ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
“УКРАЇНСЬКА АКАДЕМІЯ БАНКІВСЬКОЇ СПРАВИ
НАЦІОНАЛЬНОГО БАНКУ УКРАЇНИ”

О.О. Гордєєв, Д.В. Гордєєва, М.В. Колдовський

КОМП’ЮТЕРНІ МЕРЕЖІ

Навчальний посібник
для студентів вищих навчальних закладів

Рекомендовано Міністерством освіти і науки України

www.cisco.com www.rdm.com www.synergia.ua

Суми
ДВНЗ “УАБС НБУ”
2011

УДК 004.7(075.4)
ББК 32.965
Г68

Гриф наданий Міністерством освіти і науки України,
лист № 1/11-9229 від 05.10.2010

Рецензенти:
Т.С. Клебанова, доктор економічних наук, професор,
завідуюча кафедрою економічної кібернетики
Харківського національного економічного університету;
В.С. Харченко, доктор технічних наук, професор, завідувач кафедри
комп'ютерних систем та мереж Національного аерокосмічного
університету ім. М.Є. Жуковського "ХАІ";
Є.А. Лавров, доктор технічних наук, професор, завідувач кафедри
інформаційних систем у менеджменті Національного університету
біоресурсів і природокористування України

Гордєєв, О. О.

Г68 Комп'ютерні мережі [Текст] : навчальний посібник для студентів вищих навчальних закладів / О. О. Гордєєв, Д. В. Гордєєва, М. В. Колдовський ; Державний вищий навчальний заклад "Українська академія банківської справи Національного банку України". – Суми : ДВНЗ "УАБС НБУ", 2011. – 250 с.

ISBN 978-966-8958-72-4

Метою навчального посібника є забезпечення структурованими навчально-методичними матеріалами студентів для самостійного вивчення дисципліни "Комп'ютерні мережі". Видання містить навчально-методичні матеріали, методичні вказівки для виконання лабораторних робіт, питання для самостійного опрацювання та дискусій, завдання для самоконтролю та перевірки знань, термінологічно-тлумачний словник.

Посібник орієнтовано на студентів, які навчаються за напрямом 6.030502 "Економічна кібернетика". Він може бути корисним для студентів інших економічних і технічних напрямів підготовки.

УДК 004.7(075.4)
ББК 32.965

ISBN 978-966-8958-72-4

ЗМІСТ

ВСТУП

На сьогодні багато соціально-економічних процесів не можуть функціонувати та розвиватися без використання сучасних інформаційних технологій, до яких належать системи торгівлі на валютних та фондових ринках (e-trading), електронна комерція (e-commerce), електронний банкінг (e-banking) тощо. Зазначені інформаційні технології потребують гарантованої передачі великих обсягів даних на значні відстані. Ці потреби забезпечуються використанням сукупності комп'ютерних мереж.

З кожним роком вимоги до комп'ютерних мереж зростають, що обумовлює розвиток існуючих та появу нових технологій побудови комп'ютерних мереж, протоколів передачі даних, інструментальних засобів проектування комп'ютерних мереж та моделей обладнання. Це свідчить про необхідність появи оновлених навчальних посібників для вивчення курсу "Комп'ютерні мережі".

Пропонований посібник "Комп'ютерні мережі" розроблений відповідно до навчальної програми курсу "Комп'ютерні мережі" підготовки бакалаврів галузі знань 0305 "Економіка і підприємство" за напрямком 6.030502 "Економічна кібернетика". Він призначений для студентів зазначеної спеціальності усіх форм навчання і підготовлений з метою формування бази фундаментальних теоретичних знань та практичних навичок щодо використання сучасних технологій проектування комп'ютерних мереж та моделювання їх роботи за допомогою інструментальних засобів.

Відповідно до зазначеної мети при вивченні даної дисципліни передбачається вирішення таких завдань: вивчення теоретичних аспектів використання сучасних технологій при проектуванні комп'ютерних мереж; набуття практичних навичок із проектування комп'ютерних мереж з використанням сучасних інструментальних засобів; набуття практичних навичок при забезпеченні безпеки передачі даних у комп'ютерних мережах. Предметом вивчення є методологічні та технічні аспекти проектування комп'ютерних мереж.

Слід відзначити, що курс "Комп'ютерні мережі" є необхідним попереднім курсом для вивчення таких дисциплін, як "Безпека інформації", "Корпоративні системи", "Управління проектами інформатизації".

Зміст дисципліни надано у темах:

- класи та топології комп'ютерних мереж;
- модель OSI та інкапсуляція даних;

- середовище передачі даних та обладнання комп'ютерних мереж;
- технології побудови локальних комп'ютерних мереж;
- технології побудови розподілених комп'ютерних мереж;
- стеки протоколів комп'ютерних мереж;
- адресація в комп'ютерних мережах;
- маршрутизація в комп'ютерних мережах;
- методика проектування мережі та СКС;
- безпека комп'ютерних мереж.

Навчальний посібник містить необхідні матеріали, які сприятимуть самостійному вивченню дисципліни. У відповідних розділах подані вказівки до вивчення теоретичного матеріалу з кожної теми дисципліни, посилання на джерела, завдання для самоконтролю і перевірки знань, теми і питання для самостійного опрацювання. Також подані завдання та методичні вказівки до виконання лабораторних робіт.

1. ТИПОВА НАВЧАЛЬНА ПРОГРАМА КУРСУ

Тема 1. Класи та топології комп'ютерних мереж

Еволюція комп'ютерних мереж. Мережева архітектура. Системи пакетної обробки. Багатотермінальні системи. Поява перших локальних мереж. Локальні мережі. Мережева технологія. Класифікація комп'ютерних мереж. Комутація пакетів. Кампусна мережа. Міська мережа. Глобальна мережа. Топології комп'ютерних мереж. Топологія "шина". Топологія "кільце". Топологія "зірка". Топологія "зірка-шина". Інші можливі мережеві топології. Доступ до середовища передачі даних. Метод множинного доступу з контролем несучої і виявленням зіткнень (CSMA/CD). Метод множинного доступу з контролем несучої і запобіганням зіткнень (CSMA/CA). Маркерний метод. Загальні принципи побудови мереж. Розвиток, топологія та архітектура глобальної мережі Інтернет. Приклади мережевих топологій. Характеристики комп'ютерних мереж.

Тема 2. Модель OSI та інкапсуляція даних

Структура моделі OSI. Рівні моделі OSI. Фізичний рівень. Канальний рівень. Формування кадрів. Структура кадру. Розділення канального рівня на підрівні LLC та MAC. Мережевий рівень. Формування пакетів. Транспортний рівень. Формування сегментів. Сеансовий рівень. Представницький рівень. Прикладний рівень. Взаємодія між рівнями моделі OSI. Етапи інкапсуляції даних. Рух пакетів у мережі. Порівняння моделей TCP та OSI. Модель ATM. Переваги використання багаторівневих моделей для опису функціонування комп'ютерної мережі.

Тема 3. Середовище передачі даних та обладнання комп'ютерних мереж

Середовище передачі даних. Кабельні з'єднання. Види та структура коаксіального кабелю. Використання BNC-конекторів. Види та структура витої пари. Неекранована вита пара (UTP). Категорії неекранованої витої пари. Екранована вита пара (STP). Використання конекторів RJ-45. Види та структура оптоволоконного кабелю. Одномодовий оптоволоконний кабель. Багатомодовий оптоволоконний кабель. Бездротові з'єднання. MAC-адреси. Мережеві адаптери. Повторювачі. Концентратори. Мости. Комутатори. Маршрутизатори. Шлюзи. Супутниковий зв'язок та мобільні телефонні системи. Огляд номенклатури та характеристик активного мережевого обладнання на прикладі обладнання компанії Cisco Systems. Огляд номенклатури та

характеристик обладнання для тестування роботи комп'ютерних мереж на прикладі обладнання компанії Fluke.

Тема 4. Технології побудови локальних комп'ютерних мереж

Опис технології Ethernet та її характеристики. Опис технології Fast Ethernet та її характеристики. Опис технології Gigabit Ethernet та її характеристики. Опис технології 10 Gigabit Ethernet та її характеристики. Переваги та недоліки технологій Ethernet. Технологія Token Ring. Технологія Token Bus. Технологія FDDI. Технологія Wireless Ethernet. Стандарти IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n. Архітектура протоколів Fibre Channel. Методи забезпечення якості обслуговування (QoS). Віртуальні локальні мережі (VLAN). Технологія Bluetooth.

Тема 5. Технології побудови розподілених комп'ютерних мереж

Огляд технологій розподілених мереж (WAN). Служби розподілених мереж. Провайдери послуг розподілених мереж. Віртуальні канали розподілених мереж: постійні віртуальні канали, віртуальні канали, що комутуються. Типи каналів мереж WAN та їх пропускна здатність. Обладнання мереж WAN: маршрутизатори, комутатори розподіленої мережі, модеми, пристрої CSU/DSU, термінальні адаптери ISDN, комунікаційні сервери. Типи каналів розподілених мереж: виділені лінії, з'єднання із комутацією каналів, з'єднання із комутацією пакетів. Аналогові з'єднання віддаленого доступу (PSTN). Технологія ISDN. Технологія X.25. Технологія Frame Relay. Технологія ATM. Технологія DSL. Кабельні модеми. Проектування розподіленої мережі. Технологія Metro Ethernet. Технологія WiMAX. Використання протоколу PPP для розподілених мереж.

Тема 6. Стеки протоколів комп'ютерних мереж

Стек протоколів OSI. Протоколи FTAM, VTP, X.400, X.500. Стек протоколів TCP/IP. Протоколи IP, ICMP, IGMP, TCP, UDP, HTTP, FTP, TFTP, SNMP, Telnet, SSH, SMTP. Стек протоколів IPX/SPX. Протоколи IPX, RIP, NLSP, SPX, NCP, SAP. Стек протоколів NetBIOS/SMB. Протоколи NetBEUI, SMB. Прикладні протоколи. Транспортні протоколи. Мережеві протоколи. Історія та перспективи розвитку стеку протоколів TCP/IP. Специфікація протоколів прикладного рівня стеку TCP/IP. Специфікація протоколів транспортного рівня стеку TCP/IP.

Тема 7. Адресація в комп'ютерних мережах

Загальні принципи адресації у комп'ютерних мережах. Схеми адресації вузлів. Апаратні адреси (MAC–адреси). Символьні адреси. Числові складені адреси. Основи IP-адресації. Маска підмережі. Ідентифікатор вузла. Правила призначення IP-адрес мереж і вузлів. Класова і безкласова IP-адресація. IP-адреси для локальних мереж. Призначення IP-адрес. Планування адресації у мережі. Відображення IP-адрес на локальні адреси. Протокол дозволу адрес ARP. Протокол зворотного дозволу адрес RARP. Відображення доменних імен на IP-адреси. Сервіс DNS. Алгоритм роботи протоколу динамічної конфігурації вузлів в мережі DHCP. Формат пакету у протоколі IPv4. Опис роботи протоколу IPv6. Приклади адресації у комп'ютерних мережах.

Тема 8. Маршрутизація в комп'ютерних мережах

Основи маршрутизації. Принципи роботи засобів маршрутизації. Статична маршрутизація. Динамічна маршрутизація. Порівняння статичної та динамічної маршрутизації. Маршрутні протоколи. Протоколи маршрутизації. Дистанційно-векторний алгоритм маршрутизації. Алгоритм маршрутизації з урахуванням стану каналів. Збалансований гібридний алгоритм маршрутизації. Метод безкласової адресації CIDR. Метод призначення масок змінної довжини VLSM. Протокол маршрутизації RIPv2. Протокол маршрутизації OSPF.

Тема 9. Методика проектування мережі та СКС

Етапи проектування мережі. Вибір розміру і структури мережі. Вибір мережевої операційної системи. Вибір топології мережі та методу доступу. Вибір обладнання. Проектування структурованої кабельної системи (СКС). Основні стандарти СКС: ISO/IEC 11801 "Information technology – Generic cabling for customer premises", Європейський стандарт EN 50173 "Information technology – Generic cabling systems", Американський стандарт EIA/TIA-568B "Commercial Building Telecommunications Wiring Standard". Структура кабельної системи. Магістральна підсистема території. Магістральна підсистема будівлі. Горизонтальна підсистема. Топологія СКС. Технічні приміщення. Волоконно-оптичні компоненти СКС. Вимоги міжнародного стандарту ISO/IEC 11801:2002 до волоконно-оптичної частини СКС. Огляд, номенклатура та характеристики пасивного мережевого обладнання на прикладі обладнання компанії Reichle&De-Massari AG. Тестування оптоволоконних ліній та каналів СКС. Приклад проектування СКС.

Тема 10. Безпека комп'ютерних мереж

Антивірусна комп'ютерна програма (антивірус). Комп'ютерний вірус. Класифікація антивірусних рішень. Методи знешкодження небажаного програмного забезпечення. Мережеві екрани. Прикладний шлюз. Пакетний фільтр. Сканер вразливостей. Система виявлення вторгнень. Рішення попередження витоку інформації. Шифрування інформації. Симетричний алгоритм шифрування. Асиметричний алгоритм шифрування. Цифрові підписи. Управління відкритими ключами. Захист з'єднань. Протоколи аутентифікації.

ТЕМАТИЧНИЙ ПЛАН АУДИТОРНИХ ЗАНЯТЬ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ "КОМП'ЮТЕРНІ МЕРЕЖІ"

№ пор.	Назва теми	Погодинний розподіл навчального часу за темами			
		Лекції	Лабораторні заняття	СРС	Разом
1	Класи та топології комп'ютерних мереж	2	2	5	9
2	Модель OSI та інкапсуляція даних	2	2	5	9
3	Середовище передачі даних та обладнання комп'ютерних мереж	2	2	5	9
4	Технології побудови локальних комп'ютерних мереж	2	8	5	15
5	Технології побудови розподілених комп'ютерних мереж	2	4	5	11
6	Стеки протоколів комп'ютерних мереж	2	–	5	7
7	Адресація в комп'ютерних мережах	2	2	7	11
8	Маршрутизація в комп'ютерних мережах	2	2	7	11
9	Методика проектування мережі та СКС	2	4	5	11
10	Безпека комп'ютерних мереж	2	8	5	15
Всього		**20**	**34**	**54**	**108**

2. НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Тема 1. КЛАСИ ТА ТОПОЛОГІЇ КОМП'ЮТЕРНИХ МЕРЕЖ

Мета теми – познайомитися з передумовами виникнення комп'ютерних мереж; розглянути варіанти класифікацій комп'ютерних мереж; розглянути базові топології комп'ютерних мереж; розглянути основні методи доступу до середовища.

Ключові поняття: пакетна обробка даних, багатотермінальні системи, перші локальні мережі, класифікація комп'ютерних мереж, топології комп'ютерних мереж, методи доступу до середовища.

Еволюція комп'ютерних мереж. Системи пакетної обробки

Комп'ютерна мережа або *мережа передачі даних* являє собою деяку сукупність вузлів (комп'ютерів, робочих станцій чи іншого обладнання), з'єднаних комунікаційними каналами, а також набір обладнання, який забезпечує з'єднання станцій і передачу між ними інформації.

На сьогодні існує величезна кількість комп'ютерних мереж різного призначення, побудованих на основі різних комп'ютерних і комунікаційних технологій і обумовлених використанням тієї або іншої мережевої архітектури.

Мережева архітектура – це сукупність мережевих апаратних і програмних рішень, методів доступу та протоколів обміну інформацією.

Архітектура і номенклатура мережевого обладнання сучасних комп'ютерних мереж є результатом розвитку технічних засобів і викликані необхідністю користувачів комп'ютерної техніки обмінюватися між собою даними.

Звернімося до витоків комп'ютерних мереж. Перші комп'ютери 50-х років XX століття були громіздкими та дорогими, вони призначалися для невеликого кола користувачів. Досить часто такі комп'ютери займали цілі будівлі і були призначені для використання в режимі пакетної обробки, а не для інтерактивної роботи користувачів.

Системи пакетної обробки, як правило, будувалися на базі мейнфрейму – потужного та надійного комп'ютера універсального призначення. Користувачі готували перфокарти з даними та командами програм і передавали їх в обчислювальний центр (рис. 2.1.1). Оператори

вводили ці карти в комп'ютер, а роздруковані результати користувачі одержували, як правило, лише наступного дня. Таким чином, помилка в перфокарті означала, як мінімум, добову затримку. Звичайно, для користувачів інтерактивний режим роботи, при якому можна з термінала оперативно керувати процесом обробки своїх даних, був би зручніший. Розробники комп'ютерних мереж у той час значною мірою не враховували інтереси користувачів, оскільки намагалися досягти найбільшої ефективності роботи найдорожчого пристрою обчислювальної машини – процесора.

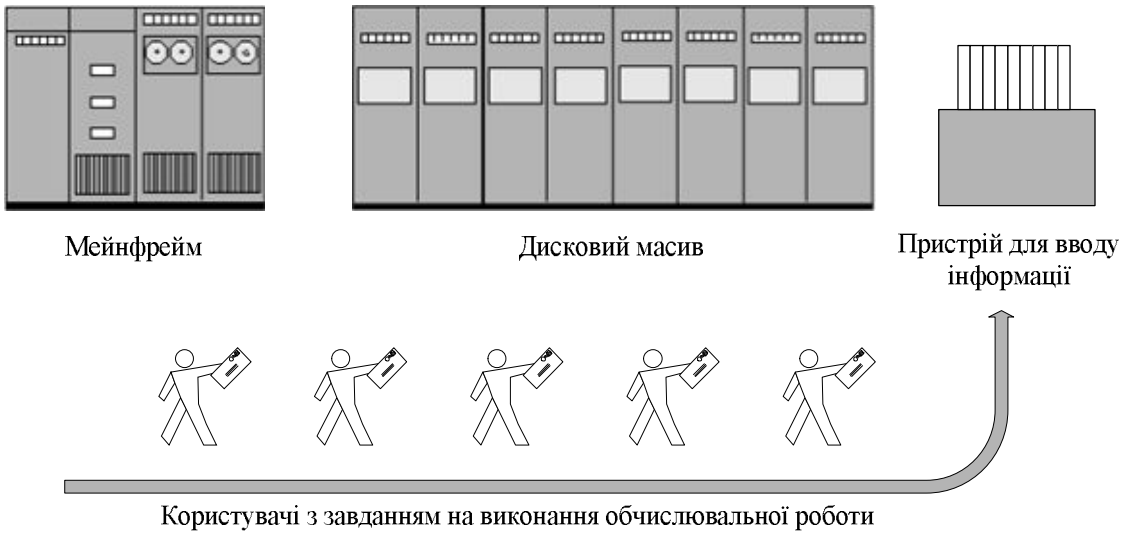


Рис. 2.1.1. Системи обробки даних на базі мейнфрейму

Багатотермінальні системи – прообраз мережі

В міру здешевлення процесорів на початку 60-х років XX століття з'явилися нові способи організації обчислювального процесу, які дозволили врахувати інтереси користувачів. Почали розвиватися інтерактивні *багатотермінальні системи розподілу часу* (рис. 2.1.2). У таких системах кожний користувач одержував власний термінал, за допомогою якого він міг вести діалог із комп'ютером. Кількість одночасно працюючих з комп'ютером користувачів залежала від його потужності, а час реакції обчислювальної системи був незначним, і користувачеві не дуже помітна була паралельна робота з комп'ютером інших користувачів.

Термінали, вийшовши за межі обчислювального центру, розосередилися по всьому підприємству. І хоча обчислювальна потужність залишалася повністю централізованою, деякі функції – такі, як введення й виведення даних, стали розподіленими. Подібні багатотермінальні централізовані системи зовні вже були дуже схожі на локальні

обчислювальні мережі. Дійсно, звичайний користувач сприймав роботу за терміналом мейнфрейму приблизно так само, як зараз він сприймає роботу з підключеним до мережі персональним комп'ютером. Користувач міг одержати доступ до загальних файлів і периферійного обладнання, при цьому в нього підтримувалася повна ілюзія одноособового володіння комп'ютером, тому що він міг запустити потрібну йому програму в будь-який момент і майже відразу одержати результат.

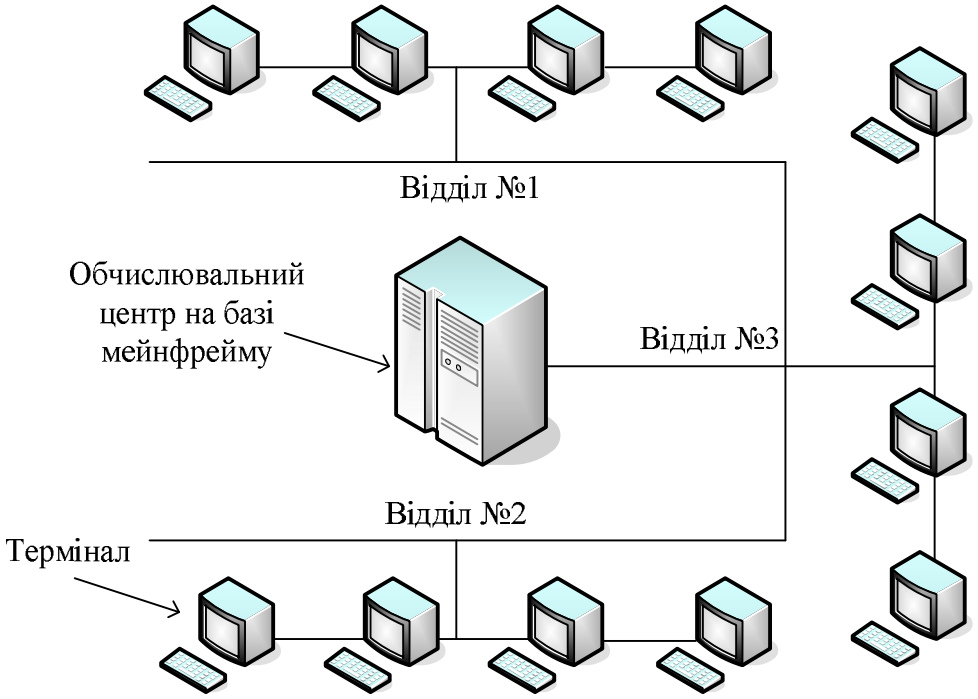


Рис. 2.1.2. Багатотермінальна система

Однак до появи локальних мереж потрібно було пройти ще великий шлях, тому що багатотермінальні системи, хоча й мали зовнішні риси розподілених систем, усе ще підтримували централізовану обробку даних. З іншого боку, і потреба підприємств у створенні локальних мереж у цей час ще не виникла – в одному будинку просто не було чого об'єднувати в мережу, тому що через високу вартість обчислювальної техніки підприємства не могли собі дозволити розкіш придбання декількох комп'ютерів. У цей період був справедливий закон Гроша, який емпірично відображав рівень технології того часу. Відповідно до цього закону швидкодія комп'ютера була пропорційна квадрату його вартості, звідси виходило, що за ту саму суму було вигідніше купити одну потужну машину, ніж дві менш потужні, так як їх сумарна потужність виявлялася значно меншою за швидкодію дорогої машини.

Поява перших локальних мереж

На початку 70-х років XX століття у результаті технологічного прориву у сфері виробництва комп'ютерних компонентів з'явилися *великі інтегральні схеми (ВІС)*. Їхня порівняно невисока вартість і гарні функціональні можливості привели до створення міні-комп'ютерів, які стали реальними конкурентами мейнфреймів. Емпіричний закон Гроша перестав відповідати дійсності, тому що десяток міні-комп'ютерів, маючи ту ж вартість, що й один мейнфрейм, вирішували деякі завдання набагато швидше.

Навіть невеликі підрозділи підприємств одержали можливість мати власні комп'ютери. Міні-комп'ютери вирішували задачі керування технологічним обладнанням, складом й інші задачі на рівні відділу підприємства. Таким чином, з'явилася концепція розподілу комп'ютерних ресурсів по всьому підприємству. Однак при цьому всі комп'ютери однієї організації, як і раніше, продовжували працювати автономно (рис. 2.1.3).

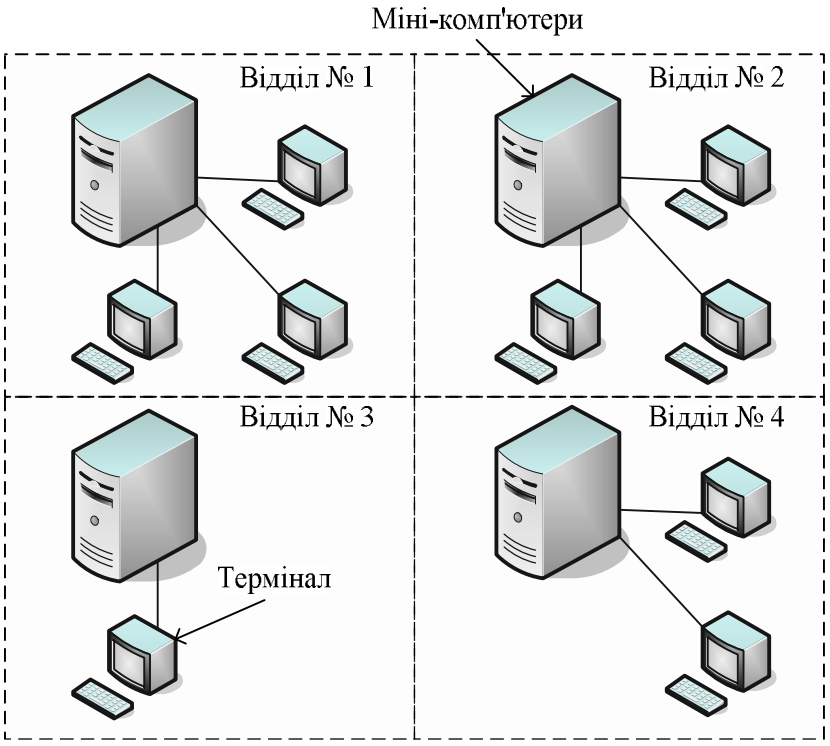


Рис. 2.1.3. Автономне використання декількох міні-комп'ютерів на одному підприємстві

Із часом потреби користувачів у швидкодії комп'ютерної техніки зростали. Їх вже не задовольняла ізольована робота на власному комп'ютері, користувачам хотілось обмінюватися комп'ютерними даними з користувачами інших підрозділів в автоматичному режимі.

Відповідь на цю потребу прийшла у вигляді появи перших локальних обчислювальних мереж (рис. 2.1.4).

Загалом представлені локальні мережі являють собою об’єднання комп’ютерів, зосереджених на невеликій території, як правило, у радіусі не більше 1-2 км, хоча в окремих випадках локальна мережа може мати й більші розміри, наприклад, кілька десятків кілометрів. У загальному випадку локальна мережа являє собою комунікаційну систему, що належить одній організації.

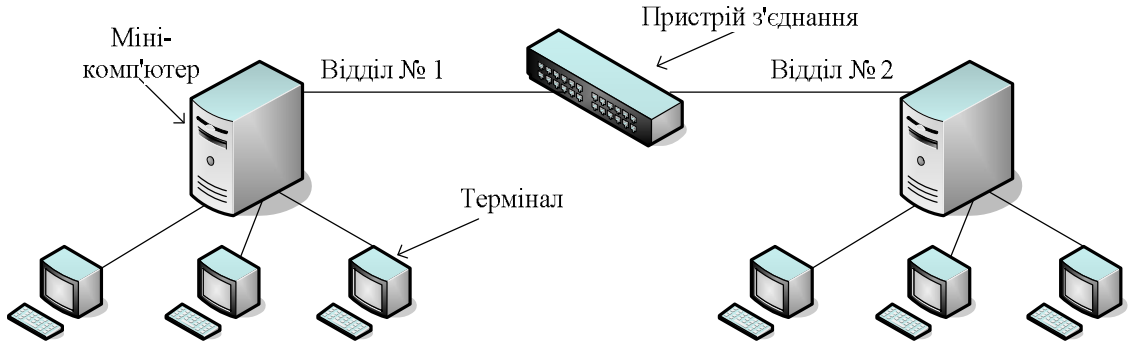


Рис. 2.1.4. Застосування пристроїв з’єднання для об’єднання відділів

Спочатку для з’єднання комп’ютерів один з одним використовувалися нестандартні мережеві технології.

Мережева технологія – це узгоджений набір програмних і апаратних засобів (наприклад, драйверів, мережевих адаптерів, кабелів і роз’ємів) і механізмів передачі даних лініями зв’язку, достатніх для побудови обчислювальної мережі.

Перші локал ьні мережі оснащувалися різноманітними пристроями з’єднання, які використовували власні способи представлення даних на лініях зв’язку, свої типи кабелів і т.д. Ці пристрої могли з’єднувати лише конкретні моделі комп’ютерів, для яких вони і були розроблені, наприклад, міні-комп’ютери PDP-11 з мейнфреймом IBM 360 або міні-комп’ютери HP з мікрокомп’ютерами LSI-11.

З’явилася необхідність уніфікації обладнання і технологій комп’ютерних мереж. Перші стандартні технології локальних мереж спиралися на принцип комутації, який був з успіхом випробуваний і довів свої переваги при передачі трафіка даних у глобальних комп’ютерних мережах.

У середині 80-х років XX століття затвердилися стандартні мережеві технології об’єднання комп’ютерів у мережу – Ethernet, ArcNet, Token Ring, Token Bus, трохи пізніше – FDDI.

Стандартні мережеві технології перетворили процес побудови локальної мережі з мистецтва в рутинну роботу. Для створення мережі досить було придбати стандартний кабель, мережеві адаптери відповідного стандарту (наприклад, Ethernet), встановити адаптери в комп'ютери, приєднати їх до кабелю стандартними з'єднувачами й установити на комп'ютери одну з популярних мережевих операційних систем (наприклад, Novell NetWare).

Прості алгоритми роботи визначили низьку вартість обладнання Ethernet. Широкий діапазон ієрархії швидкостей дозволяв раціонально будувати локальну мережу, обираючи ту технологію сімейства, яка найбільшою мірою відповідала завданням підприємства та потребам користувачів. Важливо також, що всі технології Ethernet дуже близькі одна до одної принципами роботи, що спрощувало обслуговування й інтеграцію цих мереж.

Класифікація комп'ютерних мереж

Різноманіття комп'ютерних мереж можна класифікувати за рядом ознак, зокрема:

1. *За технологією передачі даних* мережі поділяються на два типи:
   - віщання (або з'єднання один–до багатьох). При віщанні повідомлення, відправлене одним комп'ютером, одержують усі комп'ютери мережі;
   - з'єднання "точка-точка". З'єднання "точка-точка" передбачає використання індивідуального каналу зв'язку для обміну інформацією між комп'ютерами.
2. *За принципом організації обміну даними між абонентами* розрізняють мережі, побудовані на комутації:
   - каналів;
   - повідомлень;
   - пакетів.

Під комутацією розуміють технологію вибору напрямку й організації передачі даних у мережах, що мають кілька альтернативних маршрутів, за якими може проводитися обмін інформацією між двома вузлами.

Інформаційні потоки, що передаються при цьому мережею, називаються *мережевим трафіком* (від англ. *traffic* – рух).

Під комутацією каналів розуміють безпосереднє з'єднання двох вузлів за допомогою організації послідовності фізичних каналів зв'язку.

Мережа з комутацією каналів – тип комунікаційної мережі, у якій кожній парі абонентів надається фізичне з'єднання протягом сеансу їх інформаційної взаємодії. При цьому на час, протягом якого

здійснюється сеанс зв'язку між двома абонентами, канал зв'язку стає недоступним для використання іншими абонентами.

Комутація повідомлень розуміє під собою передачу між абонентами інформації у вигляді логічно завершених порцій даних, наприклад телеграм, листів або звітів. При цьому мережа з комутацією повідомлень працює аналогічно мережі з комутацією каналів, але фізичні канали зв'язку займаються не на період усього сеансу зв'язку, а тільки на період передачі повідомлення.

Мережі з комутацією повідомлень були прообразом для створення мереж з комутацією пакетів і на сьогоднішній день практично не використовуються.

Комутація пакетів – технологія доставки повідомлень, при якій дані, розбиті на окремі блоки малих розмірів, що називаються пакетами, можуть пересилатися з вихідного пункту в пункт призначення різними маршрутами. Пакети у пункті призначення потім збираються у початкові дані.

Мережа з комутацією пакетів – комунікаційна мережа, яка складається зі з'єднаних один з одним магістральними каналами вузлів комутації, у яких дані передаються у вигляді пакетів, із проміжним зберіганням цих пакетів на вузлах комутації. Зважаючи на малі розміри пакетів, що пересилаються, фізичні канали зв'язку виявляються зайнятими протягом мінімальних інтервалів часу, що дозволяє практично завжди забезпечити передачу даних між будь-якими вузлами мережі без тривалих затримок, викликаних необхідністю очікувати звільнення необхідного каналу зв'язку.

3. *За територіальною поширеністю* мережі можуть бути: локальні, кампусні, міські, глобальні.

Локальна мережа або *локальна обчислювальна мережа (Local Area Network – LAN)* – це мережа ЕОМ, яка містить у собі комп'ютери, що розташовані у межах одного приміщення, будинку або невеликої території, і дозволяє обмін даними та спільне використання різних пристроїв (принтерів, сканерів тощо).

Кампусна мережа (від англ. campus – університет, територія університету) – мережа, що охоплює територію університету або студентського містечка.

