппаратные компоненты наиболее подходящим способом.
  - Определите, какие устройства являются неисправными, и замените их соответствующими компонентами.
  - Интерпретируйте журналы регистрации ошибок, ошибки операционной системы, журналы состояния и важнейшие события.
  - Старайтесь извлекать максимальную пользу из документации, составленной предыдущим техническим специалистом.
  - Соберите ресурсы, необходимые для решения проблемы.
  - Опишите процедуру удаленного устранения неисправности функции запуска при активности в локальной сети.
  - Опишите процедуру удаленного устранения неисправности функции удаленного предупреждения.
- ❒ Выявите узкие места (они могут быть связаны с процессором, передачей данных по шине, дисковой и сетевой системой ввода/вывода и памятью).
- ❒ Выявите и устраните неисправности конфигурации и/или выполните соответствующие процедуры модернизации.
- ❒ Определите, связана ли неисправность с аппаратным обеспечением, программным обеспечением или вызвана вирусами.

Аварийное восстановление

- ❒ Составьте план аварийного восстановления.
  - Составьте план резервирования (жестких дисков, источников питания, вентиляторов, сетевых адаптеров, процессоров, источников бесперебойного питания).
  - Для того чтобы обеспечить работоспособность, пользуйтесь методиками горячей замены, теплой замены и горячего резервирования.
  - При составлении плана аварийного восстановления задействуйте принципы отказоустойчивости/устранения неисправностей.
  - Разработайте план аварийного восстановления.

- Определите типы аппаратного обеспечения резервирования.
- Определите типы схем резервирования и восстановления.
- Утвердите внесетевое хранилище резервных копий и пользуйтесь им.
- Регулярно документируйте и проверяйте план аварийного восстановления; при необходимости обновляйте его.

❒ Восстановление.

- Определите, какую аппаратуру необходимо заменить.
- Определите, какие устройства поддерживают горячую замену, а какие — нет.
- Осуществите план аварийного восстановления.

Network+

Экзамен "Специалист по сетям" (Network Specialist, Network+) — это хорошо зарекомендовавший себя сертификат CompTIA, охватывающий вопросы администрирования и сопровождения сетей, которые отражают 18—24-месячный опыт работы в индустрии информационных технологий. Экзамен Network+ был пересмотрен в 2002 г.; он подтверждает, что успешно прошедшие его кандидаты имеют представление об уровнях модели OSI, способны охарактеризовать возможности и функции компонентов сети, обладают навыками, необходимыми для монтажа, конфигурирования и поиска неисправностей основных сетевых аппаратных периферийных устройств и протоколов. Желательно, чтобы перед сдачей экзамена у кандидата был сертификат A+ или соответствующие этому уровню знания. Однако наличие сертификата A+ не является жестким требованием. В дополнение к уровню знаний, эквивалентному сертификации по программе A+, хорошо, чтобы за плечами у кандидатов было, по меньшей мере, десять месяцев опыта сопровождения или администрирования сетей.

Обновление экзамена Network+, выполненное в 2002 г., охватывает новые технологии типа беспроводных сетей и Gigabit Ethernet. Среди сетевых систем особое внимание уделяется системам Linux/UNIX, Windows 9x, Windows NT, Windows 2000 и AppleTalk в качестве сетевого протокола. Особый акцент сделан на практических навыках, наличие которых необходимо для работы в области реализации сетей и их сопровождения, в том числе и для выполнения сценариев поиска неисправностей.

Темы экзамена Network+

Для того чтобы приступить к сдаче экзамена Network+ версии 2002 г., от кандидатов требуется знание тематических областей, перечисленных в табл. П2.2. Их подробное описание приводится ниже.

Таблица П2.2. *Темы экзамена Network+*

Тема	Процентное содержание
Сетевая среда и топология сети	20
Протоколы и стандарты	25

Таблица П2.2 (окончание)

Тема	Процентное содержание
Реализация сетей	23
Сопровождение сетей	32

Сетевая среда и топология сети

- ❒ Умейте определять логические и физические топологии сети по схематичному чертежу или описанию.
- ❒ Укажите основные характеристики сетевых технологий 802.2 (LLC), 802.3 (Ethernet), 802.5 (маркерное кольцо), 802.11b (беспроводные сети) и FDDI.
- ❒ Укажите характеристики (скорость, протяженность, топология, тип кабеля и т. д.) стандартов 802.3 (Ethernet).
- ❒ Умейте различать основные типы коннекторов и/или описывать способы их применения.
- ❒ Выберите тип носителей и коннекторы, необходимые для создания нового клиента в рамках существующей сети.
- ❒ Сформулируйте назначение, возможности и функции рядовых сетевых компонентов, таких как концентраторы, коммутаторы, мосты, маршрутизаторы, шлюзы, модули обслуживания канала и данных (CSU/DSU), сетевые адаптеры, беспроводные точки доступа (WAP) и т. д.