Міська мережа (*Metropolitan Area Network – MAN*) поєднує комп'ютери на території міського району або всього міста в цілому.

Глобальна мережа (*Wide Area Network – WAN*) – сукупність мереж, що поєднують територіально розосереджені комп'ютери, які перебувають у різних містах і країнах.

4. Крім того, мережі можуть поділятися *за топологією*. Топологією мережі може бути шина, зірка, кільце, дерево, повнозв'язна, комірчаста або змішана.
5. *За швидкістю передачі даних* мережі поділяються на:
   - низької швидкості (до 10 Мбіт/с);
   - середньої швидкості (до 100 Мбіт/с);
   - високої швидкості (більше 100 Мбіт/с).
6. *За типом середовища передачі даних* мережі розділяються на: дротові (коаксіальні, на витій парі, оптоволоконні) і бездротові (радіопередача, супутникові канали).
7. *За принципом організації ієрархії комп'ютерів* мережі бувають однорангові та з виділеним сервером.

Сервер (від англ. server – службовець) – це деякий об'єкт, що надає іншим об'єктам (як правило, вони називаються клієнтами) деякі послуги.

У комп'ютерних мережах сервером зазвичай називають комп'ютер або програму, яка надає клієнтам доступ мережею до своїх служб і ресурсів з метою обміну інформацією. Комп'ютер або програма, що обмінюється із сервером інформацією та використовує його служби і ресурси, називається клієнтом.

В однорангових мережах усі комп'ютери мають однакові, рівні права (ранги). У мережах з виділеним сервером розрізняють дві архітектури використання сервера:

- *файл-сервер* – дані та програми на вимогу користувача пересилаються із сервера на комп'ютер клієнту, де можуть бути оброблені;
- *клієнт-сервер* – виконання програм і обробка даних відбуваються на сервері за запитом користувача, клієнт якого одержує лише результати запиту.

Топології комп'ютерних мереж

При організації комп'ютерної мережі дуже важливим є вибір *топології*, тобто компонування мережевого обладнання і кабельної інфраструктури. Потрібно обрати таку топологію, яка забезпечила б надійну й ефективну роботу мережі, зручне керування потоками мережевих даних. Бажано також, щоб мережа за вартістю створення й супроводу вийшла недорогою, але в той же час, залишалися можливості для її подальшого розширення, також бажано, щоб залишилися можливості для переходу до більш швидкісних технологій зв'язку.

Вибір потрібної топології є складним завданням, для вирішення якого необхідно знати види топологій, їхні переваги та недоліки.

Базові мережеві топології

Існують три базові топології, на основі яких будується переважна більшість мереж: шина, зірка, кільце.

“*Шина” (Bus).* У цій топології усі комп’ютери з’єднуються один з одним кабелем (рис. 2.1.5). Послані в таку мережу дані передаються всім комп’ютерам, але обробляє їх лише той комп’ютер, апаратна MAC-адреса якого записана у кадрі як адреса одержувача.

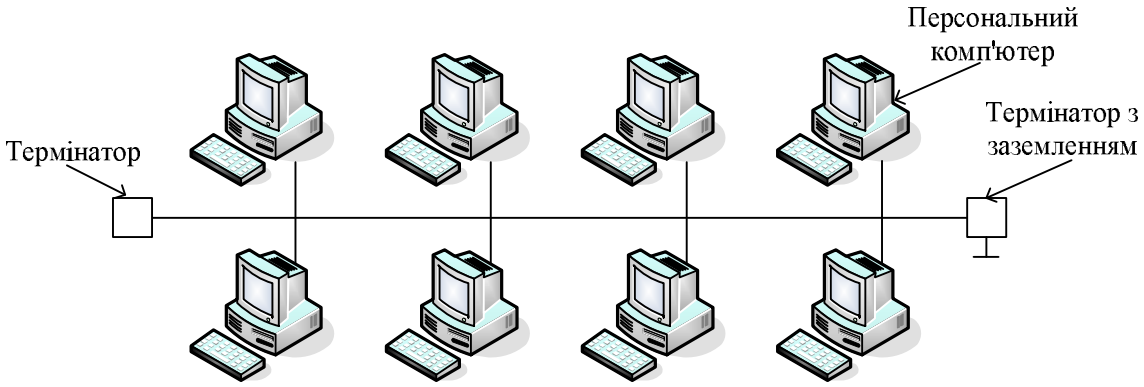


Рис. 2.1.5. Мережа з топологією “шина”

Ця топологія дуже проста в реалізації і дешева (вимагає найменше кабелю), однак має ряд істотних недоліків:

1. Такі мережі важко розширити (збільшити число комп’ютерів у мережі та кількість сегментів – окремих відрізків кабелю, що їх з’єднує).
2. Оскільки шина використовується спільно, у кожний момент часу передачу може вести тільки один з комп’ютерів. Якщо передачу одночасно починають два або більше комп’ютерів, виникає викривленість сигналу (*зіткнення,* або *колізія*), що приводить до пошкодження всіх кадрів. У цьому випадку комп’ютери змушені припиняти передачу, а потім по черзі ретранслювати дані. Вплив зіткнень тим помітніший, чим вищий обсяг переданої мережею інформації та чим більше комп’ютерів, підключених до шини. Ці два фактори знижують як максимально можливу, так і загальну продуктивність мережі, сповільнюючи її роботу.
3. “Шина” є пасивною топологією – комп’ютери тільки “прослуховують” кабель і не можуть відновлювати при передачі мережею сигнали, що затухають. Щоб подовжити мережу, потрібно використовувати *повторювачі* (*репітери*), що підсилюють сигнал перед його передачею в наступний сегмент.
4. Надійність мережі з топологією “шина” низька. Коли електричний сигнал досягає кінця кабелю, він, якщо не вжити спеціальних заходів, відбивається, порушуючи роботу всього сегмента мережі. Щоб

запобігти такому відбиттю сигналів, на кінцях кабелю встановлюються спеціальні *резистори* (*термінатори*), що поглинають сигнали. Якщо ж у будь-якому місці кабелю виникає обрив – наприклад, при порушенні цілісності кабелю або просто при від'єднанні конектора, – то виникають два незатерміновані сегменти, на кінцях яких сигнали починають відбиватися, і вся мережа перестає працювати.

Проблеми, характерні для топології "шина", привели до того, що ці мережі, настільки популярні ще декілька десятків років тому, зараз вже практично не використовуються.

"*Кільце*" *(Ring)*. У даній топології кожний з комп'ютерів з'єднується із двома іншими так, щоб від одного він одержував інформацію, а іншому передавав її (рис. 2.1.6). Останній комп'ютер підключається до першого, і кільце замикається.

Переваги топології кільце:

1. Оскільки кабелі не мають вільних кінців, то термінатори тут не потрібні.
2. Кожен комп'ютер виступає в ролі повторювача, підсилюючи сигнал, що дозволяє будувати мережі великого розміру.
3. Через відсутність зіткнень топологія має високу стійкість до перевантажень, забезпечуючи при цьому ефективну роботу з великими потоками інформації, що передаються мережею.

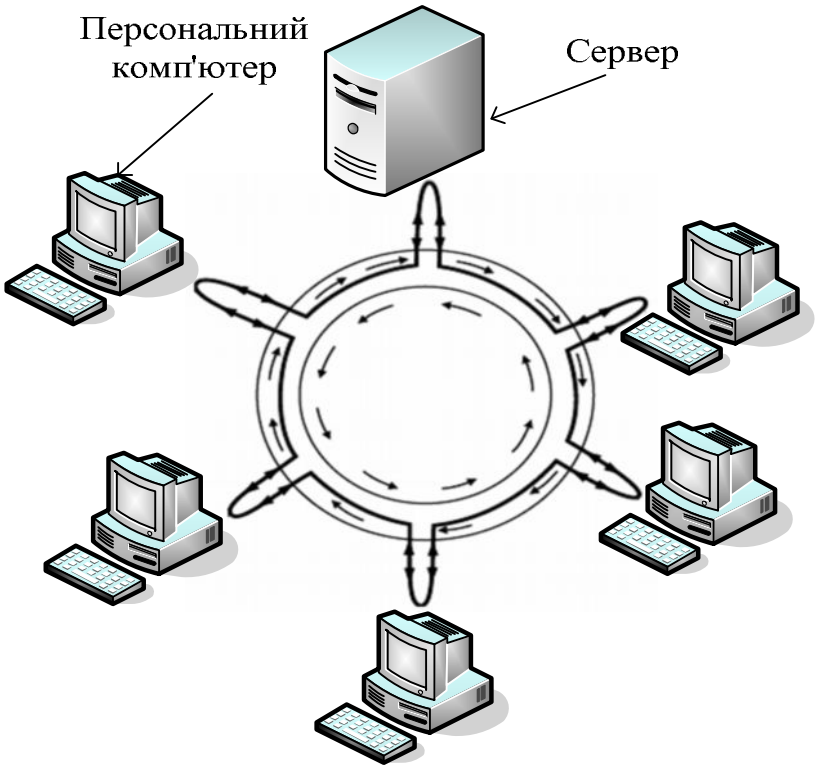


Рис. 2.1.6. Мережа з топологією "кільце"

Недоліки топології кільце:

1. Сигнал у “кільці” повинен пройти послідовно (і тільки в одному напрямку) через усі комп’ютери, кожний з яких перевіряє, чи не йому адресована інформація, тому час передачі може бути суттєвим.
2. Підключення до мережі нового комп’ютера або іншого пристрою потребує зупинки роботи всієї мережі, що порушує роботу інших комп’ютерів в мережі.
3. Вихід з ладу хоча б одного з комп’ютерів або пристрою порушує роботу всієї мережі.
4. Обрив або коротке замикання в будь-якому з кабелів кільця робить роботу всієї мережі неможливою.
5. Щоб запобігти зупинці мережі при відмові комп’ютера або обриві кабелю, як правило, прокладають два кільця, що суттєво здорожує мережу.

Активна топологія “зірка” (Active Star). Ця топологія виникла на зорі обчислювальної техніки, коли до потужного центрального комп’ютера підключалися всі інші абоненти мережі. У такій конфігурації всі потоки даних йшли виключно через центральний комп’ютер; він же повністю відповідав за керування інформаційним обміном між усіма учасниками мережі. Конфлікти при такій організації взаємодії в мережі були неможливі, однак навантаження на центральний комп’ютер було настільки великим, що нічим іншим, крім обслуговування мережі, цей комп’ютер, як правило, не займався. Вихід його з ладу приводив до відмови всієї мережі, тоді як відмова периферійного комп’ютера або обрив зв’язку з ним на роботі мережі не позначався. Зараз такі мережі зустрічаються досить рідко.

Топологія “зірка-шина” (Star Bus). Це найпоширеніша на сьогодні топологія. Периферійні комп’ютери підключаються не до центрального комп’ютера, а до пасивного концентратора, або хабу (hub) (рис. 2.1.7). Останній, на відміну від центрального комп’ютера, ніяк не відповідає за керування обміном даними, а виконує ті ж функції, що й повторювач, тобто відновлює вхідні сигнали й пересилає їх усім іншим підключеним до нього комп’ютерам і пристроям. Саме тому дана топологія, хоча фізично й виглядає як “зірка”, логічно є топологією “шина” (цей факт відображається у її назві).

Незважаючи на значні витрати кабелю, характерні для мереж типу “зірка”, ця топологія має істотні переваги перед іншими, що й обумовило її найпоширеніше застосування в сучасних мережах.

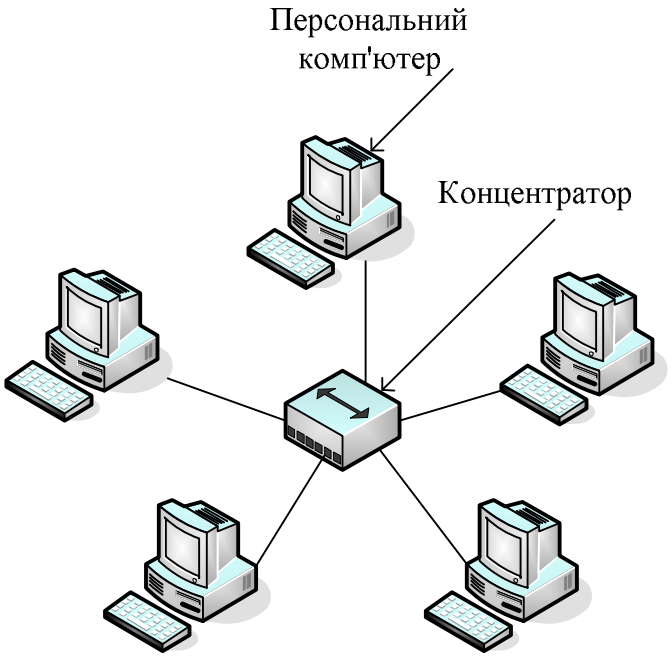


Рис. 2.1.7. Мережа з топологією “зірка-шина”

Переваги мереж типу “зірка-шина”:

1. Надійність – підключення до центрального концентратора й відключення комп’ютерів від нього ніяк не відображується на роботі іншої частини мережі; обриви кабелю впливають тільки на комп’ютери, які ним з’єднані; термінатори не потрібні.
2. Легкість при обслуговуванні й усуненні проблем – усі комп’ютери й мережеві пристрої підключаються до центрального з’єднального пристрою, що суттєво спрощує обслуговування й ремонт мережі.
3. Захищеність – концентрація точок підключення в одному місці дозволяє легко обмежити доступ до життєво важливих об’єктів мережі.

Відзначимо, що при використанні замість концентраторів більш “інтелектуального” мережевого обладнання (мостів, комутаторів і маршрутизаторів – докладніше про них буде розглянуто далі) отримуємо “проміжний” тип топології між активною й пасивною зіркою. У цьому випадку пристрій зв’язку не лише ретранслює вхідні сигнали, але й керує їх обміном.

Інші можливі мережеві топології

Реальні комп’ютерні мережі постійно розширюються і модернізуються. Тому майже завжди така мережа є гібридною, тобто її топологія являє собою комбінацію декількох базових топологій. Легко уявити собі гібридні топології, що є комбінацією “зірки” і “шини”, або “кільця” і “зірки”.

Однак особливо слід виділити *топологію "дерево" (Tree)*, яку можна розглядати як об'єднання декількох "зірок" (рис. 2.1.8). Саме ця топологія на сьогодні є найбільш популярною при побудові локальних мереж.

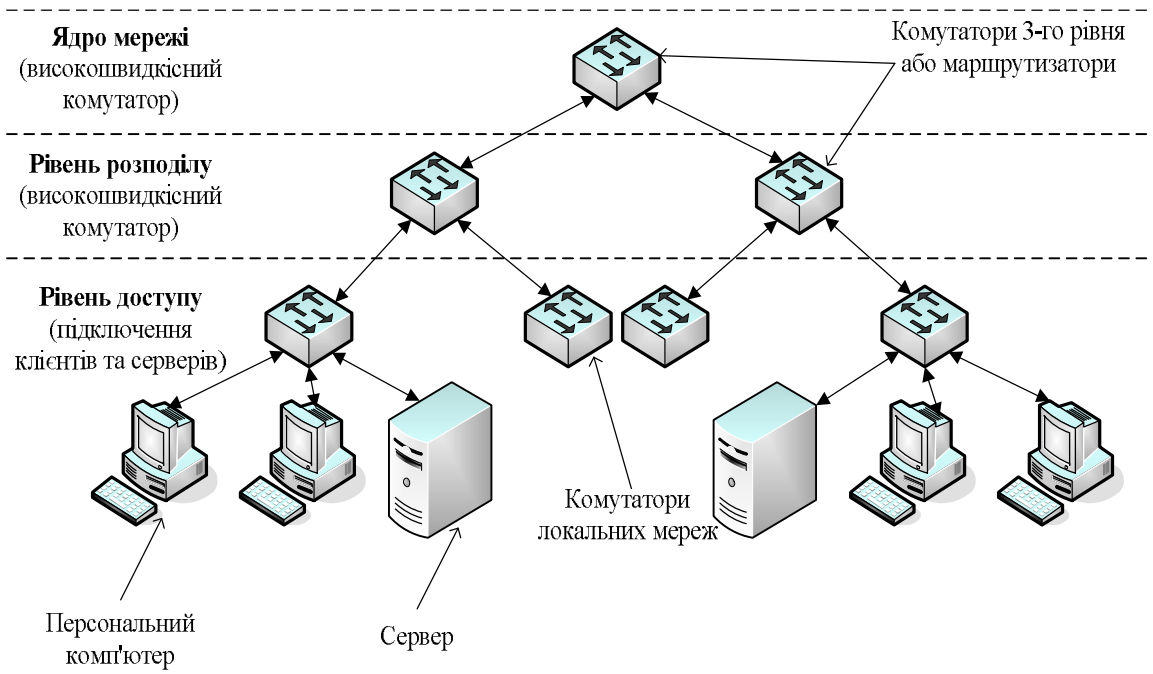


Рис. 2.1.8. Мережа з топологією "Дерево"

Також виділимо *повнозв'язну топологію,* що відповідає мережі, у якій кожен комп'ютер мережі пов'язаний з усіма іншими. Не дивлячись на логічну простоту, цей варіант є громіздким і неефективним, оскільки кожен комп'ютер в мережі повинен мати велику кількість комунікаційних портів, достатніх для зв'язку з кожним іншим комп'ютером мережі. Саме тому повнозв'язні топології застосовуються рідко.

Комірчаста топологія (mesh) виходить з повнозв'язної шляхом видалення деяких зв'язків (рис. 2.1.9). Така топологія є достатньо надійною – при обриві будь-якого каналу передача даних не припиняється, оскільки можливі декілька маршрутів доставки інформації. Комірчасті топології використовуються там, де потрібно забезпечити максимальну стійкість мережі, наприклад, при об'єднанні декількох ділянок мережі великого підприємства або при підключенні до Інтернету. При цьому суттєво збільшується витрата кабелю, ускладнюється мережеве обладнання і його налаштування.

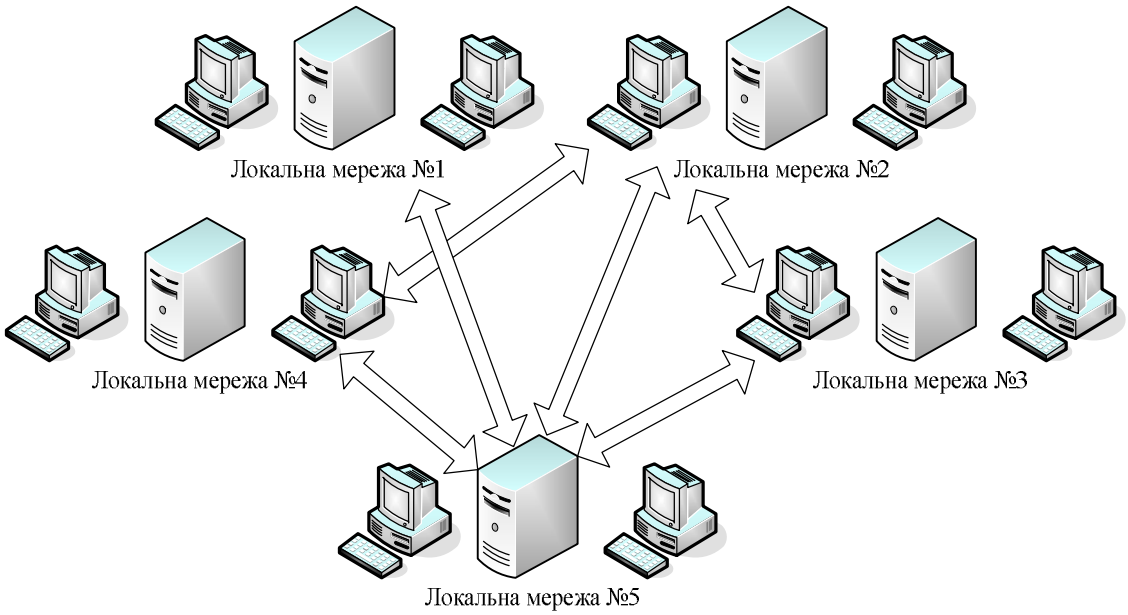


Рис. 2.1.9. Мережа з комірчастою топологією

Доступ до середовища передачі

З мережевою топологією тісно пов'язане поняття *способу доступу до середовища передачі*, під яким розуміється набір правил, що визначають, як саме комп'ютери повинні надсилати та приймати дані мережею.

Таких способів існує декілька. Основними з них є:

- множинний доступ з контролем несучої і виявленням зіткнень;
- множинний доступ з контролем несучої та запобіганням зіткнень;
- передача маркера.

При множинному доступі з контролем несучої і виявленням зіткнень (Carrier Sense Multiple Access with Collision Detection – CSMA/CD) усі комп'ютери (множинний доступ) "прослуховують" кабель (контроль несучої), щоб визначити, передаються по ньому дані чи ні. Якщо кабель вільний, будь-який комп'ютер може почати передачу, а всі інші комп'ютери повинні чекати, поки кабель не звільниться. Якщо комп'ютери почали передачу одночасно і виникло зіткнення, усі вони припиняють передачу (виявлення зіткнень), кожен на різні проміжки часу, після чого ретранслюють дані.

Серйозним недоліком цього способу доступу є те, що при великій кількості комп'ютерів і високому навантаженні на мережу число зіткнень зростає, а пропускна спроможність падає, іноді дуже істотно.

Однак цей метод дуже простий в технічній реалізації, тому саме він використовується в найбільш популярній сьогодні технології Ethernet. А щоб зменшити кількість зіткнень, у сучасних мережах застосовуються такі пристрої, як мости, комутатори і маршрутизатори.

Метод множинного доступу з контролем несучої і запобіганням зіткнень (Carrier Sense Multiple Access with Collision Avoidance – CSMA/CA) відрізняється від попереднього тим, що перед передачею даних комп'ютер посилає в мережу спеціальний невеликий пакет, повідомляючи іншим комп'ютерам про свій намір розпочати трансляцію. Так інші комп'ютери "дізнаються" про передачу, що дозволяє уникнути зіткнень. Звичайно, ці повідомлення збільшують загальне навантаження на мережу і знижують її пропускну здатність (через що метод CSMA/CA працює повільніше, ніж CSMA/CD), проте вони, безумовно, необхідні для роботи, наприклад, бездротових мереж.

У мережах *з передачею маркера (Token Passing)* від одного комп'ютера до іншого по кільцю постійно курсує невеликий блок даних, який називається маркером. Якщо у комп'ютера, що отримав маркер, немає інформації для передачі, він просто пересилає його наступному комп'ютеру. Якщо ж така інформація є, комп'ютер "захоплює" маркер, доповнює його даними і відсилає все це наступному комп'ютерові по колу. Такий інформаційний пакет передається від комп'ютера до комп'ютера, поки не досягне станції призначення. Оскільки в момент передачі даних маркер у мережі відсутній, інші комп'ютери вже не можуть нічого передавати. Тому в мережах з передачею маркера неможливі ні зіткнення, ні тимчасові затримки, що робить їх дуже привабливими для використання в системах автоматизації роботи підприємств.

Контрольні питання

1. Які властивості багатотермінальної системи відрізняють її від комп'ютерної мережі?
2. У чому полягає різниця між фізичними і логічними зв'язками?
3. За якими ознаками можна класифікувати комп'ютерні мережі?
4. Які переваги та недоліки конфігурації "зірка"? У яких локальних мережах вона застосовується?
5. Які переваги і недоліки топології "кільце"? У яких локальних мережах вона застосовується?
6. Які переваги і недоліки конфігурації "шина"? У яких локальних мережах вона застосовується?
7. У яких випадках в комп'ютерних мережах використовується "комірчаста" топологія?
8. Які методи доступу до середовища Вам відомі?

ЛІТЕРАТУРА: [3, 10, 14, 17, 23, 25, 33].

Тема 2. МОДЕЛЬ OSI ТА ІНКАПСУЛЯЦІЯ ДАНИХ

Мета теми – розглянути структуру еталонної моделі взаємодії відкритих систем – OSI; ознайомитися з функціями кожного рівня в рамках моделі OSI; розглянути етапи обробки інформації в розрізі моделі OSI; розглянути поняття інкапсуляції даних.

Ключові поняття: еталонна модель OSI, взаємодія між рівнями в моделі OSI, інкапсуляція даних.

Структура моделі OSI

За довгі роки існування комп'ютерних мереж була створена велика кількість різних мережевих протоколів. *Мережевий протокол* – це набір правил, що дозволяє здійснювати з'єднання та обмін даними між двома і більше включеними в мережу пристроями. Протоколи бувають як *відкриті* (опубліковані для безкоштовного застосування), так і *закриті* (розроблені комерційними компаніями, що вимагають ліцензування для використання). Однак усі ці протоколи прийнято співвідносити з так званою *еталонною моделлю взаємодії відкритих систем (Open Systems Interconnection Reference Model)*, або просто *моделлю OSI*. Її опис був опублікований у 1984 р. Міжнародною організацією зі стандартизації (International Standards Organization, ISO), тому для неї часто використовується інша назва: *модель ISO/OSI*. Ця модель являє собою набір специфікацій, які описують мережі з неоднорідними пристроями, вимоги до них, а також способи їх взаємодії.

Модель OSI має вертикальну структуру, у якій усі мережеві функції розподілені між сімома рівнями (рис. 2.2.1). Кожному такому рівню суворо відповідають певні операції, пристрої та протоколи.

Реальна взаємодія рівнів, тобто передача інформації усередині одного комп'ютера, можлива тільки по вертикалі та тільки із сусідніми рівнями, які розташовані вище або нижче.

Логічна взаємодія (відповідно до правил того або іншого протоколу) виконується горизонтально з аналогічним рівнем іншого комп'ютера на протилежному кінці лінії зв'язку. Кожний більш високий рівень користується послугами більш низького рівня, знаючи, у якому вигляді і яким способом (тобто через який інтерфейс) потрібно передати йому дані.

Завдання більш низького рівня – прийняти дані, додати свою інформацію (наприклад, адресну, яка необхідна для правильної взаємодії з аналогічним рівнем на іншому комп'ютері) і передати дані далі. Тільки дійшовши до найнижчого, фізичного рівня, мережевої моделі, інформація попадає в середовище передачі та досягає комп'ютера-одержувача. У ньому вона проходить крізь усі рівні у зворотному порядку, поки не досягне того ж рівня, з якого була передана комп'ютером-відправником.

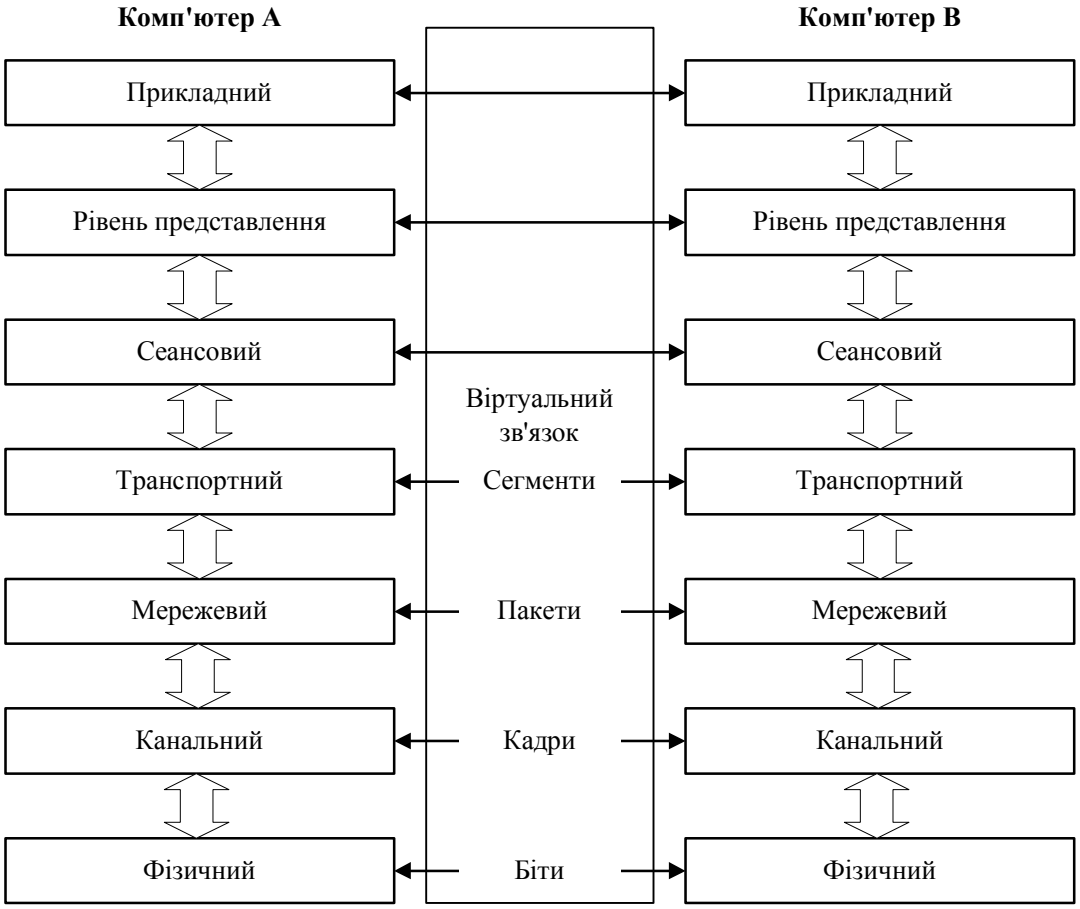


Рис. 2.2.1. Взаємодія між рівнями моделі OSI

Тепер познайомимося ближче з рівнями моделі OSI і визначимо мережеві послуги, які вони надають суміжним рівням.

Рівні моделі OSI

Рівень 0. Він не визначений у загальній схемі (див. рис. 2.2.1), але досить важливий для розуміння. Тут представлені посередники, якими власне і відбувається передача сигналів: кабелі різних типів, радіосигнали, ІЧ- сигнали і т.д. На цьому рівні нічого не описується, рівень 0 надає фізичному рівню 1 тільки *середовище передачі*.

Рівень 1 – Фізичний (Physical). Тут здійснюється передача неструктурованого потоку бітів, отриманих від канального рівня 2, по фізичному середовищу, наприклад, у вигляді електричних або світлових сигналів. При прийомі/отриманні з лінії зв’язку дані декодуються та передаються для подальшої обробки канальному рівню. Фізичний рівень відповідає за *підтримку зв’язку (link)*, тобто здійснює інтерфейс між мережевим носієм та мережевим пристроєм. На цьому рівні регламентуються напруги, частоти, довжини хвиль, типи конекторів, число й функціональність контактів, схеми кодування сигналів тощо.

Рівень 2 – Канальний (Data Link). Забезпечує *безпомилкову передачу даних*, отриманих від мережевого рівня 3, через фізичний рівень 1, який сам по собі відсутності помилок не гарантує та може видозмінювати дані. Інформація на цьому рівні розміщується в *кадрах (frames)*, де на початку *(у заголовку кадру*) розміщується адреса одержувача та відправника, а також керуюча інформація, а наприкінці – *контрольна сума*, яка дозволяє виявити виникаючі при передачі помилки (рис. 2.2.2).

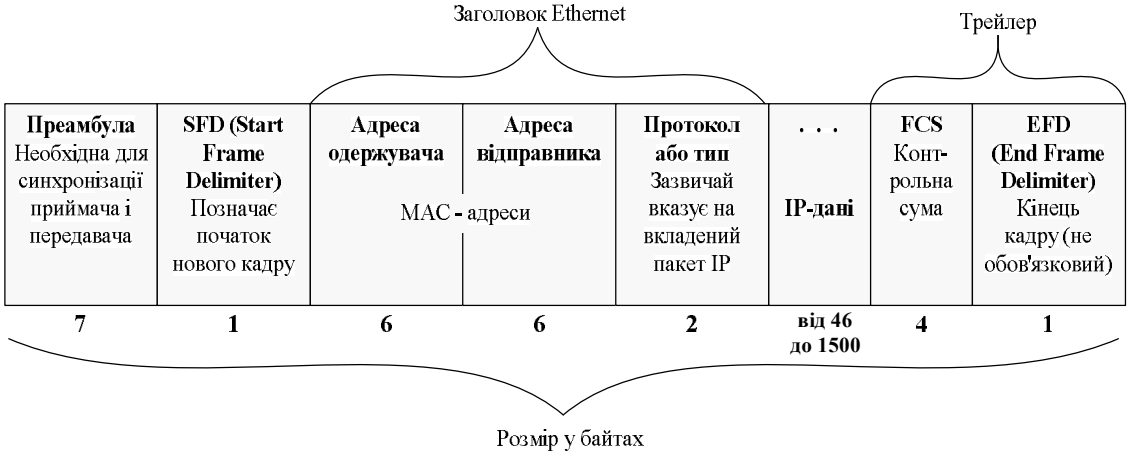


Рис. 2.2.2. Структура кадру

При одержанні даних на канальному рівні визначається початок і кінець кадру в потоці бітів. Сам кадр виймається з потоку та перевіряється на наявність помилок. Пошкоджені при передачі кадри, а також кадри, для яких не отримане підтвердження про прийняття, пересилаються заново *(ретранслюються)*. Але функція виправлення помилок за рахунок повторної передачі пошкоджених кадрів є необов'язковою, тому у деяких реалізаціях канального рівня вона відсутня, наприклад, у Ethernet, Token Ring, FDDI. Також на канальному рівні забезпечується керування доступом до середовища передачі.

Канальний рівень досить складний, тому у відповідності до *стандартів IEEE (Institute of Electrical and Electronics Engineers)*, випущених в лютому 1980 р. у рамках "*Проекту 802" (Project 802),* його часто розбивають на два підрівні (рис. 2.2.3)*: управління доступом до середовища (Media Access Control – MAC)* і *управління логічним зв'язком (Logical Link Control – LLC).*

Рівень MAC забезпечує спільний доступ мережевих адаптерів до фізичного рівня, визначення меж кадрів, розпізнавання *адрес призначення кадрів* (ці адреси часто називають фізичними, або MAC-адресами).

Рівень LLC, який діє над рівнем MAC, відповідає за встановлення каналу зв’язку та за безпомилкову відправку й приймання повідомлень із даними.

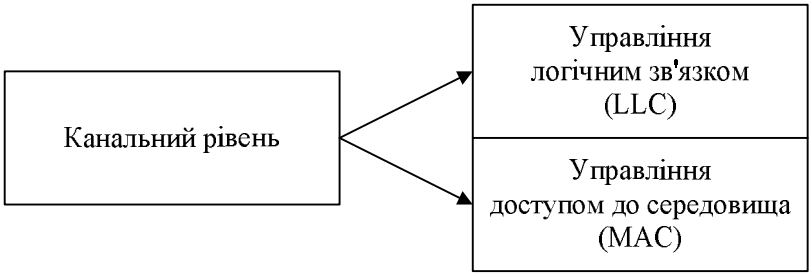


Рис. 2.2.3. Розділення канального рівня на підрівні LLC та MAC

Рівень 3 – Мережевий (Network). Цей рівень забезпечує доставку даних між двома вузлами в мережі. Повідомлення мережевого рівня називають *пакетами (packets)*. Головна задача мережевого рівня – це пошук маршруту від одного комп’ютера до іншого і передача пакета цим маршрутом. Пакет узагальнено складається із заголовка і поля даних. У полі даних розміщується сегмент транспортного рівня, а заголовок містить службову інформацію, а також адреси відправника та одержувача. На мережевому рівні вводиться адресація комп’ютерів. Адреси мережевого рівня називають логічними адресами, оскільки адресація не залежить від апаратного забезпечення. Адресація мережевого рівня ієрархічна, адреса складається мінімум з двох частин – номера мережі і номера вузла у цій мережі. Передача даних між мережами здійснюється за допомогою спеціальних пристроїв, які називаються *маршрутизаторами*. Основні задачі маршрутизатора – визначення маршруту і комутація пакета. Задача вибору маршруту називається *маршрутизацією*.

Рівень 4 – Транспортний (Transport). Цей рівень пов’язує більш високі рівні, які сильно залежать від додатків, з нижніми рівнями, які більше прив’язані до ліній зв’язку. На транспортному рівні відбувається розбиття потоку даних на сегменти при відправленні даних або збирання вихідного потоку даних із сегментів при прийманні. *Сегментом* називається блок даних транспортного рівня. Транспортний рівень призначений для доставки даних без помилок, втрат і дублювання в тій послідовності, у якій вони були передані. Він забезпечує передачу даних між двома додатками з необхідним рівнем надійності. Протоколи транспортного рівня, які гарантують надійну доставку даних, встановлюють перед обміном даними віртуальне з’єднання та у випадку втрати або пошкодження сегментів повторно їх відправляють (наприклад, TCP). Протоколи ненадійної доставки не ретранслюють дані (наприклад, UDP).

Рівень 5 – Сеансовий (Session). Дозволяє двом мережевим додаткам на різних комп'ютерах встановлювати, підтримувати й завершувати з'єднання, яке називається *мережевим сеансом*. Цей рівень також відповідає за відновлення аварійно перерваних сеансів зв'язку. Крім того, на п'ятому рівні виконується перетворення зручних для людей імен комп'ютерів у мережеві адреси (розпізнавання імен), а також реалізуються функції захисту сеансу.

Рівень 6 – Рівень представлення даних (Presentation). Визначає формати переданої між комп'ютерами інформації. Тут вирішуються такі завдання, як перекодування, стиск і розпакування даних, шифрування й дешифрування, підтримка мережевих файлових систем і т.д.

Рівень 7 – Прикладний, або Рівень додатків (Application). Забезпечує інтерфейс взаємодії програм, які працюють на комп'ютерах у мережі. Саме за допомогою цих програм користувач одержує доступ до таких мережевих послуг, як обмін файлами, передача електронної пошти, віддалений термінальний доступ і т.д.

Інкапсуляція даних

Щоб зрозуміти структуру та принципи функціонування мережі, необхідно усвідомити, що будь-який обмін даними в мережі здійснюється від джерела до одержувача (рис. 2.2.4). Інформацію, відправлену в мережу, називають *даними*, або *пакетами даних*. Якщо один комп'ютер (джерело) бажає послати дані іншому комп'ютеру (одержувачу), то дані спочатку повинні бути зібрані в пакети в процесі *інкапсуляції*, тобто перед відправленням у мережу комп'ютер поміщує дані у заголовок конкретного протоколу. Цей процес можна порівняти з підготовкою бандеролі до відправлення – обернути вміст папером, вкласти в транспортний конверт, вказати адресу відправника й одержувача, наклеїти марки й кинути в поштову скриньку.

Кожний рівень еталонної моделі залежить від послуг нижнього рівня. Щоб забезпечити ці послуги, нижній рівень за допомогою процесу інкапсуляції розміщує *PDU (Protocol Data Unit – узагальнена назва фрагменту даних на різних рівнях моделі OSI)*, отриманий від верхнього рівня, у своє поле даних. Потім можуть додаватися заголовки й трейлери, необхідні рівню для реалізації своїх функцій. Згодом, у міру переміщення даних униз по рівнях моделі OSI, до них будуть прикріплюватися додаткові заголовки й трейлери.

Наприклад, мережевий рівень забезпечує підтримку рівня представлення даних, який, у свою чергу, передає дані в міжмережеву підсистему (рис. 2.2.5).

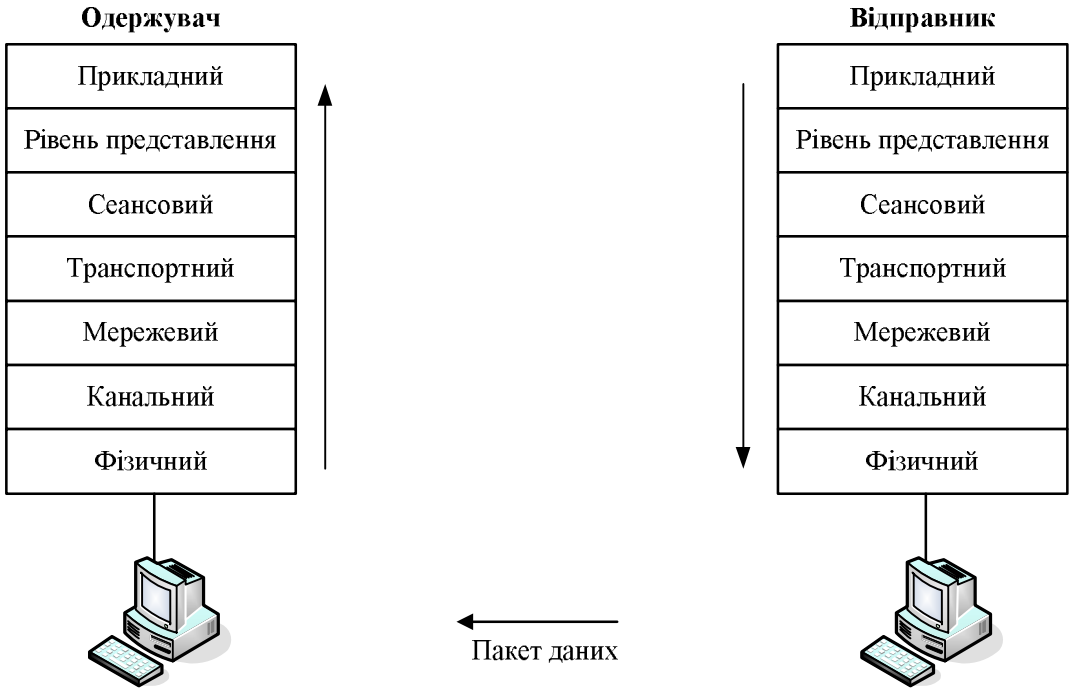


Рис. 2.2.4. Рух пакетів у мережі

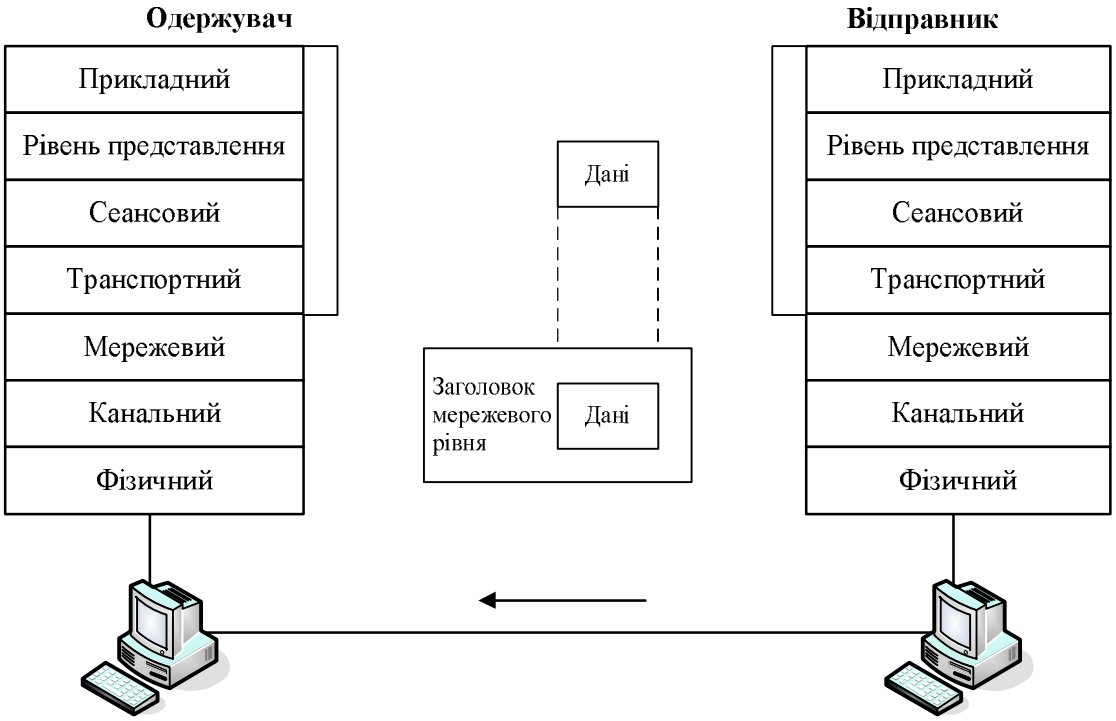


Рис. 2.2.5. Інкапсуляція даних в мережевий заголовок

Завданням мережевого рівня є переміщення даних через мережевий комплекс. Для виконання цього завдання дані інкапсулюються в заголовок, який містить інформацію, необхідну для виконання передачі, наприклад, логічні адреси відправника та одержувача (IP-адреси).

У свою чергу, канальний рівень слугує для підтримки мережевого рівня (рис. 2.2.6) та інкапсулює інформацію від мережевого рівня в кадри. Заголовок кадру містить дані (наприклад, фізичні адреси), необхідні канальному рівню для виконання його функцій.

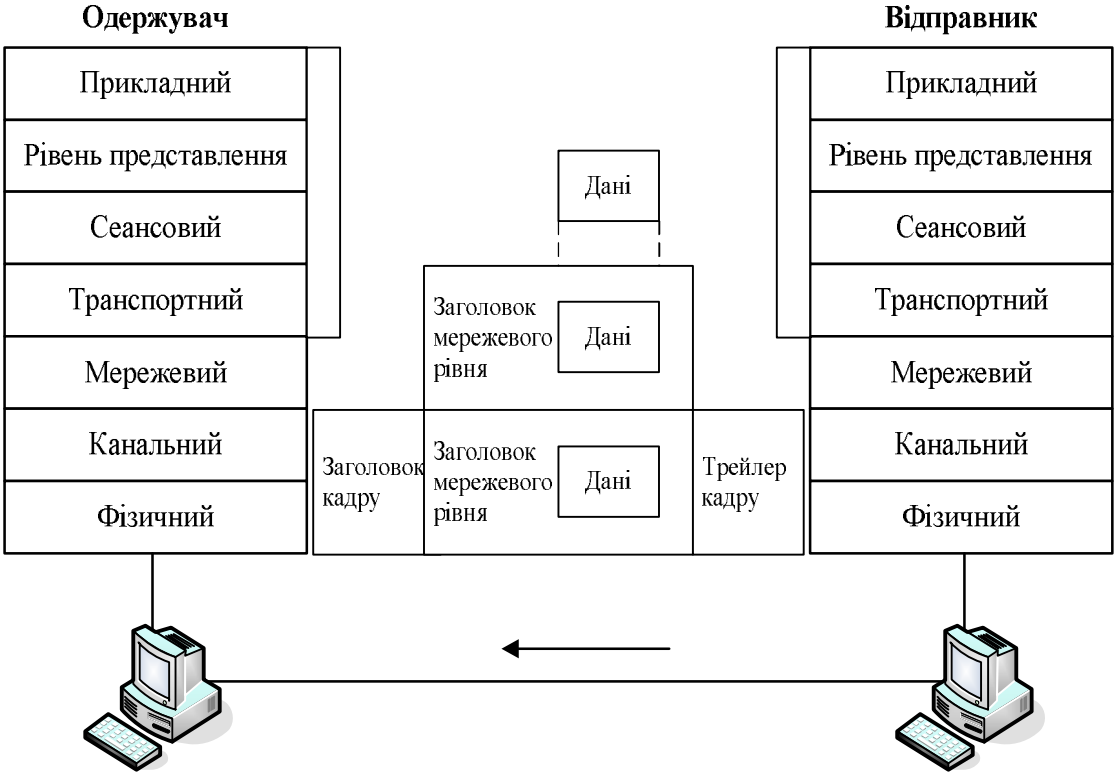


Рис. 2.2.6. Розміщення інформації в кадрі

Фізичний рівень слугує для підтримки канального рівня. Кадри канального рівня перетворюються в послідовність нулів і одиниць для передачі фізичними каналами (як правило, кабелями) (рис. 2.2.7).

При виконанні мережами послуг користувачам, потік і вид упакування інформації змінюється. У наведеному на рис. 2.2.8 прикладі інкапсуляції мають місце п’ять зазначених нижче етапів перетворення.

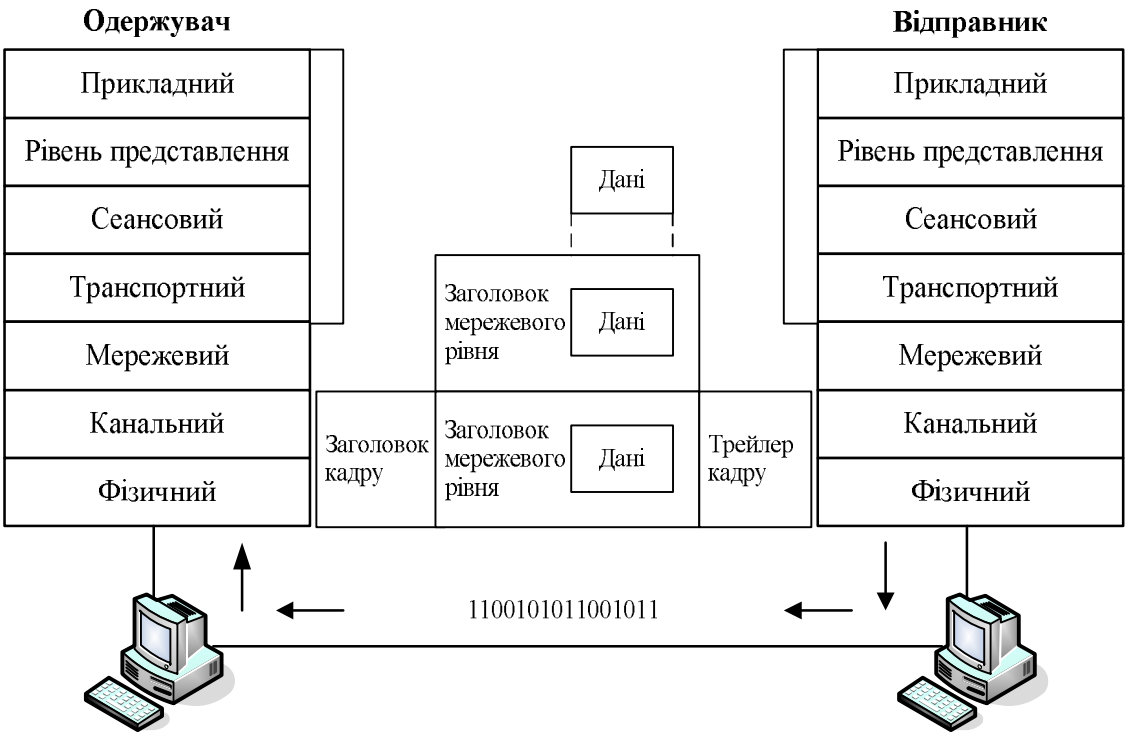


Рис. 2.2.7. Перетворення кадру в послідовність нулів і одиниць

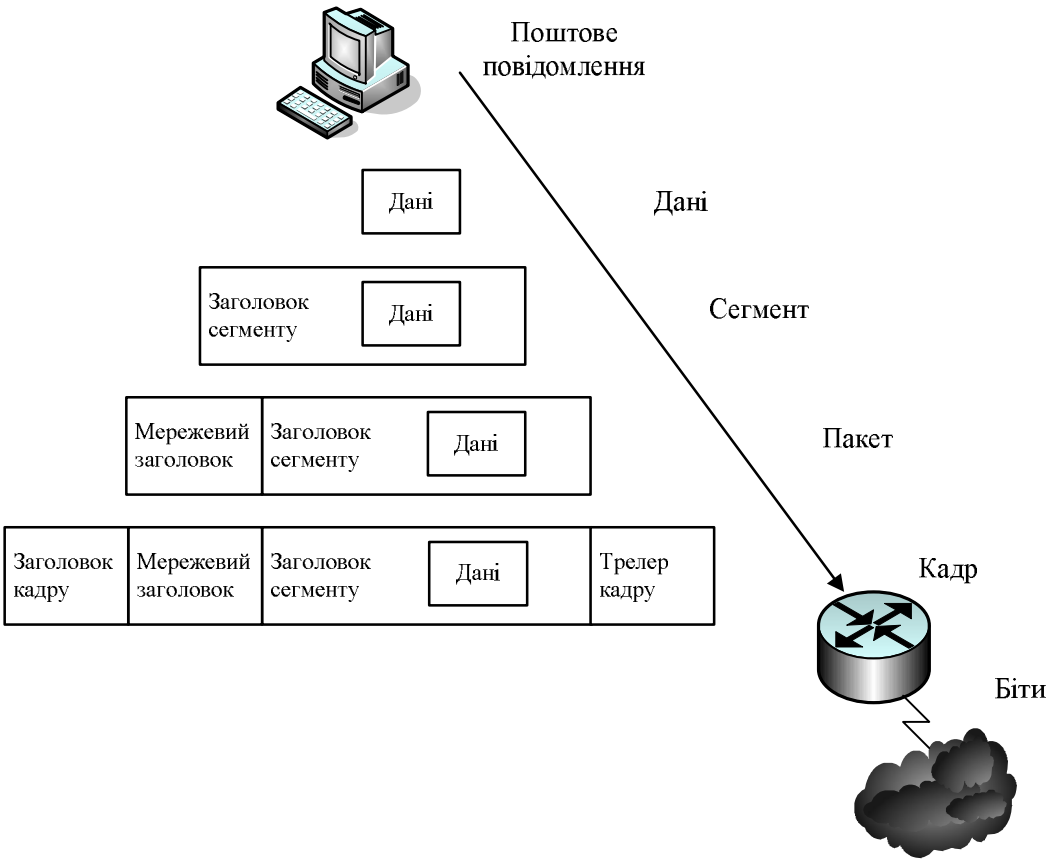


Рис. 2.2.8. Додавання нових заголовків та трейлерів

1. *Формування даних.* Коли користувач відправляє повідомлення електронною поштою, алфавітно-цифрові символи повідомлення перетворюються в дані, які можуть переміщуватися в мережевому комплексі.

2. *Пакування даних для наскрізного транспортування.* Для передачі даних через мережевий комплекс вони відповідним чином упаковуються. Завдяки використанню сегментів транспортна функція гарантує надійне з'єднання хост-машин, що беруть участь в обміні повідомленнями, на обох кінцях поштової системи.

3. *Додавання мережевої адреси в заголовок (IP-адреси).* Дані розміщуються в пакеті або дейтаграмі, яка містить мережевий заголовок з логічними адресами відправника й одержувача. Ці адреси допомагають мережевим пристроям передавати пакети через мережу обраним шляхом.

4. *Додавання локальної адреси в канальний заголовок (MAC-адреси).* Кожен мережевий пристрій повинен помістити пакети в кадр. Кадри дозволяють взаємодіяти з найближчим, безпосередньо підключеним, мережевим пристроєм у каналі. Кожен пристрій, який перебуває на шляху руху даних мережею, вимагає формування кадрів для з'єднання з наступним пристроєм.

5. *Перетворення в послідовність бітів при передачі.* Для передачі фізичними каналами (як правило, кабелями) кадр повинен бути перетворений у послідовність одиниць і нулів. Функція тактування дає можливість пристроям розрізняти ці біти в процесі їх переміщення в середовищі передачі даних. Середовище на різних ділянках шляху проходження може змінюватися. Наприклад, повідомлення електронної пошти може виходити із локальної мережі, потім перетинати магістральну мережу комплексу будинків і далі виходити в глобальну мережу, доки не дійде до одержувача, який перебуває у віддаленій локальній мережі.

Таким чином, при передачі даних від відправника до одержувача дані спочатку надходять на прикладний рівень, з прикладного – на рівень представлення, з рівня представлення на сеансовий, а далі – на транспортний рівень. На транспортному рівні потік даних розбивається на сегменти. На мережевому рівні сегмент інкапсулюється в пакет, на канальному рівні пакет інкапсулюється в кадр, а кадр на фізичному рівні біт за бітом передається через середовище передачі даних. Одержувач здійснює зворотний процес (*декапсуляцію*), тобто з кадра витягується пакет, з пакета витягується сегмент. На транспортному рівні із сегментів збирається вихідний потік даних, після чого дані передаються на сеансовий рівень, далі – на рівень представлення, далі – на прикладний рівень. Прикладний рівень передає дані з додатка одержувачу.

Контрольні питання

1. Що розуміється під терміном “мережевий протокол”?
2. Які мережеві функції виконуються в моделі OSI?
3. Який рівень згідно з моделлю OSI відповідає за вибір маршруту передачі даних?
4. За що відповідають підрівні LLC и MAC?
5. На якому рівні моделі OSI взаємодіють програми, забезпечуючи передачу повідомлень електронної пошти?
6. У якій послідовності здійснюється інкапсуляція даних?
7. У чому відмінність фрагментів інформації між собою: сегмент, пакет, кадр?

ЛІТЕРАТУРА: [1, 2, 17, 20, 23, 31, 33].

Тема 3. СЕРЕДОВИЩЕ ПЕРЕДАЧІ ДАНИХ ТА ОБЛАДНАННЯ КОМП’ЮТЕРНИХ МЕРЕЖ

Мета теми – розглянути різні типи середовищ передачі даних; познайомитися зі структурою коаксіального кабелю, витої пари, оптоволоконного кабелю; розглянути типи мережевого обладнання.

Ключові поняття: середовище передачі даних, мережеве обладнання, MAC-адреса, мережевий адаптер, концентратор, міст, комутатор, маршрутизатор, шлюз.

Середовище передачі даних

Середовищем передачі даних називається фізичне середовище, придатне для проходження сигналу. Щоб комп’ютери могли обмінюватися кодованою інформацією, середовище повинно забезпечити їхнє фізичне з’єднання один з одним.

Можна виділити два основні середовища передачі даних:

- дротове (за участю кабелів);
- бездротове (без участі кабелів).

Найчастіше в комп’ютерних мережах застосовуються кабельні з’єднання, які виступають як середовище передачі електричних або оптичних сигналів між комп’ютерами та іншими мережевими пристроями. При цьому використовуються наступні типи кабелю:

- коаксіальний кабель;
- неекранована вита пара;
- екранована вита пара;
- оптоволоконний кабель.

Основні проблеми, характерні для всіх дротових мереж – їхня низька мобільність, досить великі капіталовкладення у кабельну інфраструктуру і відносно мала дальність передачі сигналу. Бездротових

мереж це стосується меншою мірою, тому вони все частіше входять у наше життя. Для бездротової передачі даних використовують декілька способів:

- технологію радіозв'язку;
- передачу у мікрохвильовому діапазоні;
- інфрачервоне випромінювання;
- світлове випромінювання у видимому діапазоні (лазерна технологія).

Кабельні з'єднання застосовуються у високошвидкісній передачі даних на обмежених відстанях. При побудові мобільних мереж, великих корпоративних мереж або глобальних мереж застосовується комбінація кабельних та бездротових з'єднань.

Кабельні з'єднання

Коаксіальний кабель (coaxial cable). Коаксіальний кабель складається із зовнішнього циліндричного пустотілого провідника, що оточує один внутрішній дріт (рис. 2.3.1).

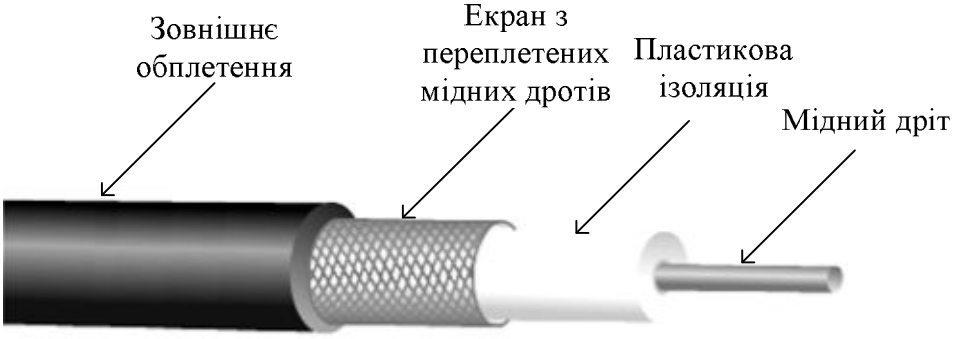


Рис. 2.3.1. Структура коаксіального кабелю

Коаксіальний кабель складається із двох провідних елементів. Один з них – мідний дріт, який перебуває в центрі кабелю й оточений шаром гнучкої ізоляції. Поверх ізоляційного матеріалу розташований екран з тонких переплетених мідних дротів або з металевої фольги, який в електричному колі відіграє роль другого дроту. Зовнішнє оплетення слугує для екранування центрального дроту від впливу перешкод. Зовні екран покритий оболонкою.

Для локальних мереж застосування коаксіального кабелю надає декілька переваг:

- коаксіальний кабель може використовуватися без посилення сигналу на більших відстанях, ніж екранована або неекранована вита пара. Це означає, що сигнал може проходити довші відстані між мережевими вузлами без повторювача для посилення сигналу;
- коаксіальний кабель дешевше за оптоволоконний.

Нарешті, протягом довгого часу коаксіальний кабель використовувався у всіх типах обміну даними, що дозволило добре вивчити дану технологію.

За товщиною коаксіальний кабель, який використовується у комп'ютерних мережах, можна розділити на два види: *товстий (Thicknet)* і *тонкий (Thinnet)*.

Як правило, з більш товстим кабелем працювати менш зручно. Про це слід пам'ятати, особливо якщо кабель треба буде прокладати по вже існуючих коробах і жолобах з обмеженим розміром. Він досить твердий через екран. У деяких ситуаціях прокласти товстий кабель досить складно, тому необхідно пам'ятати, що чим складніше середовище передачі даних в монтажі, тим дорожчий і сам монтаж. З тонким коаксіальним кабелем працювати зручніше – він більш гнучкий.

На кінцях коаксіального кабелю, як правило, використовується спеціальний роз'єм – *BNC-конектор* (рис. 2.3.2). Щоб відбитий сигнал поглинався на кінцях кабелю, встановлюються *BNC-термінатори*, один з яких обов'язково повинен бути заземлений.

Раніше при створенні комп'ютерних мереж застосовувався в основному коаксіальний кабель. Зважаючи на те, що вартість витої пари різко знизилася на сьогодні, а кабель на витій парі легше у використанні і значно гнучкіший, коаксіальний кабель використовується вкрай рідко. Зараз же він у більшості мереж замінений витою парою або оптичними кабелями.

Простий конектор «Баррел» Т-конектор Термінатор Термінатор із заземленням

Рис. 2.3.2. BNC-конектори різних типів

Неекранована вита пара (unshielded twisted-pair – UTP). Кабель на основі неекранованої витої пари використовується в багатьох мережах і являє собою чотири пари скручених між собою дротів, при цьому кожна пара ізольована від інших.

Кабель UTP, що застосовується у мережах передачі даних, має чотири пари мідних дротів. Зовнішній діаметр UTP становить близько 0,17 дюйма (4,35 мм). Невеликий діаметр кабелю дає певні переваги при монтажі. Оскільки неекранована вита пара може використовуватися в більшості мережевих архітектур, популярність її продовжує зростати.

Використання кабелю UTP простіше у монтажі та дешевше за інші типи середовища передачі даних. Фактично питома вартість UTP на одиницю довжини менше, ніж у будь-якого іншого типу кабелів, що використовуються в локальних мережах. Однак реальною перевагою витої пари залишається її розмір. Оскільки цей тип кабелю має невеликий зовнішній діаметр, він буде не так швидко заповнювати перетин коробів, як інші види. Цей фактор стає особливо важливим, коли мова йде про монтаж мережі в старих будинках. Крім того, на кінцях кабелю UTP, як правило, використовується спеціальний роз'єм – *RJ-конектор (registered jack connector)* (рис. 2.3.3).

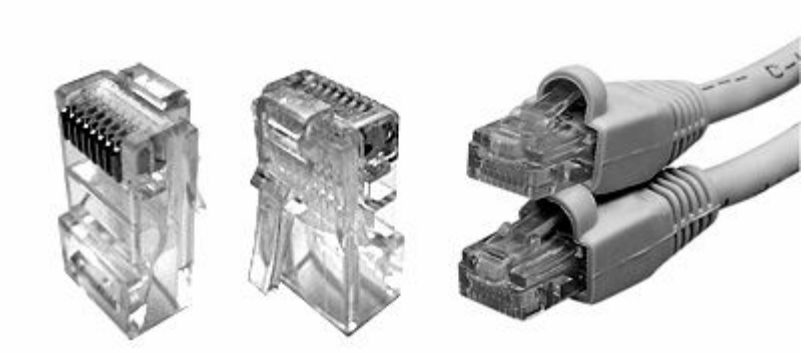


Рис. 2.3.3. RJ-конектор

Спочатку RJ-конектор застосовувався для підключення до телефонної лінії, а зараз використовується в мережевих з'єднаннях і гарантує надійне підключення. Це пояснює істотне зниження кількості потенційних джерел шуму в мережі.

Слід зазначити, що кабель UTP є більш схильним до впливу електричних шумів і перешкод, ніж інші типи носіїв. Раніше можна було говорити, що кабель UTP поступається за швидкістю передачі даних іншим видам кабелів, але зараз, фактично, UTP є найшвидшим середовищем передачі даних на основі мідних провідників. Однак, у випадку використання кабелю UTP, відстань між підсилювачами сигналу менше, ніж при використанні коаксіального кабелю.

Залежно від характеристик кабелі на витій парі розділяються на п'ять категорій:

- *кабелі категорії 1 (UTP 1)* застосовують там, де вимоги до швидкості передачі мінімальні. Зазвичай, це кабелі для передачі голосу й низькошвидкісної передачі даних. До 1983 р. кабель категорії 1 був основним кабелем для телефонного з'єднання в США;
- *кабелі категорії 2 (UTP 2)* розроблені фірмою IBM для застосування у власних кабельних системах. Головна їхня відмінність від кабелю категорії 1 – це смуга пропускання 1 МГц;

- *кабелі категорії 3 (UTP 3)* мають смугу пропускання 16 МГц. Такі типи кабелів використовувалися як для передачі даних, так і для передачі голосу, тому сьогодні кабельні системи багатьох будинків побудовані на кабелі третьої категорії;
- *кабелі категорії 4 (UTP 4)* являють собою покращений варіант кабелю категорії 3 – смуга пропускання 20 МГц, підвищена стійкість до перешкод і низькі втрати. На практиці застосовувався рідко, в основному там, де було необхідно збільшити довжину сегмента мережі;
- *кабелі категорії 5 (UTP 5)* спеціально розроблені для підтримки високошвидкісних технологій. Смуга пропускання кабелю категорії 5 – 100 МГц. Він сьогодні замінив кабель категорії 3, і всі нові технології локальних мереж орієнтуються саме на нього.