Протоколы и стандарты

- ❒ Определите MAC-адрес.
- ❒ Назовите семь уровней модели OSI и их назначение.
- ❒ Укажите различия между наиболее распространенными сетевыми протоколами с точки зрения маршрутизации, схем адресации, возможностей взаимодействия и соглашений по именованию.
- ❒ Назовите уровни модели OSI, на которых работают обычные сетевые компоненты.
- ❒ Сформулируйте назначение, функции и/или способы применения общепринятых протоколов в рамках стека TCP/IP.
- ❒ Сформулируйте функции портов TCP/UDP и дайте определение хорошо известным портам.
- ❒ Сформулируйте назначение сетевых служб типа DHCP/BOOTP, DNS, NAT/ICS, WINS и SNMP.
- ❒ Умейте различать IP-адреса (IPv4, IPv6) и их маски подсетей, принимаемые по умолчанию.
- ❒ Сформулируйте назначение организации подсетей и шлюзов по умолчанию.
- ❒ Сформулируйте различия между общедоступными и частными сетями.

- ❒ Назовите основные характеристики (например, скорость, емкость, носители) основных технологий глобальных сетей.
- ❒ Сформулируйте назначение протоколов и служб удаленного доступа.
- ❒ Назовите основные протоколы системы защиты, охарактеризуйте их назначение и задачи.

Реализация сетей

- ❒ Сформулируйте основные возможности (например, обеспечение работы компьютеров клиентов, способность к взаимодействию, аутентификация, файловые службы и печать, поддержка приложений, организация системы защиты) серверных операционных систем.
- ❒ Сформулируйте основные возможности рабочих станций клиентов (например, установление связи, локальные механизмы обеспечения защиты, аутентификация).
- ❒ Назовите основные характеристики виртуальных локальных сетей.
- ❒ Назовите основные характеристики устройств хранения данных, подключаемых к сети.
- ❒ Сформулируйте назначение и характеристики отказоустойчивости.
- ❒ Сформулируйте назначение и характеристики аварийного восстановления.
- ❒ Настройте соединение, исходя из заданного сценария удаленной связи (включающего такие характеристики, как IP, IPX, коммутация, PPPoE, аутентификация, физическое обеспечение связи и т. д.).
- ❒ Сформулируйте назначение, преимущества и характеристики применения брандмауэра.
- ❒ Сформулируйте назначение, преимущества и характеристики применения агента (proxy).
- ❒ Исходя из заданного сценария, спрогнозируйте воздействие реализации конкретной системы защиты на функциональность сети (к примеру, блокирование номеров портов, шифрование и т. п.).
- ❒ Исходя из заданной сетевой конфигурации, выберите подходящий сетевой адаптер и соответствующие настройки сетевой конфигурации (DHCP, DNS, WINS, протоколы, NetBIOS/имя хоста и т. д.).

Сопровождение сетей

- ❒ Исходя из заданного сценария поиска неисправностей, выберите подходящую для данной ситуации утилиту TCP/IP, например, Tracert, Ping, Arp, Netstat, Nbstat, Ipconfig/Ifconfig, Winipcfg, Nslookup и т. д.
- ❒ Исходя из заданного сценария поиска неисправностей, предполагающего сбой в сети небольшого/домашнего офиса (это может быть неисправность DLS, кабеля, домашнего спутникового ретранслятора, беспроводного устройства, телефонной станции), определите его причину.

- ❒ Исходя из заданного сценария поиска неисправностей, предполагающего сбой удаленной связи (например, ошибку аутентификации, конфигурацию протокола, возможность физического соединения), определите сущность проблемы.
- ❒ Исходя из заданных параметров, настройте компьютер клиента на подключение к серверам UNIX/Linux, NetWare, Windows или Macintosh.
- ❒ Исходя из имеющейся задачи по проводке кабеля, выберите подходящее средство (обжим проводов, тестер/блок проверки носителя, монтажный блок, звуковой генератор, оптический тестер и т. д.).
- ❒ Исходя из заданного сетевого сценария, определите значение визуальных индикаторов (например, светодиодов канала или конфликтов) и установите характер неисправности.
- ❒ Интерпретируйте заданные выходные данные диагностической утилиты (например, Tracert, Ping, Ipconfig).
- ❒ Исходя из заданного сценария, спрогнозируйте воздействие изменения, добавления или удаления сетевых служб (например, DHCP, DNS, WINS и т. д.) на ресурсы и пользователей сети.
- ❒ Исходя из сценария сетевой неисправности, выберите подходящий образ действий, соответствующий общей стратегии поиска неисправностей.
- ❒ Исходя из сценария поиска неисправностей, связанного с сетью определенной физической топологии (например, шинной, звездообразной/иерархической, решетчатой, кольцеобразной или беспроводной), установите область сети, на которую распространяется данная неисправность, и выявите ее причину.
- ❒ Исходя из сценария поиска сетевых неисправностей, подразумевающего проблему со связью компьютеров клиентов (типа неверного протокола или клиентского программного обеспечения, неподходящих настроек аутентификации, недостаточных прав/полномочий), определите причину ее возникновения.
- ❒ Исходя из сценария поиска сетевых неисправностей, подразумевающего проблему с проводкой/инфраструктурой, выявите причину ее возникновения (возможно, это дефект носителя, помехи, неисправность сетевого аппаратного обеспечения или другие факторы).

Предметный указатель

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

А

Б

В

Г

Д

Е

Ж

З

И

К

Л

М

Н

О

П

P

C

Т

У

Ф

Х

Ц

Ч

Ш

Э

Я