Особливе місце займають *кабелі категорій 6 і 7*, які мають смугу пропускання 200 і 600 МГц відповідно. Кабелі категорії 7 обов'язково екрануються; категорії 6 можуть бути як екранованими, так і ні. Вони використовуються у високошвидкісних мережах на відрізках більшої довжини за кабелі п'ятої категорії. Ці кабелі дорожчі за вартістю.

Екранована вита пара (*shielded twisted-pair – STP*). Кабель на основі екранованої витої пари (рис. 2.3.4) поєднує в собі методи екранування й скручування дротів. Призначений для використання в мережах передачі даних і правильно прокладений STP-кабель у порівнянні з UTP-кабелем має більшу стійкість до електромагнітних і радіочастотних перешкод без істотного збільшення ваги або розміру кабелю.

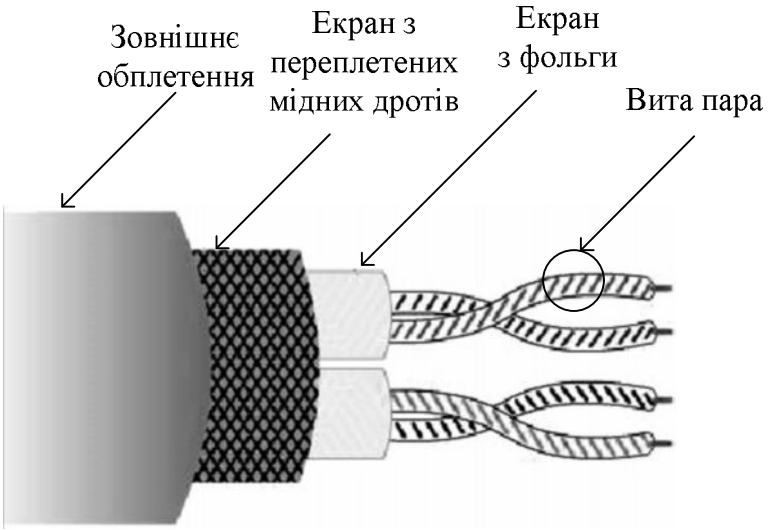


Рис. 2.3.4. Структура екранованої витої пари

Кабель STP має всі переваги та недоліки кабелю UTP, але він краще захищає від усіх типів зовнішніх перешкод. Кабель на основі екранованої витої пари дорожче, ніж на основі неекранованої.

На відміну від коаксіального кабелю, у кабелі STP екран не є частиною ланцюга передачі даних. Тому у кабеля повинен бути заземлений тільки один кінець. Зазвичай його заземлюють у концентраторі або в комутаційній шафі. Неправильне заземлення кабелю може стати основною причиною проблем у мережі, оскільки в цьому випадку екран починає працювати як антена, яка приймає електричні сигнали від інших дротів у кабелі та від зовнішніх джерел електричних шумів. І, нарешті, довжина відрізків кабелю на основі екранованої витої пари без встановлення підсилювачів сигналів не може бути такою ж великою, як при використанні інших середовищ передачі даних.

Оптоволоконний кабель (fiber optic cable). Оптоволоконний кабель є середовищем передачі даних, яке здатне проводити модульований світловий сигнал. Існують два різні типи оптоволоконного кабелю: багатомодовий (multi-mode) або одномодовий (single-mode). Суть відмінності між цими двома типами зводиться до різних режимів проходження світлових променів у кабелі. В одномодовому кабелі практично всі промені проходять той самий шлях, у результаті чого вони досягають приймача одночасно, і форма сигналу майже не змінюється. Для одномодового кабелю застосовуються лазерні прийомопередавачі, що використовують світло виключно з необхідною довжиною хвилі. У багатомодовому кабелі траєкторія світлових променів має помітний розкид, у результаті чого форма сигналу на прийомному кінці кабелю змінюється. Для передачі використовується звичайний (не лазерний) світлодіод, що знижує вартість і збільшує термін служби прийомопередавачів у порівнянні з одномодовим кабелем. Багатомодовий кабель – це основний тип оптоволоконного кабелю на теперішній час, тому що він дешевший і доступніший.

Оптоволоконний кабель несприйнятливий до електромагнітних перешкод і здатний забезпечувати більш високу швидкість передачі даних, ніж кабелі на основі витої пари і коаксіальний кабель. На відміну від інших середовищ передачі даних, що мають в основі мідні елементи, оптоволоконний кабель не проводить електричні сигнали. Замість цього в оптоволоконному кабелі відповідні до бітів сигнали замінюються світловими імпульсами.

Своїм корінням оптоволоконний зв’язок іде у винаходи, зроблені ще в XIX столітті. Але тільки в 1960-х роках з появою твердотілих лазерних джерел світла та високоякісного скла без домішок він почав активно застосовуватися на практиці. Широке поширення

оптоволоконний кабель одержав завдяки телефонним компаніям, які застосовували його в міжміському зв'язку.

Оптоволоконний кабель, що використовується в мережах передачі даних, складається із двох скловолокон, які поміщені в окремі оболонки (рис. 2.3.5). Якщо подивитися на кабель у поперечному розрізі, то можна побачити, що кожне скловолокно оточене шаром відбиваючого покриття, потім іде шар із пластмаси, що має назву кевлар (kevlar) (захисний матеріал, який зазвичай використовується в куленепробивних жилетах), і далі йде зовнішня оболонка. Зовнішня оболонка зазвичай робиться із пластику й служить для захисту всього кабелю. Вона відповідає вимогам відповідних протипожежних і будівельних норм.

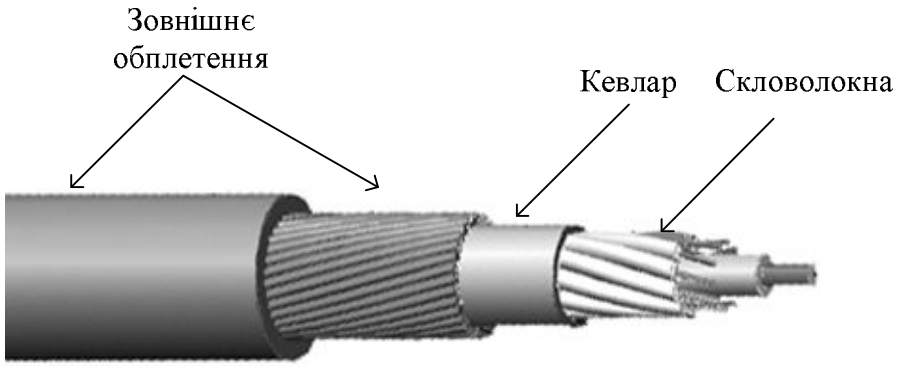


Рис. 2.3.5. Структура оптоволоконного кабелю

Призначення кевлару полягає в тому, щоб дати кабелю додаткові пружні властивості й уберегти від механічного ушкодження тендітні, товщиною з людське волосся, скловолокна. Якщо потрібен монтаж кабелю під землею, то іноді, для додання додаткової твердості, у його конструкцію вводять дріт з нержавіючої сталі.

Світлопровідними елементами оптоволоконного кабелю є центральна жила й світловідбиваюче покриття. Центральна жила – це, як правило, дуже чисте скло з високим коефіцієнтом переломлення. Якщо центральну жилу оточити покриттям зі скла або пластмаси з низьким коефіцієнтом переломлення, то світло може як би захоплюватися центральною жилою кабелю. Цей процес називається повним внутрішнім відбиттям і дозволяє оптопровідниковому волокну відігравати роль світловоду й проводити світло на величезні відстані, навіть при наявності вигинів.

Крім того, що оптоволоконний кабель стійкий до електромагнітних перешкод, він також не піддається впливу радіочастотних перешкод. Завдяки відсутності внутрішніх і зовнішніх шумів сигнал може

проходити по оптоволоконному кабелю більшу відстань, ніж у будь-яких інших середовищах передачі даних. Оскільки електричні сигнали не використовуються, оптоволоконний кабель є ідеальним рішенням для з'єднання будинків, які мають різне електричне заземлення. Беручи до уваги, що довгі прольоти мідного кабелю між будинками можуть бути місцем влучення ударів блискавки, використання оптоволокна в цій ситуації також є більш зручним.

Також, подібно кабелю UTP, оптоволоконний кабель має невеликий діаметр, він відносно плоский і схожий на шнур від лампи. Тому в один жолоб легко поміститься кілька оптоволоконних кабелів. Таким чином, цей носій є ідеальним рішенням для старих будинків з обмеженим простором.

Необхідно відзначити, що оптоволоконний кабель дорожче й складніше у монтажі за інші носії. Оскільки роз'єми для цього кабелю являють собою оптичні інтерфейси, то вони повинні бути ідеально пласко відполірованими й не мати подряпин. Таким чином, його монтаж може виявитися досить складним. Зазвичай, навіть досвідченому монтажникові для створення одного з'єднання потрібно кілька хвилин. Усе це може суттєво підвищити погодинну вартість роботи, і при створенні великих мереж вартість робіт може стати неприйнятно високою.

Бездротові з'єднання

Технології радіозв'язку пересилають дані по радіочастотах і практично не мають обмежень за дальністю. Вони використовуються як в локальних мережах, так і для мережевих з'єднань на великих відстанях. Оскільки радіосигнали легко перехопити, потрібен обов'язково захист даних кодуванням і/або шифруванням.

Передача даних у *мікрохвильовому діапазоні* використовує більш високі частоти і застосовується як на коротких відстанях (об'єднання локальних мереж в різних будівлях), так і в глобальних комунікаціях – за допомогою супутників і наземних супутникових антен. Головне обмеження такого зв'язку: і передавач, і приймач мають бути в зоні прямої видимості один одного.

Технології, що використовують *інфрачервоне (ІЧ) випромінювання*, часто застосовуються для двосторонньої або широкомовної передачі на близьких відстанях. Інфрачервона передача зазвичай використовується в складських і офісних приміщеннях, частіше за все для взаємодії з портативними (мобільними) пристроями. Хоча швидкість інфрачервоних мереж і зручність їх використання дуже привабливі, виникають труднощі при передачі сигналів на відстань більше 30 метрів. До того ж, ІЧ-сигнали легко блокуються будь-якими предметами,

а також схильні до перешкод з боку сильних джерел світла та тепла, які є практично в будь-якому приміщенні.

Для бездротових мереж також застосовують *світлове випромінювання у видимому діапазоні* (наприклад, за допомогою лазерів), хоча цей спосіб передачі використовується рідко. Проте цей спосіб з'єднання може бути зручний для зв'язку між висотними будівлями. Лазерна передача стійка до інтерференцій (перекриття сигналів), прослуховувань, але дуже залежить від атмосферних явищ і працює на коротких відстанях в умовах прямої видимості.

Обладнання комп'ютерних мереж

Будь-яка комп'ютерна мережа являє собою досить складний комплекс програмних і апаратних засобів, що здійснюють зв'язок комп'ютерів та інших пристроїв між собою.

В основі апаратної частини локальної мережі лежать стандартизовані комп'ютерні платформи різних класів – від персональних комп'ютерів до мейнфреймів. Використання тих чи інших комп'ютерних платформ, а також інших апаратних засобів обґрунтовується набором задач, на вирішення яких орієнтована комп'ютерна мережа.

Крім того, до апаратної складової комп'ютерної мережі належать кабельні системи ліній зв'язку та комунікаційне обладнання, яке дозволяє об'єднувати окремі сегменти мережі і організовувати інформаційні потоки.

Кабельна система – це набір комутаційних елементів (кабелів, роз'ємів, з'єднувачів, спеціальних шаф, кронштейнів, кабель-каналів тощо), спільне використання яких закріплено певною методикою.

До комутаційного обладнання належать:

- мережеві адаптери (Network Interface Card – NIC);
- повторювачі (repeaters);
- концентратори (hubs);
- комутатори (switches);
- мости (bridges);
- маршрутизатори (routers);
- шлюзи (gateways).

MAC-адреси і мережеві адаптери

Кожен комп'ютер, незалежно від того, підключений він до мережі чи ні, має унікальну фізичну адресу. Не існує двох однакових фізичних адрес. *Фізична адреса* (*MAC-адреса – Media Access Control*) зашита на платі *мережевого адаптера* (рис. 2.3.6).

Таким чином, у мережі саме плата мережевого адаптера підключає обладнання до середовища передачі даних. Кожна плата мережевого адаптера, який працює на канальному рівні еталонної моделі OSI, має свою унікальну MAC-адресу. У мережі, коли один пристрій прагне переслати дані іншому пристрою, він може встановити канал зв'язку із цим іншим пристроєм, скориставшись його MAC-адресою.

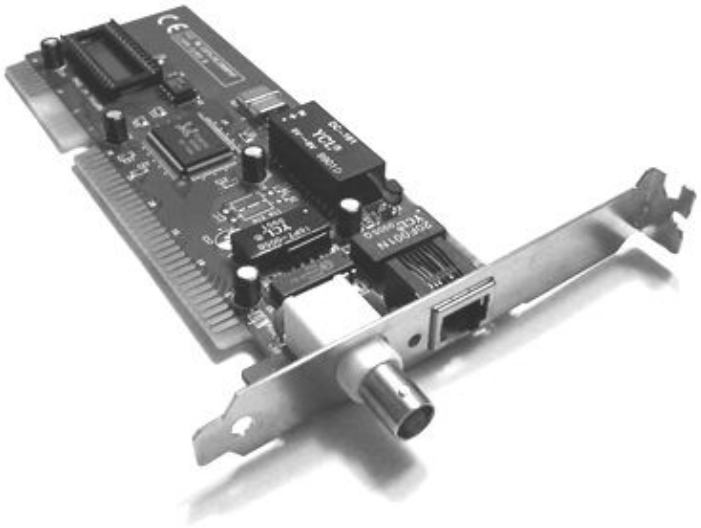


Рис. 2.3.6. Мережевий адаптер

Дані, що пересилаються джерелом, мають MAC-адресу одержувача. У міру просування пакета по середовищу передачі даних мережеві адаптери кожного з пристроїв у мережі порівнюють MAC-адресу одержувача, яка знаходиться у пакеті даних, зі своєю власною фізичною адресою. Якщо адреси не збігаються, мережевий адаптер ігнорує цей пакет, і дані продовжують рух до наступного обладнання. Якщо ж адреси збігаються, то мережевий адаптер робить копію пакета даних і розміщує її на канальному рівні комп'ютера. Після цього вихідний пакет даних продовжує рух мережею, і кожний наступний мережевий адаптер проводить аналогічну процедуру порівняння.

Мережеві адаптери перетворюють пакети даних у сигнали для передачі мережею. У ході виготовлення фірмою-виробником кожному мережевому адаптеру привласнюється фізична адреса, яка заноситься в спеціальну мікросхему, що встановлена на платі адаптера. У більшості мережевих адаптерів MAC-адреса зашивається в постійні запам'ятовувальні пристрої (ПЗП). Коли адаптер ініціюється, ця адреса копіюється в оперативну пам'ять комп'ютера. Оскільки MAC-адреса визначається мережевим адаптером, то при заміні адаптера зміниться й фізична адреса комп'ютера: вона буде відповідати MAC-адресі нового мережевого адаптера.

Для прикладу можна уявити собі готель. Припустимо, що кімната 207 має замок, що відкривається ключем А, а кімната 410 – замок, що відкривається ключем В. Ухвалене рішення поміняти замки в кімнатах 207 і 410. Після заміни ключ А буде відкривати кімнату 410, а ключ В – кімнату 207. У цьому прикладі замки відіграють роль мережевих адаптерів, а ключі – роль MAC-адрес. Якщо адаптери поміняти місцями, то зміняться й MAC-адреси.

Повторювачі

Повторювач (repeater) – апаратний пристрій, що функціонує на фізичному рівні еталонної моделі OSI і забезпечує з'єднання двох сегментів однієї й тієї ж комп'ютерної мережі.

Повторювачі реалізують одну з найпростіших форм міжмережевого обміну. Вони просто регенерують, або повторюють, пакети даних між кабельними сегментами. По суті повторювачі фізично розширюють мережу. Крім того, вони забезпечують високий рівень відмовостійкості, здійснюючи електричну розв'язку мереж, внаслідок чого проблема, яка виникла в одному кабельному сегменті, не зачіпає інші сегменти. Однак разом з пакетами вони повторюють і сигнали, які заважають функціонуванню мережі, не відрізняючи їх від пакетів даних.

Концентратори

Найпростішим пристроєм, який забезпечує зв'язок комп'ютерів один з одним, є *концентратор*, або "*хаб" (hub)*. У мережах, які використовують коаксіальний кабель, концентратори прийнято називати повторювачами.

Нижче перераховані найважливіші особливості концентраторів:

- підсилюють сигнали;
- розповсюджують сигнали в мережі;
- не виконують фільтрацію;
- не займаються маршрутизацією і комутацією;
- використовуються як точки доступу в мережі.

Концентратори працюють на фізичному рівні моделі OSI і є досить примітивним *активним обладнанням* (яке потребує підключення до електричної мережі).

Концентратор можна уявити собі у вигляді обладнання, яке містить безліч незалежних, але зв'язаних між собою модулів мережевого обладнання.

У локальних мережах концентратори виконують роль мультипортових повторювачів. У таких випадках концентратори використовуються, щоб розділити мережеві носії й забезпечити множинне підключення.

Зазвичай концентратор має від 1 до 32 гнізд (портів) для приєднання конекторів різних типів. У більшості випадків це будуть гнізда для конекторів RJ-45, однак існують і *гібридні концентратори* з портами RJ-15 і BNC, що дозволяють поєднувати сегменти на основі коаксіального кабелю. До портів можна підключати не тільки комп'ютери, але й інші концентратори, формуючи в такий спосіб *ланцюжки (каскади) концентраторів* або ще більш складні топології типу "дерево".

Недоліком використання концентратора є те, що він не може фільтрувати мережевий трафік. *Фільтрацією* називається процес, у ході якого в мережевому трафіку контролюються певні характеристики, наприклад, адреса джерела, адреса одержувача або протокол, і на підставі встановлених критеріїв ухвалюється рішення – пропускати трафік далі або ігнорувати його. У концентраторі дані, що поступили на один порт, передаються далі на всі порти. Отже, концентратор передає дані в усі ділянки або сегменти мережі, незалежно від того, повинні вони туди направлятися чи ні.

Якщо є тільки один кабель, який зв'язує всі пристрої в мережі, або якщо сегменти мережі зв'язані тільки не фільтруючими пристроями (наприклад, концентраторами), декілька користувачів можуть спробувати послати дані в один момент часу. Якщо одночасно намагаються передавати кілька вузлів, то виникає конфлікт. У цьому випадку дані від різних пристроїв зустрічаються один з одним і ушкоджуються. Область мережі, у межах якої сформувався пакет даних і виник конфлікт, називають *доменом конфлікту (колізії)*. Одним з методів рішення проблеми занадто великого трафіка й великої кількості конфліктів у мережі є використання мостів. На рис. 2.3.7 представлене об'єднання робочих станцій у комп'ютерну мережу з використанням концентратора. У даній мережі пакет, відправлений комп'ютером В комп'ютеру А, буде переданий усім робочим станціям, серверу й іншим мережевим пристроям.

Мости і комутатори

Мости (bridge), а потім і *комутатори (switch)* були розроблені, щоб допомогти в об'єднанні мереж і усуненні проблеми виникнення великої кількості колізій. Суттєвою відмінністю цих пристроїв від концентраторів є те, що вони вміють визначати MAC-адресу джерела й одержувача сигналів, а також підтримувати таблицю відповідності своїх портів і використаних у мережі MAC-адрес. Таку таблицю міст (або комутатор) формує відразу після включення за наступним принципом: як тільки порт одержує відповідь від обладнання з певною фі-

зичною адресою, у таблиці з'являється рядок відповідності "MAC-адреса <-> порт".

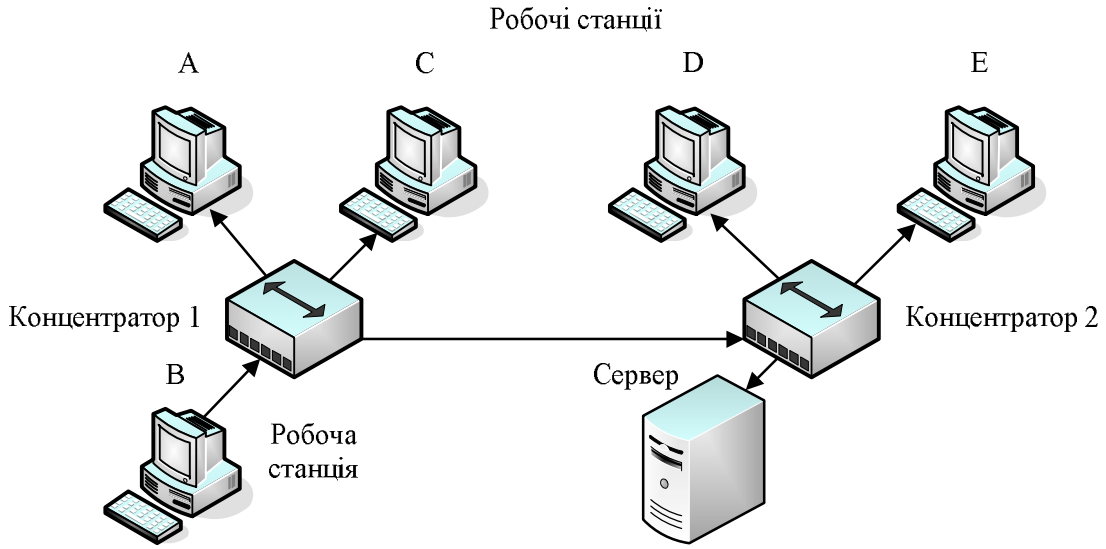


Рис. 2.3.7. Об'єднання робочих станцій в комп'ютерну мережу з використанням концентраторів

Таким чином, ці пристрої працюють не тільки на фізичному рівні моделі OSI, але й на канальному, – точніше, на підрівні керування доступом до середовища (MAC). Одержавши кадр й визначивши адресу одержувача, міст або комутатор транслює кадр тільки на той порт, з яким ця MAC-адреса зіставлена в таблиці відповідностей. Кадри, передані між комп'ютерами одного сегмента, комутатор одержує, але нікуди не транслює (рис. 2.3.8, обмін даними між комп'ютерами A та B ніяк не впливає на взаємодію комп'ютера C з сервером та комп'ютерів D і E – один з одним).

Єдиними сигналами, переданими на усі порти, є кадри, призначені для адрес, які не мають поки що записів у таблиці відповідностей, та спеціальні *широкомовні повідомлення*, призначені всім комп'ютерам локальної мережі. Щоб позначити цю особливість роботи мостів і комутаторів, говорять, що вони *формують "область широкомовлення" (Broadcast Domain)*.

Відмінність між мостами та комутаторами полягає в тому, що міст у кожний момент часу може передавати тільки один кадр, обслуговуючи передачу від одного комп'ютера до іншого (тому перші моделі мостів були двопортовими). Комутатор же вміє будувати велику кількість віртуальних каналів зв'язку між портами (тобто комутувати порти один з одним, звідси й назва пристрою), роблячи паралельну обробку кадрів, які надходять від різних портів. Звичайно продуктивність мереж, побудованих на базі комутаторів, є суттєво вищою.

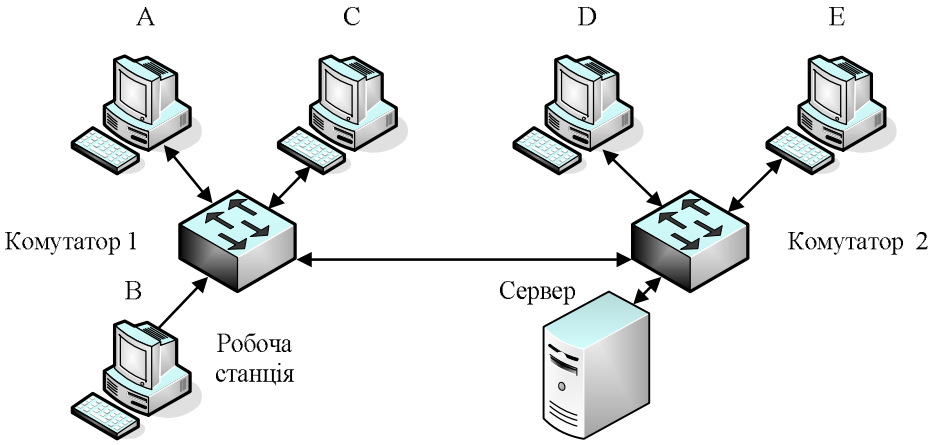


Рис. 2.3.8. Об'єднання робочих станцій в комп'ютерну мережу з використанням комутаторів

Підкреслимо, що переважна більшість сучасних мереж будується саме на комутаторах, тоді як зустріти концентратор або міст сьогодні досить важко.

Маршрутизатори

Маршрутизатор – це пристрій для з'єднання мереж, які використовують різні архітектури та протоколи. Маршрутизатори працюють на ще більш високому рівні моделі OSI – мережевому. До їхнього завдання входить аналіз адрес, які використані у протоколі цього рівня (наприклад, IP-адрес), і визначення найкращого маршруту доставки пакета даних за призначенням (докладніше маршрутизація буде розглянута у темі 8). Зазвичай маршрутизатори працюють і на більш низьких рівнях моделі OSI: як концентратори вони відновлюють рівень і форму сигналу, що передається, як мости й комутатори дозволяють уникнути колізій. Однак, на відміну від перерахованих вище пристроїв, маршрутизатори змінюють передані кадри – точніше, "розбирають" їх до мережевого рівня (декапсулюють), а потім формують заново за певними правилами (інкапсулюють). До речі, без певного налаштування маршрутизатори не передають на інші порти навіть широкомовні пакети і, таким чином, служать у мережах межами областей колізій і широкомовлення.

Таким чином, маршрутизатори можуть виконувати такі функції:

- комутувати і направляти пакети через декілька мереж;
- визначати найкращий шлях для їх передачі;
- обходити повільні та несправні канали;
- фільтрувати широкомовні повідомлення;
- діяти як бар'єр безпеки між мережами.

Маршрутизатор, на відміну від моста, має свою адресу і використовується як проміжний пункт призначення.

Крім того, разом із програмами більш високого рівня моделі OSI, маршрутизатори вміють виконувати безліч складних операцій, наприклад, виявляти проблеми в мережі й повідомляти про них, вести статистику отриманих і переданих даних, фільтрувати пакети, проводити авторизацію користувачів при виході в Інтернет тощо.

Потужні маршрутизатори є досить складними й дорогими програмно-апаратними комплексами, тому в сучасних мережах вони все частіше заміняються *комутаторами 3-го рівня* – пристроями, що займають проміжний рівень між комутаторами та маршрутизаторами. Від звичайних комутаторів вони відрізняються тим, що можуть виконувати найпростіші функції маршрутизації, залишаючись при цьому продуктивними й не дуже дорогими.

На рис. 2.3.9 представлена мережа, розділена на 5 підмереж з використанням маршрутизаторів. Тут дані між абонентами E і D передаються через 3 підмережі, причому передача даних відбувається не в усі підмережі, а лише в ту, у якій перебуває абонент-одержувач.

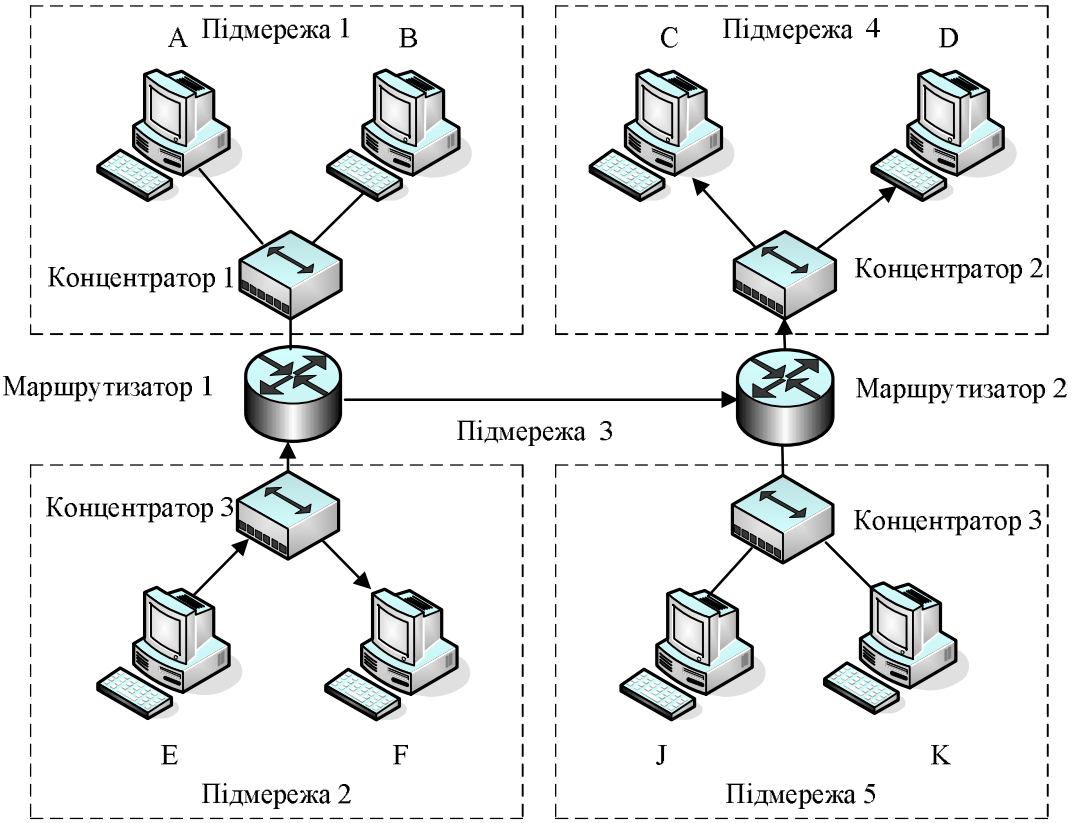


Рис. 2.3.9. Розбивка мережі на підмережі з використанням маршрутизаторів

Шлюзи

Шлюзи – це пристрої, які забезпечують зв'язок між різними архітектурами та середовищами. Взагалі кажучи, під шлюзом зазвичай мається на увазі будь-який пристрій або програма, які дозволяють поєднувати різнорідні системи (наприклад, існують поштові шлюзи, які використовуються для зв'язку різних систем електронної пошти). Але якщо мова йде про взаємодію в мережах, то тут під шлюзом мається на увазі пристрій, що сполучає різні мережеві архітектури (наприклад, шлюз з Ethernet в Token Ring). Важливо тут те, що шлюз повинен не тільки мати фізичні порти для підключення різнорідних систем, а й "розуміти" різнорідні протоколи, виступаючи для них у ролі "перекладача".

Типовим прикладом шлюзів є широко використовувані в сучасних домашніх мережах інтегровані пристрої, у яких об'єднані ADSL-модем для підключення до Інтернету, бездротова точка доступу, що працює за стандартом IEEE 802.11b (або g), і комутатор Fast Ethernet з підтримкою стандарту IEEE 802.3u.

Контрольні питання

1. Які типи середовища передачі даних Вам відомі?
2. Для чого застосовується коаксіальний кабель?
3. Які типи витої пари Вам відомі і для чого їх застосовують?
4. Який тип середовища передачі даних забезпечує передачу з використанням світового сигналу?
5. Що таке MAC-адреса і яка її основна функція?
6. Яке обладнання комп'ютерних мереж Вам відомо?
7. У чому різниця між концентратором і комутатором?
8. Що таке маршрутизатор і на якому рівні моделі OSI він працює?
9. Що таке шлюз?

ЛІТЕРАТУРА: [1, 6, 7, 8, 17, 25].

Тема 4. ТЕХНОЛОГІЇ ПОБУДОВИ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Мета теми – познайомитись із базовими технологіями побудови локальних комп'ютерних мереж; розглянути їх переваги та недоліки; розглянути специфікації технологій у відповідності з типами середовищ передачі даних.

Ключові поняття: технологія побудови локальної комп'ютерної мережі; технології Ethernet, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet; технології Token Ring, Token Bus; технологія FDDI; технологія Wireless Ethernet.

Мережева технологія – це узгоджений набір стандартних протоколів та програмно-апаратних засобів, що їх реалізують, достатній для побудови локальної обчислювальної мережі.

Мережева технологія або архітектура визначає топологію і метод доступу до середовища передачі даних, кабельну систему або середовище передачі даних, формат мережевих кадрів, тип кодування сигналів, швидкість передачі в локальній мережі.

Іноді мережеві технології називають базовими технологіями, маючи на увазі те, що на їх основі будується базис будь-якої мережі. До основних базових мережевих технологій належать такі відомі технології локальних мереж як Ethernet, Token Ring та FDDI.

Технологія Ethernet

Ethernet – це найпопулярніша на сьогодні мережева архітектура. Специфікація Ethernet була розроблена Xerox Corporation у кооперації з DEC і Intel в 1976 р., а точніше, її трохи видозмінена модифікація Ethernet II або Ethernet DIX. Архітектура Ethernet послужила основою прийнятого в 1985 р. стандарту IEEE 802.3.

Залежно від типу фізичного середовища передачі даних стандарт IEEE 802.3 має різні модифікації – 10Base-5, 10Base-2, 10Base-T, 10Base-F (табл. 2.4.1).

Таблиця 2.4.1

Характеристики специфікацій технології Ethernet

Характеристики	Специфікації			
	10Base-5	10Base-2	10Base-T	10Base-F
Тип кабелю	Товстий коаксіальний кабель RG-8/11	Тонкий коаксіальний кабель RG-58	UTP3, UTP4, UTP5	Одномодове і багатомодове оптоволокно
Максимальне число вузлів у сегменті	100	30	1024	1024
Максимальне число вузлів у мережі	296	86	1024	1024
Максимальна довжина сегмента, м	500	185	100	2000
Топологія	Загальна шина	Загальна шина	Зірка	Зірка
Діаметр мережі, м	2500	925	500	2500

Але для всіх модифікацій технологія Ethernet забезпечує швидкість передачі даних 10 Мбіт/с і використовує метод доступу до роз-

поділеного середовища передачі даних – *метод множинного доступу із контролем несучої та виявленням конфліктів (carrier sense multiple access/collision detection – CSMA/CD).*

Технологія Ethernet є технологією колективного використання середовища передачі даних. Це означає, що всі пристрої в мережі повинні стежити за передачами в мережі і конкурувати або домовлятися про можливість, або право на передачу. Це також означає, що в один і той же момент часу в мережі можлива тільки одна передача.

Щоб використовувати принцип колективної роботи із середовищем передачі даних, в Ethernet застосовується метод множинного доступу з контролем несучої і виявленням конфліктів (CSMA/CD). Його використання дозволяє пристроям домовлятися про право на передачу.

Метод CSMA/CD працює наступним чином: якщо вузол хоче здійснити передачу, він перевіряє (“прослуховує”) мережу на предмет того, передає в даний момент інший пристрій дані чи ні. Якщо мережа вільна, вузол починає процес передачі. Поки йде передача, вузол контролює мережу, щоб упевнитися, що в цей же момент часу не передає ніяка інша станція. Два вузли можуть почати передачу майже одночасно, якщо виявлять, що мережа вільна. У цьому випадку виникає конфлікт.

Коли вузол, який передає дані, дізнається про конфлікт, він передає сигнал “Наявність конфлікту”, що робить конфлікт досить довгим для того, щоб його могли розпізнати всі інші вузли мережі. Після цього всі вузли, які передають дані, припиняють відправлення кадрів на обраний випадковим чином відрізок часу, що називається *часом затримки повторної передачі*. Після закінчення цього періоду здійснюється повторна передача. Якщо наступні спроби також закінчуються невдало, вузол повторює їх до 16 разів, після чого відмовляється від передачі.

Час затримки для кожного вузла різний. Якщо різниця в тривалості цих періодів затримки досить велика, то повторну передачу вузли почнуть вже не одночасно. З кожним наступним конфліктом час затримки подвоюється, аж до десятої спроби, тим самим зменшуючи ймовірність виникнення конфлікту при повторній передачі. З 10-ї по 16-ту спробу вузли час затримки більше не збільшують, підтримуючи його постійним.

Технологія Fast Ethernet

У міру розвитку комп’ютерних технологій і появи нових потужних машин швидкість 10-14 Мбіт/с перестала бути достатньою для нормальної роботи мереж, які просто не справлялися із збільшеним навантаженням на канали зв’язку. Тому в 1995 р. були затверджені

нові стандарти – IEEE 802.3u і 802.12, які дозволяли реалізовувати взаємодію комп'ютерів через мережу на швидкості 100 Мбіт/с.

IEEE 802.3u заснований на технології Fast Ethernet, яку створила група виробників мережевого обладнання, до складу якої входили такі компанії, як 3Com і SynoOptics. Цей стандарт став доповненням до вже існуючого стандарту IEEE 802.3 (табл. 2.4.2).

Таблиця 2.4.2

Характеристики специфікацій технології Ethernet

Характеристики	Специфікації		
	100Base-TX	**100 Base-T4**	**100Base-FX**
Тип кабелю	UTP5, STP	UTP3	Багатомодове оптоволокно
Метод доступу	CSMA/CD	CSMA/CD	CSMA/CD
Максимальне число вузлів у мережі	1024	1024	1024
Максимальна довжина сегмента, м.	100	100	2000 при повнодуплексній передачі, 412 при напівдуплексній передачі
Топологія	Зірка	Зірка	Зірка
Діаметр мережі, м.	205	205	–

Виробники відмовилися від використання як фізичного середовища передачі даних коаксіального кабелю, повністю перейшовши на виту пару й оптоволокно, які дозволяють підтримувати необхідні швидкості з'єднань, і при цьому є більш зручним і економічним рішенням.

Як і стандарт IEEE 802.3, що описує технологію Ethernet, новий стандарт установив специфікації для різних середовищ передачі даних.

Одночасна передача даних в обох напрямках називається повнодуплексною передачею, а відповідний режим передачі – *повнодуплексним*.

Режим, при якому обмін даними здійснюється шляхом чергування прийому та передачі, називається *напівдуплексним*.

Технологія Gigabit Ethernet

Після розробки стандартів, що дозволяють передавати дані на швидкості 100 Мбіт/с, досить скоро знову назріла необхідність у переході на новий рівень швидкостей. Складність виникла при побудові ве-

ликих корпоративних мереж, де сервери, що працюють при 100 Мбіт/с, перевантажували магістральні канали зв'язку. Тому наступним кроком у розвитку високошвидкісних мереж стала технологія Gigabit Ethernet, яка забезпечувала можливість передачі даних на швидкості 1000 Мбіт/с.

Технології Gigabit Ethernet відповідає стандарт 802.3z, який визначає для неї як фізичне середовище передачі даних одномодовий і багатомодовий оптоволоконний кабель, а також екрановану виту пару із хвильовим опором 75 Ом. Трохи пізніше була розроблена реалізація Gigabit Ethernet для кабелю на основі витої пари категорії 5 (стандарт IEEE 802.3ab). Також визначені й відповідні до фізичних середовищ специфікації (табл. 2.4.3).

Технологія 10 Gigabit Ethernet

Новим ривком у розвитку технологій високошвидкісної передачі даних став стандарт IEEE 802.3ae – 10 Gigabit Ethernet (10 Gbe), схвалений у червні 2002 р. З його появою область використання Ethernet розширилася до масштабів міських (MAN) і глобальних (WAN) мереж.

У стандарті описано кілька специфікацій, що визначають використання як середовища передачі даних одно- і багатомодове оптоволокно, методи кодування, довжини хвиль, що використовуються, тощо.

Таблиця 2.4.3

Характеристики специфікацій технології Gigabit Ethernet

Характеристики	Специфікації			
	1000Base-LX	1000Base -SX	1000Base-T	1000Base -CX
Тип кабелю	**UTP5, STP**	**Оптоволокно**	**UTP5**	**STP Twinax**
Максимальна довжина сегмента, м.	316 – при напівдуплексній передачі. 550 – при повнодуплексній передачі багатомодовим волокном. 5000 – при повнодуплексній передачі одномодовим волокном	316 – при напівдуплексній передачі волокном 50/125. 550 – при повнодуплексній передачі волокном 50/125. 275 – при передачі волокном 62.5/125	100	25

Переваги та недоліки технологій Ethernet

Основний недолік мереж Ethernet пов'язаний з використанням в них методу доступу до середовища CSMA/CD. При збільшенні кількості комп'ютерів зростає кількість зіткнень, що знижує пропускну

здатність мережі і збільшує час доставки кадрів. Але зауважимо, що в сучасних мережах цей недолік досить легко усувається шляхом заміни концентраторів мостами і комутаторами, які вміють "ізолювати" передачу даних між двома комп'ютерами в мережі від інших.

Переваг у архітектури Ethernet досить багато. Перш за все, сама ця технологія досить проста в реалізації. Відповідно, Ethernet-пристрої (мережеві адаптери, концентратори, комутатори тощо) виявляються значно дешевшими за аналогічні пристрої інших мережевих архітектур. У Ethernet можна використовувати практично будь-які види кабелю, а застосування оптоволокна дозволяє поєднувати ділянки мереж, розташовані далеко одна від одної. Нарешті, сумісність різних варіантів Ethernet дуже висока, що дозволяє не тільки нарощувати потужності мережі з використанням існуючої кабельної інфраструктури, але й легко розширювати мережу, підключаючи до неї нові, більш швидкісні сегменти. Тому сьогодні архітектура Ethernet не тільки стала найпоширенішою в локальних мережах, але й витісняє інші технології в регіональних і глобальних мережах.

Технологія Token Ring

Стандарт IEEE 803.5 був прийнятий на основі технології Token Ring та розроблений компанією IBM у 1984 р. Мережі Token Ring будуються за топологією "кільце" і використовують маркерний метод доступу до середовища передачі даних.

Передача даних у мережах Token Ring може здійснюватися на швидкостях 4 і 16 Мбіт/с. У мережі Token Ring 16 Мбіт/с використовуються деякі вдосконалення маркерного методу доступу до середовища. Наприклад, алгоритм раннього звільнення маркера, при якому станція не чекає повернення по кільцю переданих нею кадрів з підтвердженням прийому, а передає маркер наступній станції відразу по закінченні свого пересилання кадрів.

Технологія Token Ring орієнтована на використання концентраторів, одним із завдань яких є збереження цілісності кільця при вимиканні одного або декількох комп'ютерів. Концентратори можуть бути пасивними й виконувати функцію простого з'єднувача для портів, так, щоб станції, які підключаються, утворювали кільце, або активними, при цьому концентратор виконує ще й функцію повторювача сигналів. При цьому мережа (рис. 2.4.1) має логічну топологію "кільце", хоча фізичне з'єднання комп'ютерів має структуру типу "зірка".

Для з'єднання вузлів мережі як фізичне середовище передачі даних можуть використовуватися кабелі на основі екранованої витої пари категорії 1, неекранованої витої пари категорії 3 або 6, а також оптоволокно.

У випадку використання пасивних концентраторів для екранованої витої пари допускається підключення до 260 робочих станцій, при цьому відстань між вузлами мережі не повинна перевищувати 100 м. При об'єднанні станцій за допомогою неекранованої витої пари їх максимально припустиме число скорочується до 72, а відстань між вузлами – до 45 м.

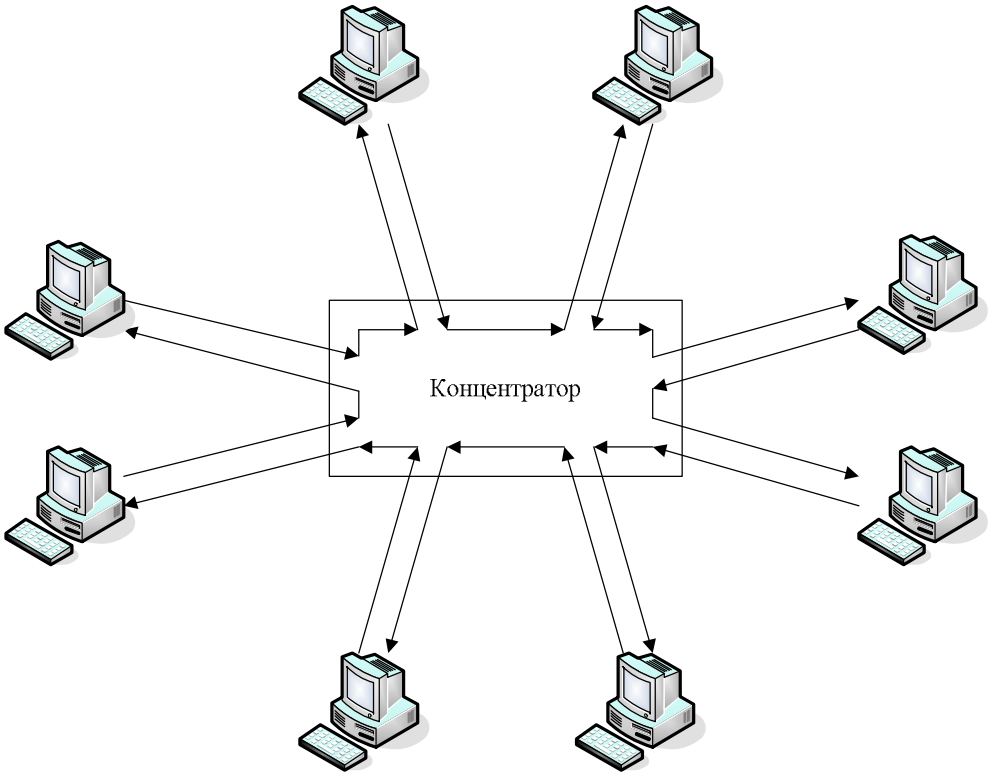


Рис. 2.4.1. Мережа на основі технології Token Ring

Якщо встановлені концентратори є активними, то максимальна довжина кабелю, що їх з'єднує, не повинна перевищувати 730 м у випадку використання екранованої витої пари, і 365 м – для неекранованої. Максимальна довжина кільця Token Ring не повинна перевищувати 4000 м.

До *переваг архітектури Token Ring* можна віднести високу дальність передачі (при використанні повторювачів можна передавати дані на відстань до 730 м), а також те, що в подібній мережі легко розрахувати максимальну затримку при передачі інформації між будь-якими двома пристроями, оскільки як метод доступу до середовища використовується передача маркера. Остання обставина особливо важлива в

автоматизованих системах управління, які вимагають обробки процесів в реальному часі.

Недоліки архітектури Token Ring: досить висока вартість, низька сумісність обладнання (наприклад, у 16-мегабітних мережах Token Ring не можна використовувати 4-мегабітні пристрої), а також досить мала (за сучасними мірками) швидкість передачі даних.

Технологія Token Bus

Стандарт IEEE 802.4 описує властивості мереж, відомих як маркерна шина (Token Bus). Такі мережі також використовують маркерний метод доступу до середовища. Замість передачі маркера від станції до станції по колу, як це відбувається в мережах Token Ring, що обумовлено топологією побудови мережі, у мережах Token Bus маркер передається від "старшої" станції до "молодшої". Старшинство підключених до мережі станцій зазвичай визначається на основі їх адрес. Маркер рухається в напрямку убування адрес. Передача маркера відбувається доти, поки він не досягне молодшої станції, після цього він повертається назад до першої станції (рис. 2.4.2).

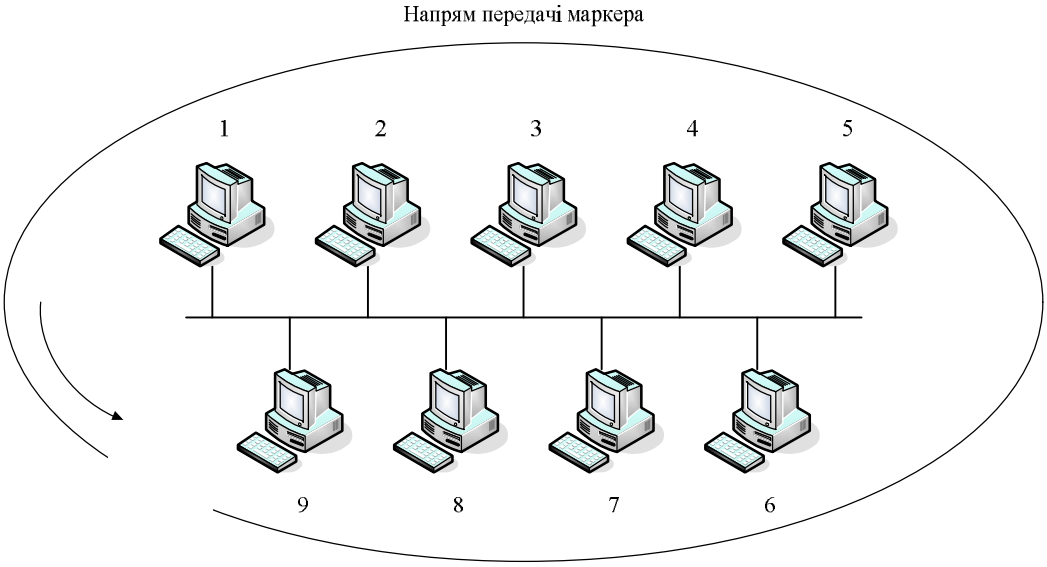


Рис. 2.4.2. Передача маркера в мережах Token Bus

Середовище передачі – коаксіальний кабель 75 Ом або оптоволокно, швидкість 1-20 Мбіт/с в залежності від середовища. З погляду структури мережі, Token Bus має фізичну топологію "загальна шина", а логічну – "кільце". Підтримується система пріоритетів, що забезпечує заданий час відгуку для різних рівнів. Використовується в промисловості, на цій топології базуються різні типи протоколів промислової автоматики, наприклад MAP (Manufacturing Automation Protocol).

Технологія FDDI

Технологію FDDI можна вважати вдосконаленим варіантом Token Ring, тому що в ній також використовується метод доступу до середовища, заснований на передачі маркера, а також кільцева топологія зв'язків, але разом з тим FDDI працює на більш високій швидкості і має більш досконалий механізм відмовостійкості.

Технологія FDDI була розроблена в 1988 р. американським інститутом із стандартизації ANSI. Як фізичне середовище передачі даних тут використовується оптоволоконний кабель. Через деякий час ця технологія була реалізована з підтримкою кабелю на основі неекранованої витої пари п'ятої категорії.

Мережа FDDI будується на основі двох оптоволоконних кілець: первинного та вторинного. При нормальній роботі мережі дані передаються по первинному кільцю, вторинне кільце при цьому не використовується.

Наявність двох кілець (рис. 2.4.3) суттєво підвищує відмовостійкість мережі. У випадку обриву мережі кільця "згортаються", і передача інформації відбувається по вторинному кільцю. Якщо утворилося кілька точок розриву кабелю, то мережа розпадається на кілька незв'язаних мереж.

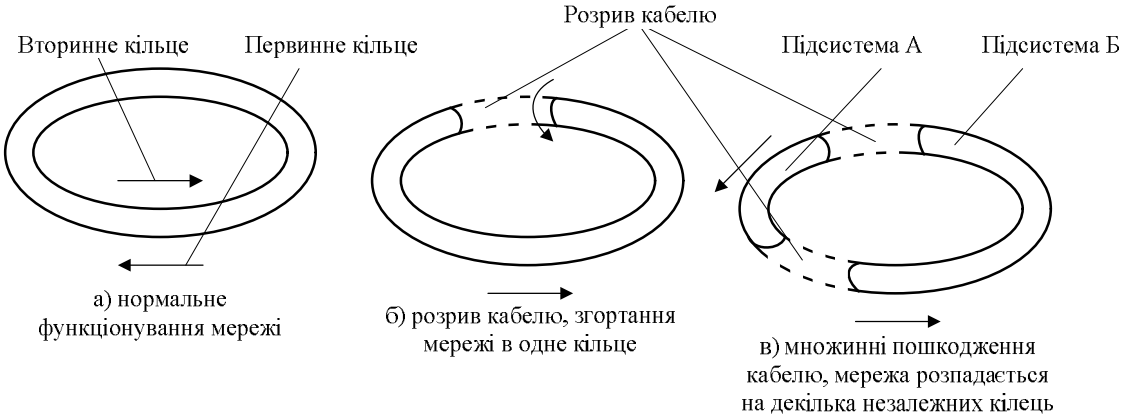


Рис. 2.4.3. Механізм забезпечення високої відмовостійкості роботи мережі

Швидкість передачі даних для мереж FDDI становить 100 Мбіт/с. Максимальна кількість вузлів становить 500. При використанні як фізичного середовища передачі даних багатомодового оптоволоконного кабелю відстань між вузлами мережі може становити до 2 км, при використанні одномодового кабелю – до 40 км. У випадку використання кабелю на основі витої пари п'ятої категорії зазначена відстань може становити до 100 м. Максимальний діаметр подвійного кільця не повинен перевищувати 100 км.

Технологія FDDI є на сьогодні найдорожчою 100 Мбіт технологією. Тому її основні сфери застосування – це магістралі кампусів і будівель, а також підключення корпоративних серверів. У цих випадках витрати виявляються обґрунтованими – магістраль мережі повинна бути відмовостійкою і швидкою, те ж саме стосується й сервера, побудованого на базі дорогої мультипроцесорної платформи і який обслуговує сотні користувачів.

Багато сучасних корпоративних мереж побудовані з використанням технології FDDI на магістралі у поєднанні з технологіями Ethernet, Fast Ethernet і Token Ring у мережах поверхів і відділів. Група центральних серверів також зазвичай підключається до магістрального кільця FDDI безпосередньо за допомогою мережевих адаптерів FDDI.

Wireless Ethernet

Часто виникають ситуації, коли монтаж кабельної системи ускладнений або економічно недоцільний. Причиною цього, наприклад, можуть бути природні перешкоди, утворені особливостями рельєфу місцевості (річки, озера, гори), або необхідність створення тимчасової локальної мережі, яку з часом потрібно буде демонтувати. У таких випадках для організації мережі без монтажу додаткових ліній зв'язку використовують *бездротові локальні мережі (Wireless LAN – WLAN)*, які дозволяють об'єднати в єдину інформаційну систему розрізнені локальні мережі та комп'ютери для забезпечення доступу всіх користувачів цих мереж до єдиних інформаційних ресурсів.

Крім того, необхідність побудови бездротових мереж викликана здешевленням, а, відповідно, і зростанням популярності мобільних пристроїв, таких, як портативні ноутбуки, кишенькові комп'ютери тощо. Зі збільшенням числа мобільних користувачів виникає гостра необхідність в оперативному здійсненні комунікацій між ними, в обміні даними, у швидкому одержанні інформації.

В основі технологій бездротових мереж лежить принцип радіозв'язку між вузлами мережі. Як вузол мережі може виступати як окремий комп'ютер або ноутбук, так і спеціальне обладнання – *точка доступу (Access Point)*, яке забезпечує доступ до кабельного сегмента будь-якої мережі або іншого комп'ютера.

Дуже часто бездротові мережі називають мережами Wi-Fi або просто Wi-Fi. Цей термін походить від назви незалежної міжнародної організації Wireless Fidelity Alliance (Wi-Fi Alliance), яка була створена в 1999 р. лідерами індустрії бездротового зв'язку і називалася Wireless Ethernet Compatibility Alliance (WECA). Завданням організації є сертифікація сумісності з технологією WLAN продукції різних виробників. Ця організація поєднує практично всіх провідних виробни-

ків – Cisco, Lucent, 3Com, IBM, Intel, Apple, Compaq, Dell, Fujitsu, Siemens, Sony, AMD та ін.

У 1990 р. комітет зі стандартів IEEE 802 сформував робочу групу по стандартах для бездротових локальних мереж 802.11. IEEE 802.11 – це набір стандартів зв'язку для комунікації в бездротовій локальній мережевій зоні частотних діапазонів 2,4, 3,6 і 5 ГГц (табл. 2.4.4).

Таблиця 2.4.4

Характеристики специфікацій Radio Ethernet

Характеристики	**Специфікації**				
	802.11a	802.11b	802.11g		802.11n
Швидкість передачі даних, Мбіт/с	До 54	До 11	До 11	До 54	Припускається, що буде до 248 для двох потоків
Число каналів	До 23	3	3		
Схема модуляції	OFDM	DSSS	DSSS	OFDM	MIMO-OFDM
Робоча частота, ГГц	5,7	2,4	2,4		2,4 або 5
Дата затвердження	Жовтень 1999 р.	Жовтень 1999 р.	Червень 2003 р.		Вересень 2009 р.
Переваги	Висока швидкість, менша схильність до перекриття хвиль	Низька вартість	Висока швидкість		Висока швидкість; сумісність з пристроями стандартів 802.11b/g та 802.11a; використання двох частотних діапазонів
Недоліки	Висока вартість; несумісність зі стандартами 802.11b та g	Низька швидкість; схильність до перекриття хвиль	Схильність до перекриття хвиль, оскільки більшість споживчих приладів використовують частоту 2,4 ГГц		

У 1997 р. була затверджена перша специфікація для радіообладнання і мереж, які працюють на частоті 2,4 ГГц, зі швидкостями доступу 1 і 2 Мбіт/с. Нова технологія передачі даних багато чого перейняла з технології Ethernet і одержала відповідну назву *Radio Ethernet*.

Однак на той час швидкість передачі даних 1-2 Мбіт/с у бездротовій мережі вже не задовольняла потреби користувачів. Щоб зробити

технологію бездротових мереж популярною, дешевою і такою, що задовольняє сучасні вимоги, розробники були змушені створити новий стандарт.

Один з перших високошвидкісних стандартів бездротових мереж – *IEEE 802.11a* – визначає швидкість передачі вже до 54 Мбіт/с. Робочий діапазон стандарту 5 ГГц. Основною особливістю стандарту є метод модуляції сигналу, який називається *мультиплексуванням з поділом по ортогональних частотах (Orthogonal Frequency Division Multiplexing – OFDM).* Метод припускає паралельну передачу корисного сигналу одночасно по декільком частотам діапазону. У результаті підвищується пропускна здатність каналу і якість сигналу.

На відміну від стандарту 802.11, орієнтованого на область частот 2,4 ГГц, специфікаціями 802.11a передбачена робота в діапазоні 5 ГГц. Більшість споживчих приладів використовує діапазон частот 2,4 ГГц, тому не буде перекриття хвиль (інтерференції). У стандарті визначено три обов'язкові швидкості передачі даних (6, 12 і 24 Мбіт/с) і п'ять додаткових (9, 18, 24, 48 і 54 Мбіт/с). Мережі, побудовані на основі цих стандартів, мають 12 каналів, які не перекриваються.

У вересні 1999 р. затверджується новий стандарт *IEEE 802.11b* (або 802.11 High rate), який дозволяє забезпечувати швидкість передачі даних до 11 Мбіт/с. У стандарті для модуляції сигналу застосовується метод *широкосмугової модуляції із прямим розширенням спектра (Direct Sequence Spread Spectrum – DSSS)*. При цьому весь робочий діапазон поділяється на 14 каналів, частоти яких рознесені на 25 МГц для виключення взаємних перешкод. Дані передаються по одному із цих каналів без перемикання на інші. Можливе одночасне використання всього трьох каналів. Швидкість передачі даних може автоматично змінюватись залежно від рівня перешкод і відстані між передавачем і приймачем.

У 2003 р. був затверджений стандарт *IEEE 802.11g*, який є розвитком специфікації IEEE 802.11b. Цей стандарт передбачає використання діапазону частот 2,4 ГГц, забезпечуючи швидкість передачі 54 Мбіт/с і перевершуючи, таким чином, нині чинний стандарт IEEE 802.11b, що забезпечує швидкість передачі 11 Мбіт/с. Крім того, він гарантує зворотну сумісність зі стандартом 802.11b. Зворотна сумісність стандарту IEEE 802.11g може бути реалізована в режимі модуляції DSSS, і тоді швидкість передачі буде обмежена 11 Мбіт/с або в режимі модуляції OFDM, при якому швидкість складає 54 Мбіт/с. Таким чином, даний стандарт є найбільш прийнятним при побудові бездротових мереж.

IEEE 802.11n – найновіша версія стандарту 802.11 для мереж Wi-Fi. Цей стандарт був затверджений 11 вересня 2009 р.

Стандарт 802.11n підвищує швидкість передачі даних практично вчетверо в порівнянні з пристроями стандартів 802.11g (максимальна швидкість яких дорівнює 54 Мбіт/с) за умови використання в режимі 802.11n з іншими пристроями 802.11n. Теоретично 802.11n здатний забезпечити швидкість передачі даних до 480 Мбіт/с. Пристрої 802.11n працюють в діапазонах 2,4-2,5 або 5,0 ГГц.

Крім того, пристрої 802.11n можуть працювати в трьох режимах:

- наслідуваному (legacy), у якому забезпечується підтримка пристроїв 802.11b/g і 802.11a;
- змішаному (mixed), у якому підтримуються пристрої 802.11b/g, 802.11a і 802.11n;
- "чистому" режимі – 802.11n (саме в цьому режимі і можна скористатися перевагами підвищеної швидкості і збільшеною дальністю передачі даних, забезпечуваними стандартом 802.11n).

Основні переваги нового стандарту забезпечуються за рахунок технології *MIMO (Multiple Input Multiple Output)*. Ця модуляція побудована на основі застосування безлічі антен, відповідно, створюється безліч інформаційних потоків, що в багато разів збільшує швидкість передачі даних.

Чорнову версію стандарту 802.11n підтримують багато сучасних мережевих пристроїв. Підсумкова версія стандарту, яка була прийнята 11 вересня 2009 р., забезпечує швидкість до 300 Мбіт/с, багатоканальний вхід/вихід, відомий як MIMO і більше покриття.

Контрольні питання

1. Які Ви знаєте мережеві архітектури? Які їх переваги та недоліки?
2. Чому архітектура Ethernet сьогодні отримала найбільше поширення?
3. Які Ви знаєте різновиди архітектури Ethernet? Чим вони відрізняються?
4. Поясніть принцип роботи концентраторів у технології Token Ring.
5. Як забезпечується висока відмовостійкість у мережах FDDI?
6. Чи можливе використання UTP кабелю категорії 5 для реалізації Gigabit Ethernet?
7. Які Ви знаєте бездротові мережеві технології?
8. Яку роль відіграє "точка доступу" в мережах WLAN?

ЛІТЕРАТУРА: [11, 12, 13, 17, 25, 34, 39, 40, 50].

Тема 5. ТЕХНОЛОГІЇ ПОБУДОВИ РОЗПОДІЛЕНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Мета теми – ознайомитися із базовими технологіями побудови розподілених комп'ютерних мереж; розглянути відмінності між варіантами з'єднання розподілених мереж (комутація каналів, комутація пакетів).

Ключові поняття: технологія побудови розподілених комп'ютерних мереж; технології Frame Relay, X.25, ATM, ISDN; комутація каналів, комутація пакетів, комутаційні віртуальні канали, постійні віртуальні канали.

Огляд технологій розподілених мереж (WAN)

У міру того, як розміри підприємства збільшуються і його підрозділи доводиться розташовувати в різних місцях, виникла необхідність у з'єднанні між собою локальних мереж цих підрозділів і створення *розподіленої мережі (wide-area network – WAN) підприємства*.

Під *розподіленою мережею WAN* розуміють комунікаційну мережу, яка функціонує на території, що географічно перевищує сферу роботи локальної мережі. Основна відмінність розподіленої мережі від локальної полягає в тому, що для використання розподіленої мережі комерційна компанія або організація повинна укласти договір з *Інтернет-провайдером (Internet Service Provider – ISP)* для того, щоб скористатися його послугами. *Інтернет-провайдер* – це організація, яка надає послуги доступу до Інтернету та інші пов'язані з Інтернетом послуги. Для одержання доступу до смуги пропускання на великій території мережа WAN зазвичай використовує канали зв'язку, які надаються операторами служб WAN. Як правило, мережа WAN з'єднує між собою філії однієї або декількох організацій, надає доступ до зовнішніх служб і забезпечує доступ віддаленим користувачам. Розподілені мережі зазвичай передають дані різних типів, такі як звук, цифрові дані і відео.

Технології розподілених мереж функціонують на трьох нижніх рівнях еталонної моделі OSI – на фізичному, канальному і мережевому.

Служби розподілених мереж

Найчастіше використовуються такі служби розподілених мереж, як телефонний зв'язок і передача даних. Ці служби функціонують на ділянці між *точкою присутності (point of presence, POP)* та *телефонною станцією (central office)* провайдера. Телефонна станція являє собою офіс місцевої телефонної компанії, до якого приєднані всі локальні відгалуження даного регіону і в якому відбувається комутація ліній абонентів.

Огляд середовища розподіленої мережі дозволяє поділити служби провайдера на три основні групи:

1. *Виклик (call setup).* Ця служба встановлює та припиняє зв'язок між користувачами телефонів. Вона називається також сигналізацією, служба установки дзвінка використовує окремий телефонний канал, який не використовується для інших цілей. Для встановлення виклику найчастіше використовується *система сигналізації 7 (Signaling System 7 – SS7)*, яка передає і приймає телефонні керуючі повідомлення і сигнали на шляху від точки передачі до пункту призначення. В українській технічній літературі SS7 називають також *загальноканальною системою сигналізації,* або *ЗКС-7*.

2. *Тимчасове мультиплексування (Time-division multiplexing – TDM)*. Для передачі інформації від багатьох джерел використовується смуга пропускання фіксованої ширини в одному і тому ж середовищі передачі. Метод комутації каналів використовує сигналізацію для визначення маршруту виклику, який являє собою виділений шлях між відправником і одержувачем. Здійснюючи мультиплексування потоків даних у фіксовані часові проміжки, TDM дозволяє уникнути перевантаження пристроїв і зміни значень затримки. Канали TDM використовуються базовою телефонною службою та ISDN.

3. *Протокол Frame Relay.* Інформація, яка міститься у фреймах, передається по певній смузі пропускання спільно з інформацією від інших передплатників. Frame Relay є статистичною мультиплексною службою, на відміну від TDM, яка використовує ідентифікатори 2-го рівня і постійні віртуальні канали. Крім того, комутація пакетів протоколом Frame Relay використовує маршрутизацію 3-го рівня, при якій адреси відправника та одержувача містяться в самому пакеті.

Провайдери послуг розподілених мереж

Технологічний прогрес останнього десятиліття зробив доступним для проектувальників мереж ряд нових рішень. При виборі оптимального варіанта розподіленої мережі необхідно оцінити переваги і вартість послуг різних провайдерів.

При укладанні договору організацією на використання ресурсів зовнішнього провайдера мережевих послуг останній пред'являє передплатнику певні вимоги до з'єднань, які стосуються, зокрема, типу обладнання, призначеного для отримання цих послуг.

Найчастіше використовують такі терміни, пов'язані з основними типами послуг в розподілених мережах:

- *стаціонарне обладнання користувача (Customer's premises equipment, CPE)*. Це пристрої, фізично розташовані в приміщеннях користувача

(рис. 2.5.1). Вони включають в себе як пристрої, які належать споживачеві, так і пристрої, орендовані у провайдера;

- *демаркація (або Демарк) (Demarcation або demarc).* Точка, в якій закінчується CPE і починається локальне відгалуження служби провайдера. Часто ця точка знаходиться в точці присутності будівлі;
- *локальне відгалуження (*або *"остання миля").* Кабель (зазвичай мідний дріт), що веде від пункту демаркації до телефонної станції провайдера;
- *комутатор телефонної станції (CO switch).* Комутуючий пристрій, який являє собою найближчу точку присутності для служби провайдера розподіленої мережі;
- *платна частина мережі (toll network).* Комутатори та інші пристрої колективного користування в середовищі провайдера. Потік даних клієнта на своєму шляху до місця призначення може проходити по них до первинного центру, потім до районного центру і далі до регіонального або міжнародного центру.

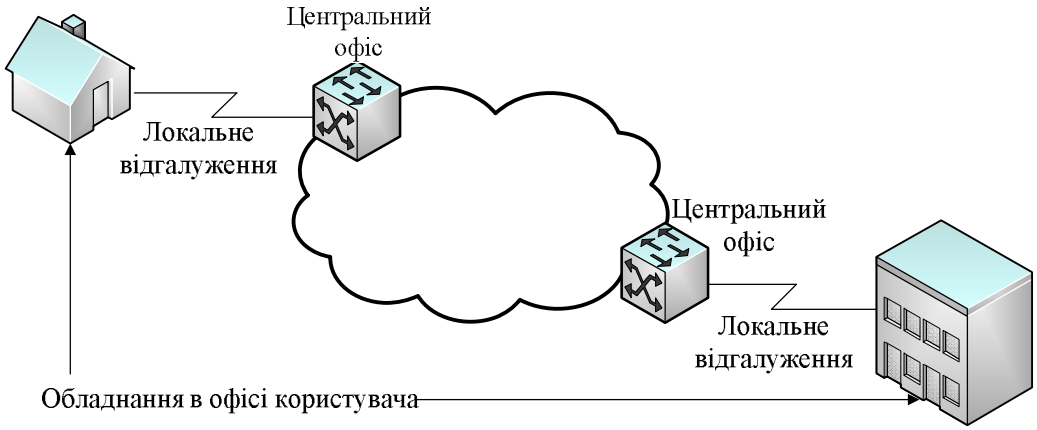


Рис. 2.5.1. Обладнання CPE

На території користувача основна взаємодія відбувається між термінальним обладнанням (data terminal equipment – DTE) та термінальним обладнанням каналу передачі даних (data circuit-terminating equipment, data communications equipment – DCE). Зазвичай DTE – це маршрутизатор, а DCE – це пристрій, який використовується для перетворення даних користувача з форми, яка використовується DTE, у форму, відповідну пристрою служби розподіленої мережі. Як показано на рис. 2.5.2, DCE являє собою приєднаний модем (modem), модуль канальної служби/модуль служби даних (channel service unit/data service unit – CSU/DSU) або термінальний адаптер/мережеве закінчення 1 (terminal adapter/network termination 1 – TA/NT1).

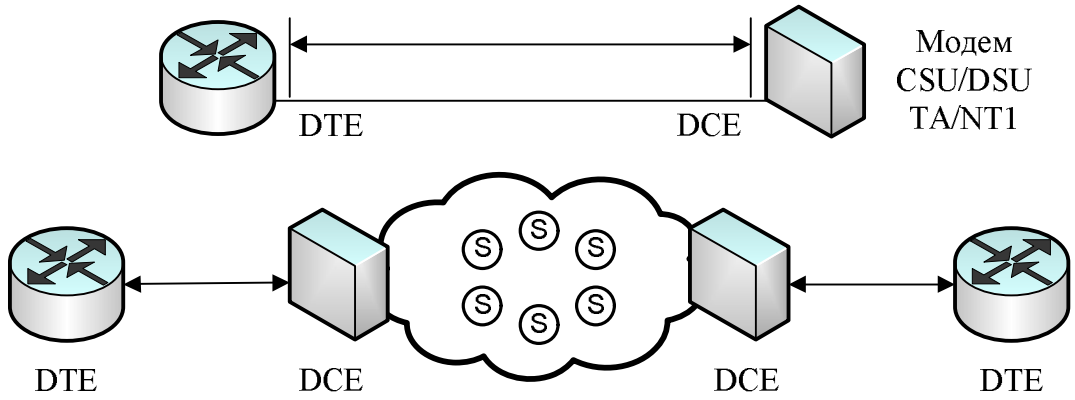


Рис. 2.5.2. Інтерфейс DTE/DCE

Відрізок шляху між двома DTE називають каналом, ланцюгом або лінією. Спочатку DCE забезпечує інтерфейс для доступу DTE до каналу середовища розподіленої мережі. Інтерфейс DTE/DCE виступає як межа, на якій відповідальність за передачу потоку даних переходить від передплатника розподіленої мережі до провайдера.

Інтерфейс DTE/DCE використовує різні протоколи (такі, наприклад, як HSSI і V.3.5), які встановлюють коди, що використовуються пристроями для взаємного обміну інформацією. Цей інтерфейс визначає, яким чином працює служба виклику і як потік даних користувача проходить розподіленою мережею.

Віртуальні канали розподілених мереж

Віртуальний канал (virtual circuit) створюється для забезпечення надійного зв'язку між двома мережевими пристроями. На противагу каналу типу "точка-точка" він являє собою не фізичний, а логічний ланцюг. Існують два типи віртуальних каналів: *комутовані віртуальні канали (switched virtual circuit – SVC)* і *постійні віртуальні канали (permanent virtual circuit – PVC)*.

Комутовані віртуальні канали створюються динамічно за запитом і припиняють своє існування після закінчення передачі. Процес здійснення зв'язку по комутованому віртуальному каналу складається з трьох етапів: створення каналу, передача даних і відключення каналу. Фаза встановлення каналу включає в себе створення віртуального ланцюга між пристроями джерела та одержувача. На етапі передачі даних здійснюється передача інформації, а фаза закінчення дії каналу містить у собі розрив зв'язку між пристроями джерела та одержувача. Комутовані віртуальні канали використовуються в ситуаціях, коли обмін інформацією між пристроями має одиничний характер. Такому каналу потрібна велика смуга пропускання в зв'язку з наявністю фаз встановлення

і розриву зв’язку, однак при цьому забезпечується зниження витрат у порівнянні з ситуацією постійно включеного віртуального ланцюга.

Постійний віртуальний канал має тільки один режим роботи – передачу даних. Такі канали використовуються в тих випадках, коли обмін даними між пристроями носить постійний характер. Постійні віртуальні канали використовують меншу смугу пропускання за рахунок відсутності фаз встановлення і розриву ланцюга, але збільшують витрати у зв’язку з постійною готовністю каналу до передачі даних.

Стандарти сигналізації та швидкості передачі в розподілених мережах

У провайдера розподіленої мережі можна замовити канали з різною швидкістю передачі даних, яка вимірюється в бітах у секунду (біт/с). Ця швидкість визначає, як швидко дані будуть передаватися розподіленою мережею. У табл. 2.5.1. наведені основні типи каналів зв’язку розподілених мереж WAN та їх смуга пропускання.

Таблиця 2.5.1

Типи каналів мереж WAN та їх пропускна здатність

Тип лінії	Стандарт сигналу	Швидкість передачі
56	DS0	56 Кбіт/с
64	DS0	64 Кбіт/с
T1	DS1	1,544 Мбіт/с
E1	ZM	2,048 Мбіт/с
J1	Y1	2,048 Мбіт/с
E3	M3	34,064 Мбіт/с
T3	DS3	44,736 Мбіт/с
OC-1	SONET	51,840 Мбіт/с
OC-3	SONET	155,520 Мбіт/с
OC-9	SONET	466,560 Мбіт/с
OC-12	SONET	622,08 Мбіт/с
OC-IS	SONET	933,12 Мбіт/с
OC-24	SONET	1244,16 Мбіт/с
OC-36	SONET	1866,24 Мбіт/с
OC-48	SONET	2488,32 Мбіт/с
OC-96	SONET	4976,640 Мбіт/с
OC-192	SONET	9953,280 Мбіт/с

Обладнання мереж WAN

По суті мережі WAN являють собою групи мереж LAN, з'єднаних між собою каналами зв'язку, які надаються провайдерами служб. Оскільки ці канали зв'язку не можуть бути безпосередньо приєднані до мереж LAN, виникає необхідність у різному типі обладнання, що реалізує цей інтерфейс.

Розподілені мережі використовують різні типи пристроїв, включаючи наступні:

1. *Маршрутизатори*, які виконують різноманітні функції, зокрема, регулювання мережевих процесів і управління портами інтерфейсів.
2. *Комутатори*, які здійснюють передачу голосових, цифрових і відеосигналів в межах смуги пропускання розподіленої мережі.
3. *Модеми*, які реалізують інтерфейс для служб голосових даних. Модеми включають в себе пристрої CSU/DSU і TA/NT1, що підтримують інтерфейс зі службами ISDN.
4. *Комунікаційні сервери*, основним завданням яких є встановлення і відключення зв'язку з користувачем.

Маршрутизатори являють собою пристрої, що реалізують мережеві служби. Комп'ютери локальних мереж, яким потрібно передати дані, направляють їх на маршрутизатор, який має як LAN-інтерфейси, так і WAN- інтерфейси, як показано на рис. 2.5.3. Для передачі даних на відповідний WAN-інтерфейс маршрутизатор використовує адресну інформацію. Маршрутизатори є активними інтелектуальними пристроями, отже вони можуть брати участь у керуванні роботою мережі. Вони здійснюють це шляхом динамічного контролю ресурсів і підтримки виконання мережею своїх завдань, таких як підтримка зв'язку, забезпечення надійності передачі даних, контролю керування та гнучкості при зміні умов роботи.

Комутатори розподіленої мережі являють собою мережеві пристрої з декількома портами, які зазвичай комутують потоки даних таких протоколів, як Frame Relay, X.25 і комутована мультимегабітна служба даних (Switched Multimegabit Data Service – SMDS). Комутатори розподілених мереж функціонують на канальному рівні еталонної моделі OSI. Комутатори фільтрують, перенаправляють і підтримують потік фреймів на основі адреси пункту призначення кожного фрейму.

Модеми являють собою пристрої, які перетворюють один в одного цифрові й аналогові сигнали шляхом модуляції і демодуляції, що дозволяє передавати цифрові дані звичайними телефонними лініями. У відправника цифрові сигнали перетворюються у форму, потрібну для передачі даних по аналогових каналах зв'язку. У пункті призначення ці аналогові сигнали перетворюються в первинну цифрову форму.

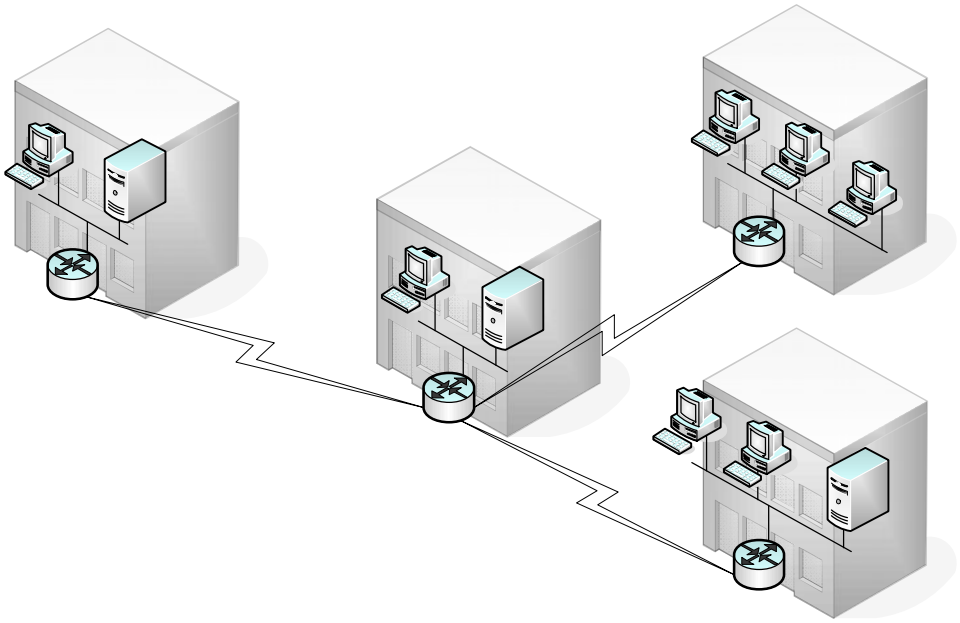


Рис. 2.5.3. Мережі WAN і LAN, з’єднані між собою за допомогою маршрутизаторів

На рис. 2.5.4 показаний приклад зв’язку між модемами, що здійснюється через розподілену мережу.

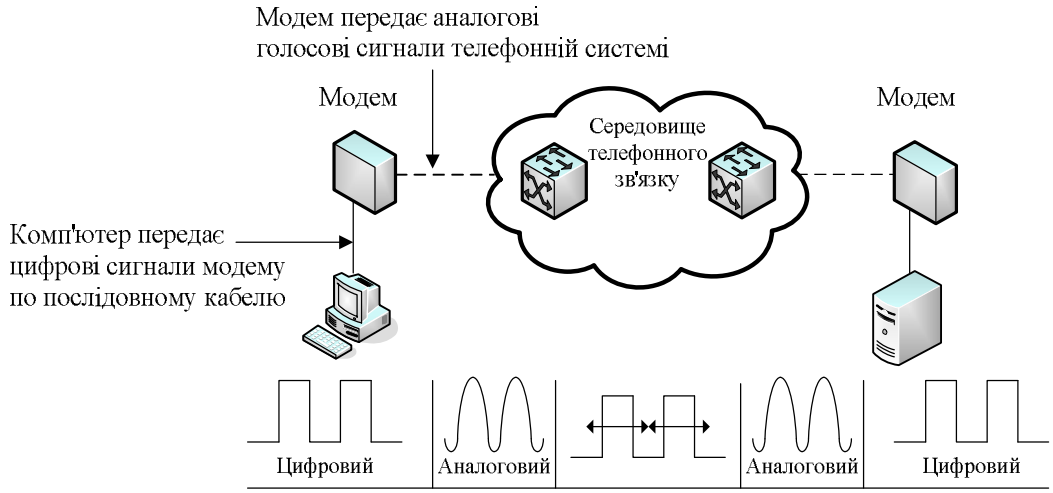


Рис. 2.5.4. Мережі WAN та модеми

Пристрій CSU/DSU – це пристрій з цифровим інтерфейсом (іноді два окремі цифрові пристрої), який адаптує фізичний інтерфейс на пристрої DTE (такому, наприклад, як термінал) до інтерфейсу на DCE-пристрої (такому, як комутатор) у мережі з комутованим носієм. На рис. 2.5.5 показано розміщення CSU/DSU в розподіленій мережі. Іноді CSU/CDU об’єднуються в одному корпусі з маршрутизатором.

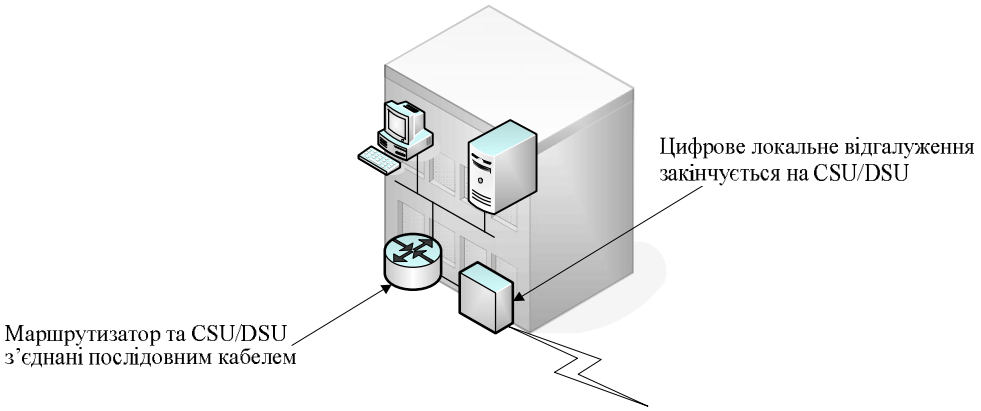


Рис. 2.5.5. Модуль CSU/DSU мережі WAN

Термінальний адаптер ISDN (Integrated Services Digital Network) – це пристрій, який використовується для з'єднання інтерфейсу базової швидкості передачі (Basic Rate Interface – BRI) з іншими інтерфейсами. Термінальний адаптер зазвичай являє собою ISDN-модем.

Комунікаційні сервери, які концентрують передачу даних віддалених користувачів, використовуються для забезпечення дистанційного доступу до мереж LAN. Вони можуть мати різні комбінації аналогових і цифрових (ISDN) інтерфейсів і одночасно передають дані десятків і сотень користувачів.

Типи каналів розподілених мереж

Існують два типи каналів, які використовуються в розподілених мережах: виділені лінії і комутовані з'єднання. Комутовані з'єднання, у свою чергу, можуть виконувати комутацію пакетів чи каналів.

Виділені лінії

У тих випадках, коли потрібні постійні виділені з'єднання, використовуються орендовані лінії із пропускною здатністю до 2,5 Гбіт/с.

Канали "точка-точка" забезпечують заздалегідь установлені канали зв'язку мереж WAN від офісу користувача до віддаленої мережі через несучу мережу, таку, наприклад, як мережа телефонної компанії. Канали "точка-точка" зазвичай орендуються в оператора зв'язку і тому часто називаються *орендованими лініями*. Оператори зв'язку пропонують виділені лінії з різними можливими значеннями пропускної здатності.

Вартість виділеної лінії зазвичай визначається необхідною пропускною здатністю і відстанню між точками, що з'єднуються. Канали "точка-точка", як правило, коштують дорожче, ніж служби спільного використання, такі як Frame Relay. Вартість рішень, що використовують виділені лінії, значно підвищується, якщо ці лінії з'єднують вели-

ку кількість мережевих вузлів. Пропускна здатність виділених ліній забезпечує відсутність затримки й деренчання. Для деяких додатків, таких як електронна торгівля, постійна доступність таких з'єднань є суттєвою.

Для кожного з'єднання виділеної лінії потрібен послідовний порт маршрутизатора. Потрібні також модулі CSU/DSU і канал від провайдера служби. Виділені лінії часто використовуються для побудови WAN-мереж, оскільки забезпечують постійну виділену смугу пропускання. Такі лінії традиційно користуються більшим попитом, однак вони мають і ряд недоліків. Обсяг передачі даних мережею WAN часто змінюється, тому пропускна здатність каналу рідко відповідає конкретним потребам користувачів. Крім того, кожній кінцевій точці потрібен окремий інтерфейс маршрутизатора, тому маршрутизатор у центральній точці зіркоподібної топології виявляється досить дорогим. Будь-які зміни параметрів виділеної лінії, як правило, вимагають відвідування вузла оператором для зміни пропускної здатності.

Виділені лінії можуть використовуватися для створення безпосередніх з'єднань типу "точка-точка" між мережами LAN підприємства. Вони також використовуються для приєднання окремих філій до мережі з комутацією пакетів. У такому каналі можуть бути мультиплексовані кілька з'єднань, що зменшує довжину лінії й вимоги до кількості інтерфейсів центральних маршрутизаторів у топології мережі.

З'єднання із комутацією каналів

Комутація каналів (circuit switching) може бути використана при встановленні з'єднання для передачі голосових або звичайних даних між двома географічно віддаленими пунктами. Перед початком передачі корисних даних необхідно створити з'єднання шляхом встановлення комутаторів. Це здійснюється телефонною службою шляхом набору номера у звичайних голосових лініях або в цифрових каналах ISDN.

Коли абонент робить телефонний дзвінок, набраний номер використовується для встановлення комутаторів у проміжних пунктах всією довжиною маршруту таким чином, щоб утворювався безперервний канал від телефонної трубки сторони, яка викликає, до телефонного апарата сторони, яку викликають. Оскільки для створення каналу використовується операція комутації, така телефонна система називається мережею з комутацією каналів. Якщо в такій системі замінити слухавки модемами, приєднаними до комп'ютерів, то таким комутованим каналом можна передавати комп'ютерні дані. На рис. 2.5.6 наведений приклад мережі з комутацією каналів.

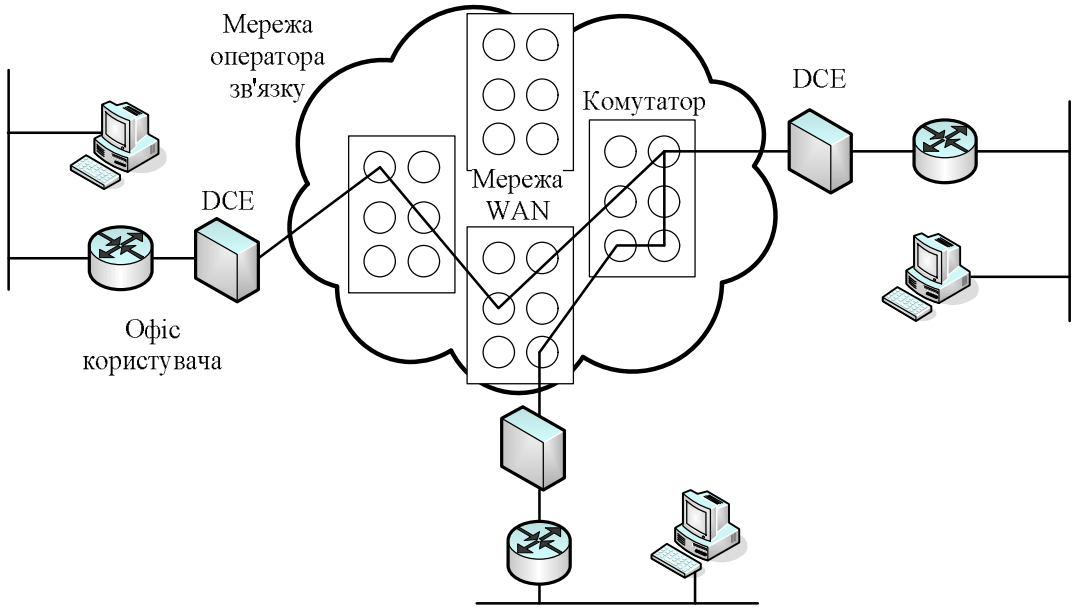


Рис. 2.5.6. Комутація каналів

На практиці канал може містити в собі ділянки, середовищем передачі яких може бути не тільки мідний кабель, а, наприклад оптоволоконний кабель або мікрохвильовий зв'язок. На внутрішніх ділянках маршруту між окремими проміжними точками можуть передаватися дані й інших користувачів, тому для надання їм усім по черзі можливості використовувати з'єднання використовується *мультиплексування з поділом часу (Time-division Multiplexing – TDM)*. Використання TDM гарантує, що кожному користувачеві буде надана певна частина пропускних можливостей даного з'єднання.

Якщо канал використовується для передачі комп'ютерних даних, то використання таких фіксованих частин пропускної здатності може виявитися неефективним. Наприклад, якщо канал використовується для доступу до Internet, то при передачі Web-сторінки відбувається сплеск активності, після якого наступає період бездіяльності каналу поки користувач читає сторінку, а потім новий сплеск при одержанні нової. Такі коливання інтенсивності між нульовою і максимальною типові для потоків даних у комп'ютерних мережах. Оскільки користувач має виключне право на використання такої фіксованої пропускної здатності, то комутовані канали є дорогим способом передачі даних.

Прикладами з'єднань із комутацією каналів можуть бути:

- загальнодоступна телефонна мережа, що комутується (Public Switched Telephone Network – PSTN);
- інтерфейс базової швидкості ISDN (Basic Rate Interface – BRI);
- інтерфейс первинної швидкості ISDN (Primary Rate Interface –PRI).

З'єднання із комутацією пакетів

Багатьом користувачам WAN-мереж не вдається добитися ефективного використання пропускної здатності, яка надається виділеним каналом, постійним або таким, що комутується, внаслідок того, що їх потоки даних мають вибуховий характер. Для більш раціонального обслуговування таких користувачів провайдери служб надають технології, у яких дані передаються в позначених гніздах, фреймах або пакетах мережами з *комутацією пакетів (packet switching)*.

Оскільки канали, які з'єднують проміжні пункти або комутатори в мережі провайдера, виділяються окремому користувачеві тільки в тому випадку, якщо в нього є дані для передачі, стає можливим використання каналів багатьма користувачами, а вартість каналу для кожного користувача може виявитися значно нижчою за вартість при використанні виділеного з'єднання з комутацією каналів. З іншого боку, внаслідок того, що окремому пакету, можливо, доведеться очікувати передачі на комутаторі доти, поки пакет іншого користувача не залишить канал, *затримка (delay, latency)* і *варіація затримки* (також називається *деренчанням (variability of delay, jitter)*) у мережах з комутацією пакетів більша, ніж в мережах з комутацією каналів. Незважаючи на затримку й деренчання, властиві спільно використовуваним мережам, сучасні технології забезпечують задовільну передачу такими мережами голосових даних і навіть відео. На рис. 2.5.7 наведений приклад мережі з комутацією пакетів.

Комутатори в мережах з комутацією пакетів повинні бути здатні визначити за адресною інформацією кожного пакета наступний канал, у який слід відправити цей пакет. Для визначення цього каналу може бути використано два підходи: *без орієнтації на з'єднання (connectionless)* і *орієнтований на встановлення з'єднання.* У системах без орієнтації на з'єднання, таких, наприклад, як Internet, вся адресна інформація міститься в кожному пакеті. У системах, орієнтованих на з'єднання, маршрут кожного пакета визначений і кожному пакету потрібен лише ідентифікатор. У технології Frame Relay такий ідентифікатор називається *ідентифікатором канального рівня (data-link connection identifier – DLCI)*. Комутатор визначає маршрут у висхідному напрямку, переглядаючи таблицю ідентифікаторів, яка знаходиться в його оперативній пам'яті. Сукупність позицій у всіх таких таблицях визначає конкретний маршрут або канал у системі; якщо такий "канал" фізично існує тільки під час проходження пакету даним каналом, то він називається *віртуальним каналом*.

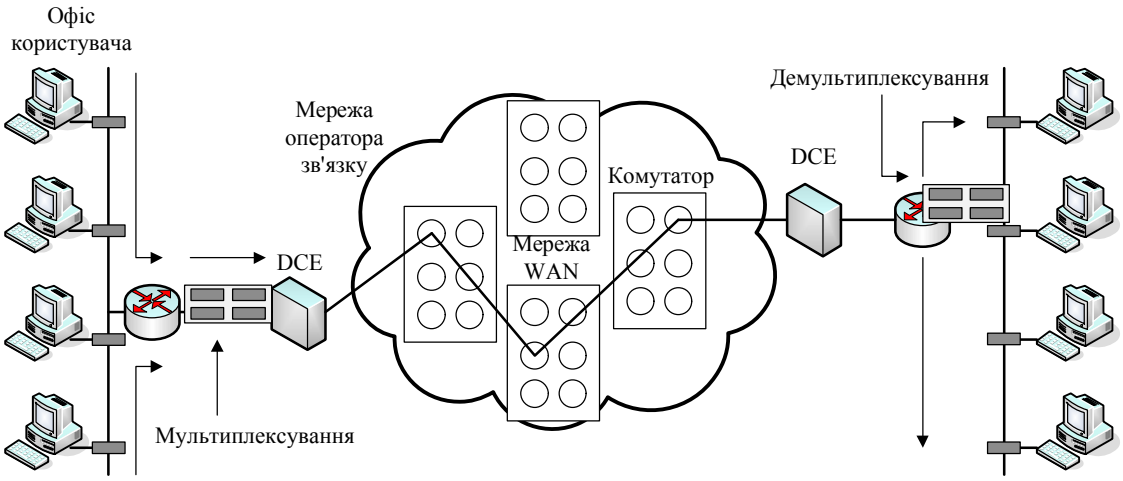


Рис. 2.5.7. Мережа, що використовує комутацію пакетів

Якщо маршрути створюються відразу після включення комутаторів, то вони називаються *постійними віртуальними каналами (Permanent Virtual Circuits, PVC)*; якщо маршрути створюються на вимогу, то вони називаються *віртуальними каналами, що комутуються (Switched Virtual Circuit – SVC)*. Позиції таблиць, що утворюють віртуальний канал, можуть бути заповнені шляхом розсилання мережею запитів на з'єднання (які комутуються віртуальний каналом – SVC). Дані, які повинні пройти каналом SVC, повинні очікувати заповнення відповідних позицій таблиць, однак після встановлення канал SVC зможе функціонувати протягом декількох годин, днів або навіть тижнів. У тому випадку, коли канал повинен бути доступний постійно (канал PVC), позиції таблиць заповнюються під час завантаження комутаторів, тому канали PVC завжди доступні.

Прикладами технологій, що використовують з'єднання з комутацією пакетів або гнізд, є X.25, Frame Relay, ATM.

Технології WAN-мереж

Аналогові з'єднання віддаленого доступу (PSTN)

У тих випадках, коли мережею передаються невеликі обсяги даних і потоки даних мають пульсуючий характер, використання модемів і аналогових телефонних ліній дозволяє здійснювати виділені з'єднання, що комутуються, з невеликою пропускною здатністю.

У традиційній телефонії телефонний апарат користувача з'єднаний з мережею PSTN мідним кабелем – локальним відгалуженням. Під час телефонної розмови сигнал у локальному відгалуженні являє собою електричну копію голосу абонента і є безупинно мінливим сигналом.

Локальне відгалуження не дозволяє безпосередньо передавати двійкові комп'ютерні дані, однак при використанні модему комп'ютерні дані можуть бути передані голосовою телефонною мережею. Модем модулює бінарні дані на аналогових сигналах і, навпаки, демодулює аналогові сигнали в бінарні дані.

Швидкість такого перетворення обмежена фізичними характеристиками локального відгалуження і його приєднання до PSTN і не може перевищувати верхньої межі, яка дорівнює приблизно 33 Кбіт/с. Ця швидкість може бути підвищена приблизно до 56 Кбіт/с за умови, що сигнал надходить із цифрового джерела.

На невеликих підприємствах ця швидкість може виявитися задовільною для таких операцій, як обмін комерційною інформацією (дані продажів, прейскуранти, стандартні звіти тощо) і для електронної пошти. Для передачі більших файлів або резервування даних користувач може скористатися перевагами низької вартості такого зв'язку в неробочий час і у вихідні дні. Тарифи такого зв'язку залежать від відстані між кінцевими точками, часу доби й тривалості виклику.

Перевагами використання модему і аналогової лінії є простота і невелика вартість реалізації. Недоліками є невисока швидкість передачі і відносно великий час, що витрачається на встановлення з'єднання. Часто в ситуаціях, коли використовуються модеми, досить тривалий час встановлення з'єднання не є проблемою. Постійна виділена лінія не викликає затримки й деренчання для даних, переданих по каналу "точка-точка", однак голосові й відеодані не можуть адекватно передаватися при таких низьких швидкостях.

Технологія ISDN

За минулий час передача даних з'єднаннями або магістралями мережі PSTN аналогових мультиплексованих сигналів з поділом частот поступилася місцем передачі *мультиплексованих цифрових сигналів з поділом часу (time-division multiplexed – TDM)*. Очевидним наступним кроком є переведення локального відгалуження на передачу цифрових сигналів, що забезпечує комутовані з'єднання з більшою пропускною здатністю.

Служба цифрової мережі інтегрованих служб (Integrated Services Digital Network – ISDN) перетворює локальне відгалуження в цифрове з'єднання TDM. Це з'єднання має канали носія із пропускною здатністю 64 Кбіт/с (B-канали) для передачі голосу й даних і сигнальний канал (дельта-канал або D-канал) для встановлення виклику та для інших цілей.

Інтерфейс базової швидкості ISDN (Basic Rate Interface – BRI). призначений для домашніх офісів і малих підприємств, забезпечує два

B-канали й один D-канал із пропускною здатністю 16 Кбіт/с (рис. 2.5.8). Для великих підприємств призначений *інтерфейс первинної швидкості передачі ISDN (Primary Rate Interface – PRI)*. Інтерфейс PRI надає в Північній Америці 23 B-канали і один D-канал, що забезпечує сумарну пропускну здатність до 1,544 Мбіт/с (ця величина містить у собі деякий обсяг службового навантаження для синхронізації). У Європі, Австралії й інших частинах світу PRI ISDN надає 30 B-каналів і один D-канал, які забезпечують сумарну пропускну здатність до 2,048 Мбіт/с (враховуючи деякий обсяг службового навантаження для синхронізації) рис. 2.5.8. Відзначимо, що швидкість передачі інтерфейсу PRI у Північній Америці відповідає швидкості передачі лінією T1. Швидкість міжнародного інтерфейсу PRI відповідає швидкості передачі лінією E1.

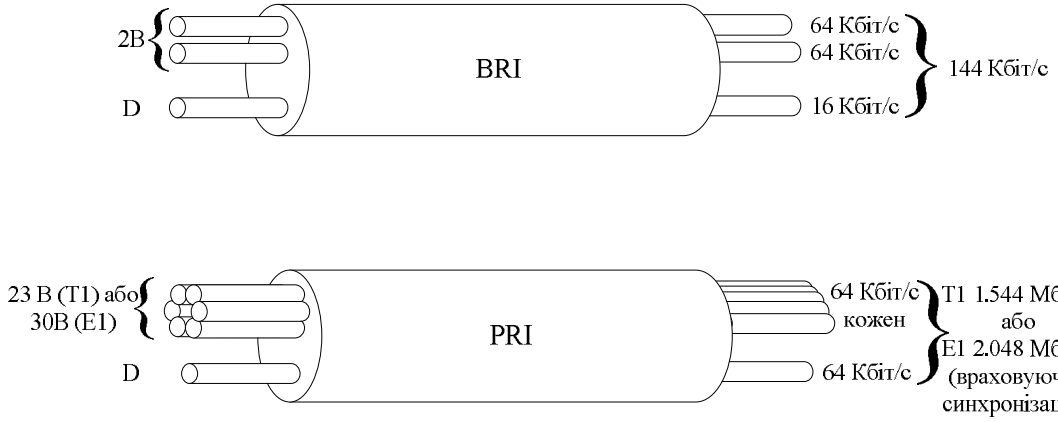


Рис. 2.5.8. Канали ISDN

D-канал інтерфейсу BRI завантажений явно недостатньо, оскільки йому потрібно управляти лише двома B-каналами. Тому деякі провайдери використовують його для передачі даних з невеликими бітовими швидкостями, таких, наприклад, як дані з'єднань X.25 зі швидкістю 9,6 Кбіт/с.

Для невеликих WAN-мереж BRI ISDN забезпечує ідеальний механізм зв'язку. Інтерфейс BRI має невеликий час встановлення виклику (менше однієї секунди), а його B-канал 64 Кбіт/с забезпечує більшу пропускну здатність, ніж аналоговий модемний канал. Якщо потрібна більша пропускна здатність, то можлива активізація другого B-каналу, що забезпечує пропускну здатність 128 Кбіт/с. Хоча й недостатнє для передачі відео, таке підвищення дозволяє підтримувати на додаток до передачі даних декілька телефонних розмов.

Іншим можливим застосуванням технології ISDN є її використання за необхідності як додаткового джерела підвищення пропускної здатності для вже наявного з'єднання виділеною лінією. Виділена лінія проектується для основних потоків навантаження, а ISDN додається при пікових навантаженнях. ISDN може бути також використана як резервна лінія у випадку непередбачених збоїв у виділеній лінії.

Тарифи служби ISDN на кожний B-канал аналогічні тарифам голосових з'єднань, тобто два одночасні з'єднання 64 Кбіт/с коштують удвічі дорожче, ніж одне.

При використанні інтерфейсу PRI ISDN дві кінцеві точки можуть бути з'єднані декількома B-каналами, що дозволяє забезпечити відеоконференцію або кілька широкосмугових з'єднань для передачі даних без затримки або деренчання. На більших відстанях використання декількох з'єднань може стати досить дорогим.

Технологія X.25

На противагу дорогим виділеним лініям провайдери служб телекомунікацій розробляють мережі з комутацією пакетів, у яких спільне використання каналів зменшує витрати користувачів. Першою із таких мереж з комутацією пакетів була група протоколів, стандартизована як X.25. Служба протоколу X.25 забезпечує низькошвидкісне спільно використовуване з'єднання зі змінною пропускною здатністю, яке може бути постійним або комутованим. На рис. 2.5.9 показана WAN-мережа протоколу X.25.

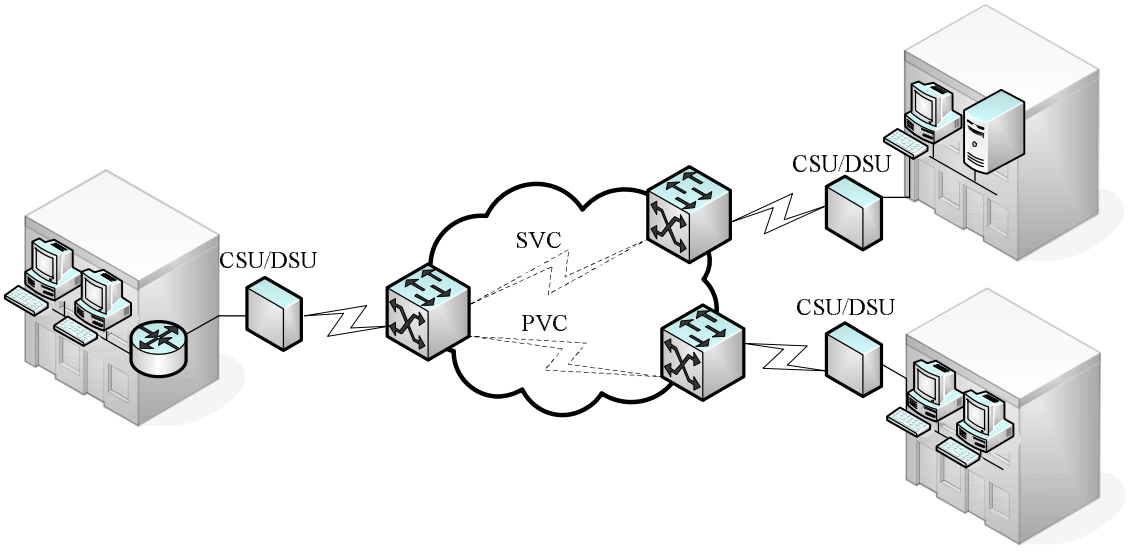


Рис. 2.5.9. WAN-мережа протоколу X.25

Користувачі служби одержують мережеву адресу. У такій мережі можуть бути створені віртуальні канали, якими одержувачам передаються пакети запиту на встановлення з'єднання. Створений канал

SVC ідентифікується своїм номером. Пакети даних, позначені цим номером, доставляються за відповідною адресою. В одному з'єднанні можуть бути активними кілька каналів.

Абоненти служби приєднуються до мережі X.25 виділеними лініями або з'єднаннями дистанційного доступу. У мережах X.25 також можуть бути присутніми попередньо встановлені з'єднання між користувачами, які являють собою постійні канали PVC.

Мережі X.25 можуть виявитися дуже ефективними відносно вартості, оскільки тарифи в них засновані на обсязі переданих даних, а не на відстані або тривалості з'єднання. Доставка даних може відбуватися з будь-якою швидкістю аж до максимальної для даного з'єднання. Ця якість мережі забезпечує певний рівень гнучкості при її використанні. Мережі X.25 зазвичай мають невисоку пропускну здатність, з максимальним значенням, рівним 48 Кбіт/с. Крім того, передача пакетів даних часто супроводжується затримками, характерними для спільно використовуваних мереж.

Технологія Frame Relay

У зв'язку зі збільшенням попиту на широкосмугову комутацію пакетів з низькою затримкою провайдери зв'язку почали використовувати технологію *Frame Relay (Frame Relay – FR)*. Хоча загальна структура такої мережі схожа на мережу X.25, допустимі швидкості передачі даних в ній досягають значень до 4 Мбіт/с, а деякі провайдери пропонують і більші швидкості.

Мережі Frame Relay відрізняються від мереж X.25 у декількох аспектах. Найбільш важливою відмінністю є те, що Frame Relay використовує значно простіший протокол на канальному рівні. Для позначення модуля даних на канальному рівні використовується термін *фрейм (frame)*.

Протокол Frame Relay не здійснює контролю помилок і керування потоками. Завдяки спрощеній обробці фреймів досягається мала затримка. Заходи, прийняті для запобігання скупчення фреймів на проміжних комутаторах, допомагають зменшити рівень деренчання.

Більшість з'єднань Frame Relay використовують постійні канали PVC, а не комутовані канали SVC. З'єднання із межею мережі часто здійснюється виділеною лінією. Тарифи Frame Relay ґрунтуються на пропускній здатності порту на межі мережі й зазначеної в контракті пропускної здатності або *погодженої швидкості передачі інформації (committed information rate – CIR)* різних каналів PVC, що проходять через цей порт.

Frame Relay забезпечує постійні, спільно використовувані з'єднання, із середньою шириною смуги пропускання, якими передаються як звичайні, так і голосові дані. Технологія Frame Relay є ідеа-

льним варіантом для з'єднання між собою LAN-мереж підприємства. Маршрутизатору LAN-мережі потрібен тільки один інтерфейс, навіть якщо використовуються кілька віртуальних каналів, а коротка лінія доступу або локальне відгалуження до межі мережі Frame Relay забезпечує ефективні з погляду фінансових витрат з'єднання між розділеними більшими відстанями LAN-мережами.

Технологія ATM

Паралельно з розвитком технології Frame Relay провайдери служб зв'язку усвідомили необхідність у технології постійного спільного використання з дуже малою затримкою, низьким рівнем деренчання і пропускною здатністю, значно більшою, ніж була доступна раніше. Таким рішенням стала технологія *асинхронного режиму передачі (Asynchronous Transfer Mode – ATM)*. У мережах ATM досягаються швидкості передачі до 155 Мбіт/с. Структура мережі ATM аналогічна структурам інших мереж спільного доступу, таких як X.25 і Frame Relay, однак технологія ATM забезпечує з'єднання з дуже високими швидкостями передачі даних. Ця технологія особливо ефективна при передачі даних, для яких вкрай небажана затримка, таких як відео.

Режим асинхронної передачі являє собою технологію, що дозволяє передавати голос, відео й звичайні дані відкритими (загальнодоступними) і приватними мережами. Основою архітектури ATM є не фрейми, а гнізда. Ці гнізда ATM мають фіксовану довжину 53 байти. Таке гніздо містить у собі 5-байтовий ATM-заголовок, за яким ідуть 48 байтів корисного навантаження. Використовувані в ATM невеликі гнізда фіксованої довжини в 53 байти добре підходять для передачі голосових і відеоданих, оскільки для таких даних неприпустима затримка. Вони не можуть очікувати закінчення передачі великого пакета даних.

53-байтове гніздо ATM, у якому на 48 байтів корисного навантаження доводиться 5 байтів службових даних, менш ефективне, ніж фрейми і пакети технологій Frame Relay і X.25, які мають більший розмір. Якщо в гніздах передаються розбиті на частини пакети мережевого рівня, то рівень службового навантаження зростає, оскільки комутатор ATM повинен бути здатним зібрати первісні пакети в пункті призначення. Для передачі того самого обсягу даних мережевого рівня типовій лінії ATM потрібно на 20 % більше пропускної здатності, ніж каналу Frame Relay.

У технології ATM використовуються як канали PVC, так і канали SVC, хоча в WAN-мережах частіше використовуються постійні канали PVC. Як і в інших технологіях спільного доступу, ATM дозволяє реалізувати кілька віртуальних каналів в одному з'єднанні виділеною лінією із межею мережі.

Технологія DSL

Телефонна система накладає обмеження на пропускну здатність локального відгалуження. Відділення локального відгалуження від телефонної системи дозволяє забезпечити значно більшу пропускну здатність без прокладання нового кабелю. На рис. 2.5.10 показане DSL-з'єднання.

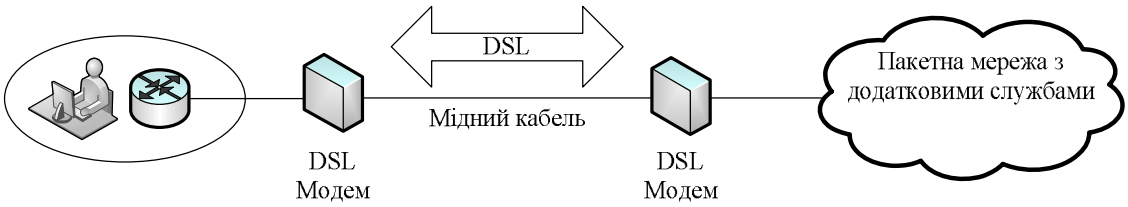


Рис. 2.5.10. DSL-з'єднання

Технологія *цифрового абонентського каналу (Digital Subscriber Line – DSL)* дозволяє відокремити локальне відгалуження від комутатора телефонної станції або *апаратури локального оператора зв'язку (local exchange)*. Замість цього з'єднання DSL приєднує локальне відгалуження даного абонента, разом з локальними відгалуженнями інших абонентів даної зони до мультиплексора доступу абонентського цифрового каналу *(Digital Subscriber Line Access Multiplexor – DSLAM)*, також розташованому на телефонній станції. Для підтримки звичайної телефонної служби мультиплексор DSLAM приєднується до комутатора телефонної станції. Він також приєднується, зазвичай, за допомогою з'єднання ATM до Internet-служби провайдера DSL.

Канал DSL підтримує постійне з'єднання. Як тільки користувач включає комп'ютер, приєднаний до модему DSL, відразу ж здійснюється DSL-з'єднання. При такому підході не витрачається час на набір номера та на встановлення з'єднання. Двома основними типами технологій DSL є асиметрична (asymmetric – ADSL) і симетрична (symmetric – SDSL). Усі форми служби DSL попадають в одну із цих двох категорій; у кожній з них є кілька різновидів. Для узагальненого позначення всіх різних форм служби DSL іноді використовується абревіатура xDSL. У ADSL доступна смуга пропускання каналу розподілена між вихідним і вхідним трафіком несиметрично – для більшості користувачів вхідний трафік значно більш суттєвий, ніж вихідний, тому надання для нього більшої частини смуги пропускання цілком виправдано. Симетрична служба надає однакову швидкість в обох напрямках.

Різновиди служби DSL надають різну пропускну здатність, при цьому в більшості з них пропускна здатність більша, ніж у виділених ліній T1 і E1. Швидкість передачі, яка досягається при цьому, значною

мірою залежить від реальної довжини локального відгалуження, а також від типу і стану кабелю. Для задовільної якості служби довжина локального відгалуження не повинна перевищувати 5,5 км. Варто відзначити, що абонент не може безпосередньо приєднатися до мережі підприємства. Для цього він повинен спочатку приєднатися до Internet-провайдера, а потім створити IP-з'єднання через мережу Internet з підприємством. Такий спосіб зв'язку пов'язаний з певними загрозами безпеки інформації.

Кабельні модеми

У міському середовищі для розповсюдження телевізійних сигналів широко використовується коаксіальний кабель. Мережа кабельного телебачення також може бути використана для доступу до мережі, надаючи значно більшу смугу пропускання, ніж звичайне локальне відгалуження телефонної служби.

Кабельні модеми дозволяють здійснювати двосторонню передачу даних в обох напрямках, використовуючи ті ж коаксіальні лінії, за якими передається кабельне телебачення. Деякі провайдери кабельних служб обіцяють швидкості передачі, що в 6,5 раза перевершують швидкості виділених ліній T1. Така швидкість робить кабель привабливим середовищем для швидкої передачі великих обсягів цифрової інформації, включаючи відео, аудіофайли і великі обсяги звичайних цифрових даних. Таким чином, кабельні модеми забезпечують швидкості більші, ніж у виділених ліній, з меншими витратами і більш простим встановленням. Кабельні модеми забезпечують цілодобове з'єднання. Відразу після включення живлення комп'ютера користувач підключається до мережі Internet. Таке встановлення дозволяє економити час і зусилля на набір номера для з'єднання. Однак постійне включення ("always-on") кабельного з'єднання означає, що приєднаний комп'ютер виявляється постійно вразливим до атак хакерів і повинен бути надійно захищений за допомогою брандмауера.

Кабельний модем здатний забезпечити доставку даних зі швидкістю 30-40 Мбіт/с по одному кабельному каналу 6 МГц. Це в 500 разів швидше, ніж модем 56 Кбіт/с.

При використанні кабельного модему абонент може продовжувати прийом кабельного телебачення одночасно з отриманням даних на персональному комп'ютері.

Як і у випадку використання DSL, у абонента немає іншого вибору, окрім як скористатися послугами Internet-провайдера, що надає службу кабельного модему, і приєднуватися до мережі свого підприємства за допомогою додатка TCP/IP, такого як Telnet. Іншим недоліком є

те, що всі локальні абоненти спільно використовують смугу пропускання кабелю, так само, як це відбувається у випадку коаксіальних з'єднань Ethernet. У міру того, як до служби підключається все більша кількість користувачів, реальна смуга пропускання може виявитися значно меншою, ніж очікувана. Ще більш серйозною проблемою є забезпечення необхідного рівня безпеки.

Контрольні питання

1. Що таке WAN?
2. Яку функцію виконують пристрої DTE/DCE? Наведіть приклади пристроїв DTE/DCE.
3. Чим відрізняються з'єднання із комутацією пакетів і комутацією каналів?
4. Чим відрізняються комутовані віртуальні канали від постійних віртуальних каналів?
5. Що таке BRI і PRI? Чим вони відрізняються?
6. Які особливості технологій X.25 та Frame Relay?
7. У яких випадках застосовуються виділені лінії?
8. Що таке DSL, ATM, ISDN?

ЛІТЕРАТУРА: [2, 4, 18, 31, 32, 44].

Тема 6. СТЕКИ ПРОТОКОЛІВ КОМП'ЮТЕРНИХ МЕРЕЖ

Мета теми – ознайомитись з різними видами стеків протоколів; розглянути протоколи комп'ютерних мереж і їх співвідношення із моделлю OSI; розглянути відмінності і особливості протоколів.

Ключові поняття: стек протоколів, види стеків протоколів, стек протоколів OSI, стек протоколів TCP/IP, стек протоколів IPX/SPX, стек протоколів NetBIOS/SMB.

Стеки протоколів

Стек протоколів – це ієрархічно впорядкована сукупність протоколів, достатніх для реалізації взаємодії вузлів у комп'ютерній мережі.

На відміну від моделі, що являє собою концептуальну схему взаємодії систем, стек протоколів – це набір конкретних специфікацій, що дозволяє реалізувати мережеву взаємодію.

Існує досить багато стеків протоколів, які широко використовуються у мережах. Це стеки, які з'явилися на основі міжнародних і національних стандартів, та стеки, запропоновані фірмами-виробниками мережевого обладнання, які одержали поширення завдяки поширеності обладнання саме цих фірм.

Прикладами популярних стеків протоколів можуть служити: стек IPX/SPX фірми Novell, стек TCP/IP, що використовується у мережі Internet і в багатьох мережах на основі операційної системи UNIX, стек Decnet корпорації Digital Equipment і деякі інші. Окремі з них будуть більш докладно розглянуті нижче.

Застосування в мережі різних стеків комунікаційних протоколів породжує велику різноманітність характеристик і структур цих мереж. У невеликих мережах достатньо використання одного стеку, але у великих корпоративних мережах, що поєднують різні підмережі, як правило, паралельно використовуються декілька стеків.

Протоколи можуть бути реалізовані у вигляді програмних елементів операційної системи. Наприклад, дуже часто протоколи канального рівня виконані у вигляді драйвера мережевого адаптера, а функції протоколів верхніх рівнів представляються серверними або клієнтськими компонентами мережевих служб.

У комунікаційному обладнанні реалізуються протоколи нижніх рівнів, які більш стандартизовані, ніж протоколи верхніх рівнів, що є передумовою для успішної спільної роботи обладнання від різних виробників.

Наприклад, на фізичному та канальному рівнях практично у всіх стеках використовуються ті самі протоколи. Це добре стандартизовані протоколи Ethernet, Token Ring, FDDI та інші, що дозволяють використовувати у всіх мережах однакову апаратуру.

Протоколи більш високих рівнів, починаючи з мережевого, у існуючих стандартних стеках відрізняються більшою різноманітністю та найчастіше не відповідають рекомендованій моделлю OSI розбивці на рівні. Наприклад, функції сеансового рівня і рівня представлення можуть бути об’єднані із прикладним рівнем.

Така невідповідність пояснюється тим, що мережева модель OSI з’явилася як результат узагальнення вже існуючих і реально використовуваних стеків, а не навпаки.

Стек протоколів OSI

Кожному рівню моделі OSI відповідає один або кілька протоколів, які виконують функції забезпечення мережевої взаємодії.

Стек протоколів OSI відповідає моделі OSI і включає протоколи для всіх семи рівнів (табл. 2.6.1).

На фізичному і канальному рівнях стека OSI використовуються стандартні протоколи Ethernet, Token Ring тощо.

Мережевий рівень реалізований за допомогою протоколів ES-IS і IS-IS.

Таблиця 2.6.1

Стек протоколів OSI

Рівень моделі OSI	Протоколи OSI
7. Прикладний	FTAM, VTP, X.400 і X.500
6. Представлення	Протокол представлення OSI
5. Сеансовий	Сеансовий протокол OSI
4. Транспортний	Транспортний протокол OSI
3. Мережевий	ES-IS, IS-IS
2. Канальний	Ethernet, Token Ring, FDDI, X.25, ISDN, ATM, LAP-D, PPP та інші
1. Фізичний	Специфікації фізичних середовищ

ES-IS (End System to Intermediate System routing exchange protocol) – протокол маршрутизації кінцевих систем, за допомогою якого кінцеві системи (робочі станції) сповіщають про себе проміжні системи (наприклад, концентратори).

IS-IS (Intermediate System to Intermediate System routing exchange protocol) – протокол маршрутизації проміжних станцій, за допомогою якого проміжні системи обмінюються інформацією про діючі маршрути в мережі.

Ці протоколи використовуються для "розвідки" і побудови повної, послідовної картини топології мережі, щоб забезпечити можливість маршрутизації пакетів, які пересилаються.

Транспортний, сеансовий і рівень представлення реалізовані відповідними протоколами OSI, які мають мале поширення.

Найбільшу популярність отримали протоколи прикладного рівня стека OSI. Це, передусім, протоколи FTAM, VTP, X.400 та X.500.

FTAM (File Transfer Access and Management) – протокол передачі, забезпечення доступу і управління файлами.

VTP (Virtual Terminal Protocol) – протокол, що описує роботу віртуального терміналу.

X.400 – являє собою набір рекомендацій Міжнародного консультативного комітету з телеграфії та телефонії (CCITT – *від франц. Comité Consultatif International Téléphonique et Télégraphique*), у яких описуються системи пересилання електронних повідомлень. Протокол X.400 визначає структуру повідомлень електронної пошти так, що всі повідомлення задовольняють стандартний формат.

X.500 – розширення стандарту X.400, який визначає формат адреси повідомлення, що й дозволяє всім системам електронної пошти

зв’язуватися між собою. З самого початку метою рекомендацій X.500 є розробка стандартів глобальної довідкової служби. Однак процес доставки повідомлення вимагає знання адреси одержувача. При великих розмірах мереж виникає проблема зберігання, пошуку й одержання адрес. Рішенням цієї проблеми є довідкова служба, яка допомагає одержувати адреси відправників і одержувачів, що й являє собою розподілену базу даних імен і адрес.

Модель OSI зробила популярною ідею загальної моделі рівнів протоколів, яка визначає взаємодію між мережевим обладнанням і програмним забезпеченням. Проте стек протоколів OSI, розроблений як частина проекту й спрямований забезпечити однорідність при побудові мереж, і, як наслідок, універсальність взаємодії, був сприйнятий багатьма як занадто ускладнений і мало реалізований. Справа в тому, що розробка й впровадження стека OSI припускала відмову від існуючих протоколів і перехід на нові на всіх рівнях стека. Це дуже ускладнило реалізацію стека й послужило причиною для відмови від нього багатьох компаній, що зробили значні інвестиції в інші мережеві технології.

Таким чином, коли були реалізовані протоколи для моделі OSI, виявився ряд проблем:

- протоколи засновані на концепціях, які мають мало сенсу в сучасних мережах;
- специфікації у деяких випадках виявилися неповними або такими, що суперечать одна одній;
- за функціональними можливостями протоколи ISO/OSI поступалися іншим протоколам;
- наявність великої кількості рівнів вимагає більшої обчислювальної потужності і, як наслідок, призводить до зменшення швидкодії.

Стек протоколів TCP/IP

Стек TCP/IP, який також часто називається стеком Інтернет, сьогодні є найбільш популярним і таким, що швидко розвивається (табл. 2.6.2).

Цей стек був розроблений з ініціативи Міністерства оборони США й орієнтувався на забезпечення зв’язку різнорідних обчислювальних мереж.

Оскільки стек протоколів TCP/IP був розроблений до появи мережевої моделі ISO/OSI, то відповідність його рівнів рівням моделі OSI носить досить умовний характер, хоча він також має багаторівневу структуру.

Таблиця 2.6.2

Стек протоколів TCP/IP

Рівні моделі OSI	Протоколи TCP/IP	Рівні TCP/IP
7	HTTP, FTP, TFTP, Telnet, SSH, SMTP, SNMP та інші	1
6		
5	TCP, UDP	2
4		
3	IP, ICMP, IGMP	3
2	Не регламентовано, але підтримуються всі популярні стандарти	4
1		

Стек був реалізований для роботи в операційній системі Unix, популярність якої привела до широкого поширення протоколів TCP/IP, завдяки яким стек і одержав свою назву.

Найнижчий рівень стека – рівень інтерфейсу з мережею, відповідає фізичному й канальному рівням моделі OSI. У стеку TCP/IP цей рівень не регламентований, але реалізована підтримка практично всіх популярних стандартів фізичного й канального рівня: Ethernet, Token Ring, FDDI (для локальних мереж), X.25, ISDN, SLIP/PPP (для глобальних мереж).

Рівень міжмережевої взаємодії (рівень 3) забезпечує маршрутизацію й передачу даних мережею, виконуючи, таким чином, функції, відповідні до мережевого рівня моделі OSI. На цьому рівні використовуються протоколи IP, ICMP, IGMP.

IP (Internet Protocol) – міжмережевий протокол, який забезпечує передачу даних у мережах. Протокол IP специфікований в RFC 791. До його основних функцій належать адресація та фрагментація пакетів. Протокол не гарантує надійну доставку даних, не має механізму підтверджень доставки повідомлень, не виконує контроль помилок для поля даних, не підтримує повторну передачу та не виконує функцію управління потоком (flow control). Виявлені помилки можуть бути оголошені за допомогою протоколу ICMP, який підтримується модулем IP протоколу.

ICMP (Internet Control Message Protocol) – протокол міжмережевих керуючих повідомлень, призначений для організації зворотного зв'язку з окремими вузлами мережі при обміні інформацією про помилки, наприклад, про неможливість доставки пакета, про перевищення часу життя або тривалості складання пакета із фрагментів, про

ненормальні значення параметрів. Крім того, за допомогою цього протоколу передаються пакети, які використовуються для тестування, і пакети, які містять службові інформаційні повідомлення, наприклад, про зміну маршруту пересилання й типу обслуговування, про стан системи тощо. Протокол ICMP не робить протокол IP засобом надійної доставки повідомлень. Для цих цілей існує TCP.

IGMP (Internet Group Management Protocol) – протокол, що використовується IP-вузлами і маршрутизаторами для того, щоб підтримувати групову розсилку повідомлень. Він дозволяє всім системам фізичної мережі знати, які IP-вузли в даний час об'єднані в групи і до яких груп вони належать. Ця інформація необхідна для групових маршрутизаторів, саме так вони дізнаються, які групові дейтаграми необхідно перенаправляти і на які інтерфейси. IGMP визначений в RFC 1112.

Рівень 2 стека TCP/IP називається основним і забезпечує функції транспортування інформації з мережі. При цьому використовуються два протоколи TCP і UDP, що реалізують різні механізми доставки даних та мають різні ступені надійності.

TCP (Transmission Control Protocol) – протокол керування передачею, що працює з установкою логічного з'єднання між віддаленими прикладними процесами, а також використовує принцип автоматичної повторної передачі пакетів, які містять помилки. TCP визначений в RFC 793.

UDP (User Datagram Protocol) – протокол користувальницьких дейтаграм (синонім терміна "пакет"), який є спрощеним варіантом TCP і працює без встановлення логічного з'єднання, відповідно, не забезпечує перевірку на наявність помилок і підтвердження доставки пакета. UDP визначений в RFC 768.

Верхній рівень стеку TCP/IP називається прикладним. До протоколів цього рівня належать такі широко використовувані протоколи, як HTTP, FTP, telnet, SMTP, SNMP і багато інших.

HTTP (HyperText Transfer Protocol) – протокол передачі гіпертексту. Основою HTTP є технологія "клієнт-сервер", тобто клієнти ініціюють з'єднання і посилають запит, а сервери очікують з'єднання для отримання запиту, роблять необхідні дії і повертають назад повідомлення з результатом. HTTP насьогодні використовується у Всесвітній павутині для отримання інформації з веб-сайтів.

FTP (File Transfer Protocol) – протокол передачі файлів, який використовує як транспортний протокол із встановленням з'єднань – TCP, що підвищує надійність передачі файлів. Протокол, призначений для забезпечення передачі та прийому файлів між серверами та клієнтами.

TFTP (Trivial File Transfer Protocol) – найпростіший протокол передачі файлів. На відміну від FTP, цей протокол базується на роботі з UDP, при цьому протокол реалізує тільки передачу файлів.

SNMP (Simple Network Management Protocol) – простий протокол керування мережею, призначений для передачі інформації, що визначає формати повідомлень, якими обмінюються клієнти й сервери, а також формати імен і адрес вузлів мережі.

Telnet – протокол, що забезпечує передачу потоку байтів між процесами або між процесом і терміналом, який зазвичай використовується для емуляції терміналу віддаленої станції.

SSH (Secure Shell Protocol) є аналогом протоколу Telnet, але при цьому здійснюється шифрування даних для передачі.

SMTP (Simple Mail Transfer Protocol) – простий протокол передачі пошти, який використовується для забезпечення передачі електронних поштових повідомлень із застосуванням транспортного протоколу TCP.

Стек протоколів *IPX/SPX*

Цей стек є оригінальним стеком протоколів фірми Novell, розробленим для мережевої операційної системи NetWare ще на початку 80-х років. Протоколи Internetwork Packet Exchange (IPX) і Sequenced Packet Exchange (SPX), які й дали назву стека, є прямою адаптацією протоколів XNS фірми Xerox, поширених набагато менше, ніж стек IPX/SPX. Популярність стека IPX/SPX безпосередньо пов'язана з операційною системою (ОС) Novell NetWare.

Даний стек орієнтувався на роботу в локальних мережах невеликих розмірів, які мають невеликі обчислювальні потужності, тому протоколи IPX/SPX мають свої особливості (табл. 2.6.3).

Таблиця 2.6.3

Стек протоколу IPX/SPX

Рівні моделі OSI	Протоколи IPX/SPX
7	NCP, SAP
6	
5	
4	SPX
3	IPX, RIP, NLSP
2	Підтримуються всі популярні стандарти
1	

На рівні, який відповідає фізичному й канальному рівням моделі OSI, стек IPX/SPX підтримує всі популярні протоколи цих рівнів.

Наступний рівень, який виконує функції мережевого рівня моделі OSI, реалізований протоколами IPX, RIP і NLSP.

IPX (Internetwork packet exchange) – міжмережевий обмін пакетами – протокол, що регламентує обмін даними мережею і працює за дейтаграмним принципом, тобто без встановлення попереднього логічного з'єднання, що забезпечує більш економне споживання обчислювальних ресурсів.

RIP (Routing Information Protocol) – протокол маршрутної інформації, являє собою один з найстаріших протоколів, які реалізують процеси обміну маршрутною інформацією, однак він і дотепер надзвичайно розповсюджений в обчислювальних мережах.

NLSP (Netware Link Servies Protocol) – протокол керування зв'язками NetWare – протокол, розроблений під операційні системи NetWare, який забезпечує передачу даних і дозволяє вибирати оптимальні маршрути в мережі.

На рівні, який відповідає транспортному, використовується протокол SPX, що дав частину назви стека, де він і використовується.

SPX (Sequenced Packet exchange) – упорядкований обмін пакетами – комунікаційний протокол, розроблений для використання в мережах NetWare. SPX працює з встановленням логічного з'єднання й забезпечує гарантовану доставку й порядок повідомлень у потоці пакетів, для посилання яких використовує протокол IPX.

На верхніх рівнях використовуються протоколи NCP і SAP.

NCP (Netware Core Protocol) – основний протокол для передачі інформації між сервером NetWare і робочою станцією. За допомогою функцій цього протоколу робоча станція підключається до сервера, має можливість переглянути файлову систему сервера, копіює віддалені файли, здійснює розподіл мережевого принтера між робочими станціями тощо.

SAP (Service Advertising Protocol) – протокол оголошення про сервіс, за принципом дії подібний протоколу RIP. Аналогічно з тим, як різні вузли мережі обмінюються маршрутною інформацією за допомогою протоколу RIP, мережеве обладнання одержує можливість обмінюватися інформацією про наявні мережеві сервіси, використовуючи протокол SAP.

На сьогоднішній день стек IPX/SPX реалізований не тільки в NetWare, але й у декількох інших популярних мережевих ОС, наприклад Microsoft Windows. Починаючи з версії 5.0, фірма Novell як

основний протокол своєї серверної операційної системи стала використовувати протокол TCP/IP, і з того часу практичне застосування IPX/SPX стало неухильно знижуватися.

Стек протоколів *NetBIOS/SMB*

Стек NetBIOS/SMB – спільний проект компаній Microsoft та IBM, розроблений у 1984 р. (табл. 2.6.4).

Стек працює з усіма найбільш розповсюдженими протоколами нижнього рівня.

На верхніх рівнях працюють протоколи NetBEUI та SMB.

Протокол NetBIOS (Network Basic Input/Output System) став розширенням стандартних функцій базової системи введення/виведення (BIOS – Base Input/Output System), який забезпечує підтримку роботи в мережі. У подальшому NetBIOS був замінений протоколом NetBEUI. При цьому NetBIOS все ж був збережений для забезпечення сумісності додатків.

Таблиця 2.6.4

Стек протоколів NetBIOS/SMB

Рівні моделі OSI	Протоколи NetBIOS/SMB
7	SMB
6	
5	NetBIOS, NetBEUI
4	
3	
2	Підтримуються всі популярні стандарти
1	

NetBEUI (NetBIOS Extended User Interface) – протокол розширеного користувальницького інтерфейсу NetBIOS, який надає функції, що відносяться до сеансового, транспортного і частково до мережевого рівнів моделі OSI. NetBIOS підтримує як дейтаграмний спосіб обміну даними, так і обмін із установленням логічних з'єднань. Однак цей протокол не забезпечує маршрутизацію пакетів, тому його застосування обмежується тільки невеликими локальними мережами. Для вирішення цієї проблеми використовується NBF (NetBEUI Frame) – реалізація цього протоколу, який вперше з'явився в операційній системи Microsoft Windows NT. Проте в складних мережах використовують більш універсальні протоколи стеків TCP/IP та IPX/SPX.

SMB (Server Message Block) – протокол, який виконує функції прикладного рівня і рівня представлення моделі OSI, визначає взаємодію робочої станції та сервера. SMB надає основні мережеві сервіси, необхідні додаткам: керування сесіями передачі даних, встановлення та ліквідацію логічного з'єднання, доступ для роботи з файлами, друк по мережі, передачу повідомлень тощо.

Інші стеки протоколів

Такі стеки, як AppleTalk компанії Apple, SNA фірми IBM або стек DECnet корпорації Digital Equipment, одержали менше поширення, тому що застосовуються в основному в операційних системах і мережевому обладнанні, вироблених перерахованими фірмами, і, відповідно, орієнтованих на використання системних архітектур і апаратних платформ цих же фірм.

Будь-який протокол за тими або іншими умовами може відповідати деякому рівню моделі OSI. Однак з огляду на те, що розробники не суворо дотримуються моделі OSI і багато протоколів і стеків з'явилося до розробки еталонної моделі, найчастіше протоколи можуть відноситися відразу до декількох рівнів, або навпаки, виконувати тільки частину функцій одного з рівнів. Усе це приводить до того, що для того щоб забезпечити успішну роботу протоколів і реалізувати закінчений набір функцій, що забезпечують обмін даними мережею, доводиться використовувати протоколи з одного стека. Це приводить до несумісності зі стандартною моделлю відкритих систем.

Розбіжності і особливості поширених протоколів

Протоколи, що використовуються для обміну даними в локальних мережах, поділяються за своєю функціональністю на три типи:

- прикладні;
- транспортні;
- мережеві.

Прикладні протоколи виконують функції трьох верхніх рівнів моделі OSI – прикладного, рівня представлення і сеансового. Вони забезпечують взаємодію додатків і обмін даними між ними. До найбільш популярних прикладних протоколів належать:

- *FTAM (File Transfer Access and Management)* – протокол OSI доступу до файлів;
- *X.400* – протокол OSI для міжнародного обміну електронною поштою;
- *X.500* – протокол OSI служб файлів і каталогів на декількох системах;
- *SMTP (Simple Mail Transfer Protocol)* – протокол Інтернету для обміну електронною поштою;

- *FTP (File Transfer Protocol)* – протокол Інтернету для передачі файлів;
- *Telnet* – протокол Інтернету для реєстрації на віддалених серверах і обробки даних на них;
- *SMB (Server Message Blocks)* – протокол взаємодії робочої станції і сервера фірми Microsoft;
- *NCP (NetWare Core Protocol)* – протокол передачі даних між сервером NetWare і робочою станцією фірми Novell;
- *Apple Talk и Apple Share* – набір мережевих протоколів фірми Apple;
- *AFP (AppIeTalk Filling Protocol)* – протокол віддаленого доступу до файлів фірми Apple;
- *DAP (Data Access Protocol)* – протокол доступу до файлів мереж DECnet.

Транспортні протоколи реалізують функції транспортного і сеансового рівня моделі OSI. Вони ініціюють і підтримують сеанси зв'язку між вузлами мережі і забезпечують необхідний користувачам рівень надійності передачі даних. Найпопулярніші серед них наступні:

- *TCP (Transmission Control Protocol)* – протокол Інтернету для гарантованої доставки даних, розбитих на послідовність фрагментів;
- *SPX (Sequential Packet Exchange)* – протокол стека IPX/SPX для передачі даних, розбитих на послідовність фрагментів, фірми Novell;
- *NetBIOS (Network Basic Input/Output System)* – протокол встановлення і контролю сеансів зв'язку між комп'ютерами;
- *ATP (AppIeTalk Transaction Protocol), NBP (Name Binding Protocol)* – протоколи сеансів зв'язку і транспортування даних фірми Apple.

Мережеві протоколи виконують функції трьох нижніх рівнів моделі OSI – мережевого, канального й фізичного. Ці протоколи управляють адресацією, маршрутизацією, перевіркою помилок і повторною передачею кадрів, забезпечуючи послуги зв'язку, і визначають правила здійснення зв'язку в окремих середовищах передачі даних, наприклад, Ethernet або Token Ring. До найпопулярніших мережевих протоколів належать:

- *IP (Internet Protocol)* – протокол Інтернету для передачі пакетів;
- *IPX (Internetwork Packet Exchange)* – протокол для передачі і маршрутизації пакетів фірми Novell;
- *NetBEUI* – транспортний протокол, що забезпечує послуги транспортування даних для сеансів і додатків NetBIOS фірми Microsoft;
- *DDP (Datagram Delivery Protocol)* – AppleTalk-протокол транспортування даних фірми Apple.

Крім особливостей, обумовлених виконуваними функціями, відмінності і особливості протоколів характеризуються їхньою орієнтаці-

єю на роботу в різних операційних системах і з різними апаратними платформами.

У ході обміну даними мережею протоколи різних рівнів тісно взаємодіють один з одним. Протоколи більш високих рівнів використовують можливості й сервіси протоколів нижніх рівнів.

Додатки обмінюються інформацією за допомогою засобів, що надаються прикладними протоколами, які, у свою чергу, забезпечують передачу даних за рахунок використання відповідних транспортних протоколів.

Транспортні протоколи здійснюють передачу даних, використовуючи послуги мережевих протоколів, відповідальних за керування адресацією, маршрутизацію в мережах, забезпечення надійності передачі даних тощо.

Контрольні питання

1. Що таке стек протоколів?
2. Які різновиди стеків протоколів Вам відомі?
3. Які протоколи входять до стека протоколів моделі OSI?
4. Які протоколи входять до стека протоколів TCP/IP?
5. Які протоколи входять до стека протоколів IPX/SPX?
6. Які протоколи входять до стека протоколів NetBIOS/SMB?
7. Чи підтримує стек TCP/IP протокол UDP?
8. Яке призначення протоколу TCP?

ЛІТЕРАТУРА: [2, 9, 23,25, 26, 36, 41, 46, 47, 48, 53, 55, 56].

Тема 7. АДРЕСАЦІЯ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Мета теми – ознайомитися із принципами адресації в комп'ютерних мережах; розглянути класи мережевих адрес; ознайомитися із доменною системою імен.

Ключові поняття: адресація в комп'ютерних мережах; класи мережевих адрес; протокол ARP; протокол DHCP; доменна система імен.

Загальні принципи адресації у комп'ютерних мережах

При об'єднанні в мережу трьох і більш вузлів виникає проблема ідентифікації конкретного вузла, якому призначені дані, що пересилаються. Інакше кажучи, виникає проблема адресації вузлів комп'ютерної мережі.

Адресація є однією з ключових функцій протоколів мережевого рівня, які забезпечують обмін даними між хостами в тій же мережі або в різних мережах.

Термін “хост” (від англ. host) використовують як синонім терміна “вузол мережі”, зазвичай говорячи про мережі, об’єднані на основі використання стека TCP/IP.

Проектування і впровадження ефективного плану адресного простору гарантує, що мережі будуть працювати ефективно і раціонально.

На практиці адресація проводиться не для самих вузлів мережі, а для їхніх мережевих інтерфейсів, тобто наборів засобів і правил, які дозволяють здійснювати обмін інформацією. Це пояснюється тим, що один вузол мережі може мати кілька мережевих інтерфейсів, наприклад, у мережі, яка має фізичну топологію “кільце”, кожному вузлу необхідно мінімум два мережеві інтерфейси, що зв’язують його з його сусідами.

Існує безліч систем адресації і, відповідно, безліч форматів представлення адрес.

До адреси вузла мережі і схеми його призначення можна пред’явити декілька вимог:

- адреса повинна унікально ідентифікувати комп’ютер в мережі будь-якого масштабу;
- схема призначення адрес повинна зводити до мінімуму ручну працю адміністратора і ймовірність дублювання адрес;
- адреси повинні мати ієрархічну структуру, зручну для побудови великих мереж. Цю проблему добре ілюструють міжнародні поштові адреси, які дозволяють поштовій службі, що організує доставку листів між країнами, користуватися тільки назвою країни адресата і не враховувати назву міста, а тим більше вулиці. У великих мережах, які складаються з багатьох тисяч вузлів, відсутність ієрархії адреси може привести до великих витрат – кінцевим вузлам і комунікаційному обладнанню доведеться оперувати з таблицями адрес, що складаються з тисяч записів;
- адреса повинна бути зручною для користувачів мережі, а це значить, що вона повинна мати символьне подання, наприклад Servers або www.microsoft.com;
- адреса повинна мати при можливості компактне подання, щоб не перевантажувати пам’ять комунікаційної апаратури – мережевих адаптерів, маршрутизаторів тощо.

Неважко помітити, що ці вимоги суперечливі. Наприклад, адреса, яка має ієрархічну структуру, швидше за все буде менш компактною, ніж неієрархічна (таку адресу часто називають “плоскою”, тобто вона не має структури). Символьна ж адреса швидше за все буде займати більше пам’яті, ніж числова адреса.

Оскільки всі перераховані вимоги важко поєднати в рамках якої-небудь однієї схеми адресації, то на практиці зазвичай використовується одразу декілька схем, тому комп'ютер одночасно має декілька адрес-імен. Кожна адреса використовується в тій ситуації, коли відповідний вид адресації найбільш зручний. А щоб не виникало плутанини і комп'ютер завжди однозначно визначався своєю адресою, використовуються спеціальні допоміжні протоколи, які за адресою одного типу можуть визначити адреси інших типів.

Найбільше поширення отримали три схеми адресації вузлів:

1. *Апаратні (hardware) адреси*. Ці адреси призначені для мережі невеликого або середнього розміру, тому вони не мають ієрархічної структури. Типовим представником адреси такого типу є адреса мережевого адаптера локальної мережі (MAC-адреса). Така адреса зазвичай використовується тільки апаратурою, тому її намагаються зробити за можливістю компактною і записують у вигляді двійкового або шістнадцяткового значення, наприклад, 00-11-D8-5E-E6-59. При заданні апаратних адрес зазвичай не потребується виконання ручної роботи, тому що вони вбудовуються в апаратуру компанією-виробником, але за потребою мережевий адміністратор їх може змінювати. Крім відсутності ієрархії, використання апаратних адрес пов'язано ще з одним недоліком – при заміні апаратури, наприклад, мережевого адаптера, змінюється і адреса комп'ютера. Більш того, при встановленні декількох мережевих адаптерів у комп'ютера з'являється кілька адрес, що не дуже зручно для користувачів мережі.

2. Символьні адреси або імена. Ці адреси призначені для запам'ятовування людьми і тому зазвичай несуть смислове навантаження. Символьні адреси легко використовувати як в невеликих, так і великих мережах. Для роботи у великих мережах символьне ім'я може мати складну ієрархічну структуру, наприклад ftp-archl.ucl.ac.uk. Ця адреса говорить про те, що цей комп'ютер підтримує ftp-архів в мережі одного з коледжів Лондонського університету (University College London – ucl) і ця мережа належить до академічної галузі (ac) Internet Великобританії (United Kingdom – uk). При роботі в межах мережі Лондонського університету таке довге символьне ім'я явно надмірне і замість нього зручніше користуватися коротким символьним ім'ям, на роль якого добре підходить наймолодша складова повного імені, тобто ім'я ftp-archl.

3. Числові складені адреси. Символьні імена зручні для людей, але через змінний формат і потенційно велику довжину їх передача по мережі не дуже економічна. Тому в багатьох випадках для роботи у великих мережах як адреси вузлів використовують числові складені

адреси фіксованого і компактного форматів. Типовими представниками адрес цього типу є IP- та IPX-адреси. У них підтримується дворівнева ієрархія, адреса поділяється на старшу частину – номер мережі і молодшу – номер вузла. Такий розподіл дозволяє передавати повідомлення між мережами тільки на підставі номера мережі, а номер вузла використовується тільки після доставки повідомлення в потрібну мережу; так само, як назва вулиці використовується листоношею тільки після того, як лист доставлено в потрібне місто. Останнім часом, щоб зробити маршрутизацію у великих мережах ефективнішою, пропонуються більш складні варіанти числової адресації, відповідно до яких адреса має три і більше складових. Такий підхід, зокрема, реалізований у новій версії протоколу IPv6, призначеного для роботи в мережі Internet.

У сучасних мережах для адресації вузлів застосовуються, як правило, одночасно всі три наведені вище схеми. Користувачі адресують комп'ютери символьними іменами, які автоматично замінюються у повідомленнях, що передаються по мережі, на числові адреси. За допомогою цих числових адрес повідомлення передаються з однієї мережі в іншу, а після доставки повідомлення в мережу призначення замість числової адреси використовується апаратна адреса комп'ютера. Сьогодні така схема характерна навіть для невеликих автономних мереж, де, здавалося б, вона явно надлишкова – це робиться для того, щоб при включенні цієї мережі у велику мережу не потрібно було змінювати склад операційної системи.

У сучасних операційних системах найчастіше використовується набір протоколів TCP/IP. На жаль, одного тільки встановлення протоколу TCP/IP для роботи комп'ютера в мережі буде недостатньо. Стек не запрацює, поки в мережі не буде правильним чином налаштована IP-адресація і маршрутизація. (Порівняємо роботу мережі з роботою пошти: як зможе листоноша доставити повідомлення адресату, якщо дороги та транспорт хоча й працюють, але на будинках немає номерів, а поштові відділення не знають, як пересилати листи з одного міста до іншого?). Тому більш детально розглянемо IP-адресацію в мережі.

Основи IP-адресації

Першим обов'язковим параметром у властивостях протоколу TCP/IP будь-якого комп'ютера є наявність його IP-адреси.

IP-адреса – це унікальна 32-розрядна послідовність двійкових цифр, за допомогою якої комп'ютер однозначно ідентифікується в IP-мережі. (Нагадаємо, що на канальному рівні в ролі таких же унікальних адрес комп'ютерів виступають MAC-адреси мережевих адаптерів,

неможливість збігу яких контролюється виробниками на стадії виробництва.)

Ми будемо обговорювати найпоширенішу на сьогодні четверту версію протоколу IP – IPv4. Проте вже створена наступна версія протоколу – IP версії 6 (IPv6), у якій IP-адреса представляється у вигляді 128-бітної послідовності двійкових цифр. Ця версія протоколу IP поки що не отримала широкого розповсюдження, хоча і підтримується багатьма сучасними маршрутизаторами та операційними системами.

Багато країн, які активно розвиваються у технічному відношенні (Китай, Японія, Корея та ін.) починають відчувати дефіцит IP-адрес, що ідентифікують не тільки комп'ютери, але й інші пристрої з функціями доступу в Інтернет. Прийнятий зараз 32-бітовий стандарт забезпечує кількість IP-адрес, яка дорівнює майже 4,3 млрд, але їх більша частина закріплена за США (близько 70 %), Канадою та європейськими країнами, а от, наприклад, КНР отримала їх всього 22 млн., що для них є недостатнім. Нова, 128-розрядна версія протоколу IPv6, дозволить збільшити кількість IP-адрес до значної кількості.

Для зручності роботи з IP-адресами 32-розрядну послідовність зазвичай поділяють на 4 частини по 8 бітів (на октети), кожен октет переводять у десяткове число і при записі поділяють ці числа крапками. У такому вигляді (це подання називається "десяткові числа з крапками", або, англійською, "dotted-decimal notation") IP-адреси займають набагато менше місця і набагато легше запам'ятовуються (табл. 2.7.1).

Таблиця 2.7.1

Різні представлення IP-адреси

IP-адреса у 32-розрядному вигляді	11000000 10101000 00000101 11001000			
IP-адреса, розбита на октети	11000000	10101000	00000101	11001000
Октети у десятковому вигляді	192	168	5	200
IP-адреса у вигляді десяткових чисел, розділених крапками	192.168.5.200			

Проте однієї тільки IP-адреси комп'ютеру для роботи в мережі TCP/IP недостатньо. Другим обов'язковим параметром, без якого протокол TCP/IP працювати не буде, є наявність маски підмережі.

Маска підмережі – це 32-розрядне число, яке складається з одиниць, які йдуть спочатку, та з нулів, які йдуть наприкінці, наприклад (в десятковому поданні) 255.255.255.0 або 255.255.240.0.

Маска підмережі відіграє винятково важливу роль в IP-адресації і маршрутизації. Мережа може бути неоднорідною (гетерогенною), тобто складатися з фрагментів різної топології та різнотипних технічних засобів. Для правильної взаємодії в такій мережі кожен учасник повинен вміти визначати, які IP-адреси належать його локальній мережі, а які – є віддаленими мережами.

Тут і використовується маска підмережі, за допомогою якої здійснюється поділ будь-якої IP-адреси на дві частини: *ідентифікатор мережі* (Net ID) та *ідентифікатор вузла* (Host ID). Такий поділ виконується дуже просто: там, де в масці підмережі стоять одиниці, знаходиться ідентифікатор мережі, а де стоять нулі – ідентифікатор вузла.

Наприклад, у IP-адресі 192.168.5.200 при використанні маски підмережі 255.255.255.0 ідентифікатором мережі буде число 192.168.5.0, а ідентифікатором вузла – число 200. Варто нам змінити маску підмережі, скажімо, на число 255.255.0.0, як і ідентифікатор вузла, і ідентифікатор мережі зміняться на 192.168.0.0 і 5.200, відповідно, і в залежності від цього інакше буде вести себе комп'ютер під час відправлення IP-пакетів.

Правила призначення IP-адрес мереж і вузлів

Тепер, коли ми знаємо, що таке IP-адреса, маска підмережі, ідентифікатори мережі і вузла, корисно запам'ятати правила, які слід застосовувати при призначенні цих параметрів:

1. Ідентифікатор мережі не може містити тільки двійкові нулі або тільки одиниці. Наприклад, адреса 0.0.0.0 не може бути ідентифікатором мережі.
2. Ідентифікатор вузла також не може містити тільки двійкові нулі або тільки одиниці – такі адреси зарезервовані для спеціальних цілей:
   - усі нулі в ідентифікаторі вузла означають, що ця адреса є адресою мережі. Наприклад, 192.168.5.0 є правильною адресою мережі при використанні маски 255.255.255.0 і її не можна використовувати для адресації комп'ютерів;
   - усі одиниці в ідентифікаторі вузла означають, що ця адреса є широкомовною адресою для даної мережі. Наприклад, 192.168.5.255 є адресою широкомовлення в мережі 192.168.5.0 при використанні маски 255.255.255.0 і її не можна використовувати для адресації комп'ютерів.

3. Ідентифікатор вузла в межах однієї і тієї ж підмережі повинен бути унікальним.
4. Діапазон адрес від 127.0.0.1 до 127.255.255.254 не можна використовувати як IP-адреси комп'ютерів. Уся мережа 127.0.0.0 з маскою 255.0.0.0 зарезервована під так звані "адреси заглушки" (loopback), що використовуються IP для звернення комп'ютера до самого себе.

Класова і безкласова IP-адресація

Первинна система IP-адресації в Інтернеті була наступна. Весь простір можливих IP-адрес (а це більше чотирьох мільярдів, точніше 4294967296 адрес) було розбито на п'ять *класів*, причому належність IP-адреси до певного класу визначалася бітами першого октету (табл. 2.7.2). Зауважимо, що для адресації мереж і вузлів використовувалися тільки класи A, B та C. Крім того, для цих мереж були визначені *фіксовані маски підмережі за замовчуванням*, рівні, відповідно, 255.0.0.0, 255.255.0.0 і 255.255.255.0, які не тільки жорстко визначали діапазон можливих IP-адрес вузлів у таких мережах, але й механізм маршрутизації.

Таблиця 2.7.2

Класи адрес в первинній схемі IP-адресації

Клас	Перші біти в октеті	Можливі значення першого октету	Можлива кількість мереж	Можлива кількість вузлів у мережі
A	0	1-126	126	16777214
B	10	128-191	16384	65534
C	110	192-223	2097152	254
D	1110	224-239	Використовується для багатоадресного розсилання (multicast)	
E	1111	240-254	Зарезервований як експериментальний	

Адреси класу A призначені для використання у великих мережах масштабу регіону або країни, число таких мереж досить обмежене. Мережі класу B мають середні розміри та зазвичай використовуються в університетах і великих компаніях. Адреси класу C використовуються в малих мережах, які мають невелику кількість вузлів. IP-адреси класу D використовують для звертання до груп комп'ютерів. Адреси класу E зарезервовані для майбутнього використання.

Щоб розрахувати максимально можливу кількість вузлів у будь-якій IP-мережі, досить знати, скільки бітів міститься в ідентифікаторі

вузла, або, інакше, скільки нулів є у масці підмережі. Це число використовується як показник ступеня двійки, а потім від результату віднімаються дві зарезервовані адреси (мережі і широкомовлення). Аналогічним способом легко обчислити і можливу кількість мереж класів A, B або C, якщо врахувати, що перші біти в октеті вже зарезервовані, а в класі A не можна використовувати IP-адреси 0.0.0.0 і 127.0.0.0 для адресації мережі.

Для отримання потрібного діапазону IP-адрес організаціям пропонувалося заповнити реєстраційну форму, у якій слід вказати поточне число комп'ютерів і плановане зростання комп'ютерного парку протягом двох років.

Спочатку дана схема добре працювала, оскільки кількість мереж була невеликою. Однак з розвитком Інтернету такий підхід до розподілу IP-адрес став викликати проблеми, особливо гострі виникли для мереж класу B. Дійсно, організаціям, у яких число комп'ютерів не перевищувало кількох сотень (скажімо, 500), доводилося реєструвати для себе цілу мережу класу B. Тому кількість доступних мереж класу B стала на очах "танути", але при цьому величезні діапазони IP-адрес (у нашому прикладі – понад 65000) не використовувалися.

Щоб вирішити цю проблему, була розроблена *безкласова схема IP-адресації (Classless InterDomain Routing – CIDR)*, у якій не лише відсутня прив'язка IP-адреси до класу мережі і до маски підмережі за замовчуванням, але й допускається застосування так званих *масок підмережі зі змінною довжиною (Variable Length Subnet Mask – VLSM)*. Наприклад, якщо при виділенні мережі для вищевказаної організації з 500 комп'ютерами замість фіксованої маски 255.255.0.0 використовувати маску 255.255.254.0, то вийде діапазон з 512 можливих IP-адрес, чого буде цілком достатньо. 65000 адрес, які залишилися невикористаними, можна зарезервувати на майбутнє або роздати іншим бажаючим підключитися до Інтернету.

Цей підхід дозволив набагато ефективніше виділяти організаціям потрібні їм діапазони IP-адрес, і проблема з нестачею IP-мереж і адрес стала менш гострою.

IP-адреси для локальних мереж

Розподілом IP-адрес у світі займається приватна некомерційна корпорація ICANN (Internet Corporation for Assigned Names and Numbers), а точніше організація IANA (Internet Assigned Numbers Authority), яка працює під її патронажем.

Усі використовувані в Інтернеті адреси повинні реєструватися в IANA, яка гарантує їх унікальність у масштабі всієї планети. Такі адреси називають *реальними*, або *публічними (public) IP-адресами*.

Для локальних мереж, не підключених до Інтернету, реєстрація IP-адрес не потрібна, тому, в принципі, тут можна використовувати будь-які можливі адреси. Однак, щоб не допускати можливих конфліктів при подальшому підключенні таких мереж до Інтернету, RFC 1918 рекомендує застосовувати в локальних мережах тільки наступні діапазони так званих *приватних (private) IP-адрес* (в Інтернеті ці адреси не існують і використовувати їх там немає можливості):

- 10.0.0.0-10.255.255.255;
- 172.16.0.0-172.31.255.255;
- 192.168.0.0-192.168.255.255.

Призначення IP-адрес

Найпростіший спосіб встановлення параметрів протоколу IP – призначити їх вручну. Перевагою такого методу є те, що мережеві адміністратори повністю контролюють усі IP-адреси комп'ютерів у мережі, що може бути важливим з погляду захисту даних або взаємодії з Інтернетом. Однак у цього способу багато недоліків. По-перше, легко помилитися і ввести неправильні параметри маски або шлюзу, або, що ще гірше, призначити IP-адресу, яка повторюється в мережі. По-друге, при змінах параметрів IP-адресації у мережі (наприклад, при зміні IP-адреси маршрутизатора) доведеться переналаштовувати всі комп'ютери. Але найнеприємніше, що при такому способі налаштування практично неможливо працювати у великих корпоративних мережах з мобільними пристроями, наприклад, ноутбуками або КПК, які часто переміщуються з одного сегмента мережі в інший.

Тому в організаціях частіше застосовують спеціальні сервери, що підтримують *протокол динамічної конфігурації вузлів (Dynamic Host Configuration Protocol – DHCP)*, задача яких полягає в обслуговуванні запитів клієнтів на отримання IP-адреси та іншої інформації, необхідної для належного функціонування в мережі. Саме тому комп'ютери з операційними системами Windows за замовчуванням налаштовані на автоматичне отримання IP-адреси.

Якщо сервер DHCP недоступний (відсутній або не працює), то починаючи з версії Windows 98, комп'ютери самостійно призначають собі IP-адресу. При цьому використовується *механізм автоматичної особистої IP-адресації (Automatic Private IP Addressing – APIPA)*, для якого корпорацією Microsoft в IANA був зареєстрований діапазон адрес 169.254.0.0-169.254.255.255.

Планування адресації мережі

Розподіл адрес мережевого рівня усередині корпоративної мережі повинен бути добре продуманим. Мережеві адміністратори використовують у своїх мережах адреси не випадковим чином. Адреси в мережі не повинні бути випадковими.

Розподіл мережевих адрес всередині мережі повинен плануватися і документуватися з метою:

- запобігання дублюванню адрес;
- забезпечення і контроль доступу;
- моніторинг забезпечення безпеки і продуктивності.

Запобігання дублюванню адрес

Кожен хост в мережі повинен мати унікальну адресу. Без належного планування та документації призначення мережевих адрес можна легко призначати однакові адреси більш ніж одному хосту.

Забезпечення і контроль доступу

Деякі хости надають ресурси внутрішній мережі, а також зовнішній мережі. Одним з прикладів таких пристроїв є сервери. Доступ до цих ресурсів може контролюватися через адреси мережевого рівня. Якщо адреси цих ресурсів не плануються і не задокументовані, безпеку і доступність пристроїв важко контролювати. Наприклад, якщо мережевим адміністратором налаштовано, що користувачі можуть мати доступ тільки до адрес визначеного діапазону, а сервер має адресу, присвоєну випадково, то доступ до нього користувачів може бути заблокований.

Моніторинг безпеки та продуктивності

Крім того, необхідно стежити за безпекою і продуктивністю мережевих хостів та мережі в цілому. Як частина процесу контролю, досліджується мережевий трафік, шукаючи адреси хостів, які створюють або отримують надлишкові пакети. Якщо виконане належне планування та ведеться документація мережевої адресації, то можна ідентифікувати пристрій у мережі, на який або з якого надходить надлишковий трафік.

Призначення адрес у мережі

У мережі існують різні типи хостів:

- кінцеві пристрої користувачів;
- сервери та периферійні пристрої;
- хости, які доступні з Інтернету;
- проміжні пристрої.

Кожен з цих різних типів пристроїв повинен бути виділений до логічного блоку адрес в межах діапазону адрес у мережі, для того щоб було легше контролювати доступ до них та безпеку. Також можна виділяти в окремі логічні блоки пристрої за географічною ознакою або, наприклад, за професійною ознакою (наприклад, можна виділити в окремий логічний блок пристрої відділу продажів, в окремий – відділу маркетингу тощо).

Також при плануванні схеми IP-адресації обов'язково необхідно вирішити, для яких пристроїв використовувати приватні, а для яких – публічні адреси.

Для цього необхідно розглянути наступні фактори:

- чи буде використовуватися пристроїв, підключених до мережі, більше ніж публічних адрес, виділених провайдером мережі;
- чи необхідно забезпечити зовнішній доступ до пристроїв локальної мережі;
- якщо є пристрої, яким можуть бути присвоєні приватні адреси і яким потрібен доступ до Інтернету, то можна чи ні забезпечити трансляцію мережевих адрес (Network Address Translation – NAT).

Якщо таких пристроїв більше, ніж доступно публічних адрес, тільки ті пристрої, які будуть мати прямий доступ до Інтернету – такі, як веб-сервер –вимагають публічну адресу. Служба NAT дозволяє заощадити IP-адреси, транслюючи декілька приватних IP-адрес в одну зовнішню публічну IP-адресу (або в декілька, але меншої кількості, ніж внутрішні). За таким принципом побудована більшість мереж у світі: на невеликий район домашньої мережі місцевого провайдера або на офіс виділяється одна публічна IP-адреса, за якою працюють і отримують доступ в Інтернет приватні IP-адреси.

Відображення IP-адрес на локальні адреси

Щоб визначити фізичну адресу вузла за мережевою адресою, використовується *протокол дозволу адрес ARP (Address Resolution Protocol)*. У локальних мережах для визначення потрібної адреси ARP використовує розсилання широкомовних запитів. Протокол дозволу адрес формує запит, указуючи в ньому мережеву адресу, для якої потрібно визначити відповідну фізичну адресу вузла, інкапсулює цей запит у кадр протоколу канального рівня, який використовується в даній мережі, і робить широкомовне розсилання отриманого кадру.

Вузол мережі, що одержав такий запит, порівнює зазначену у запиті мережеву адресу зі своєю мережевою адресою. У випадку, якщо адреси співпадають, вузол формує відповідь, що містить обидві адреси вузла – фізичну і мережеву – і відправляє її відправникові ARP-запиту.

Пакети, що містять ARP-запити й ARP-відповіді, мають однаковий формат.

Для рішення зворотного завдання, тобто визначення IP-адреси за відомою фізичною адресою, використовується протокол *зворотного дозволу адрес RARP (Reverse Address Resolution Protocol*). Необхідність використання протоколу зворотного дозволу адрес зазвичай обумовлюється використанням бездискових робочих станцій, завантаження операційної системи яких проводиться з єдиного сервера.

Застосування RARP можливе при наявності в мережі спеціального сервера, який відповідає на RARP-запити, ґрунтуючись на інформації, яка зберігається в його ARP-таблиці та дозволяє провести відповідність фізичних адрес мережевим (табл. 2.7.3).

Таблиця 2.7.3

Приклад ARP-таблиці

IP-адреса	MAC-адреса
101.0.10.3	08:00:F0:00:2F:D1
101.0.10.10	08:00:5A:19:BA:15
101.0.10.17	08:00:11:56:A4:76

У відповідь на запит такий сервер відсилає пакет, що містить обидві адреси запитуючого вузла – мережеву і фізичну.

Відображення доменних імен на IP-адреси

Окрім числових схем адресації, також застосовуються схеми адресації, які використовують символьне представлення адрес. Символьні адреси набагато простіше запам’ятовувати, цьому сприяє ще й той факт, що зазвичай вони несуть деяке змістовне навантаження. Тому такі адреси зручні там, де необхідно забезпечити інтерфейс людини з мережевою програмою.

Однак символьні адреси мають змінний формат досить великої максимально можливої довжини, тому зберігання й передача мережею таких адрес викликають ряд складностей і є не дуже економічними.

У мережі Інтернет використовується IP-адресація, але оскільки користувачам додатків більш зручно працювати із символьними адресами, то на прикладних рівнях використовується символьна система адресації, кожна адреса якої ставиться у відповідність якійсь IP-адресі.

Раніше символьна адресація забезпечувалася засобами операційних систем, що зберігали таблиці відповідності фізичної адреси вузла мережі і його символьної адреси. Однак такі системи розроблялися

для роботи в невеликих локальних мережах. При цьому імена вузлів мали лінійну структуру, тобто не розділялися на кілька частин. Щоб визначити фізичну адресу вузла, що відповідає деякому символьному імені, проводилося опитування всіх вузлів локальної мережі, що здійснювалося за допомогою механізму широкомовних запитів.

Але в більших мережах або в мережах, що поєднують декілька підмереж, більш ефективне застосування ієрархічної системи адресації, і, відповідно, адрес, які складаються із декількох "вкладених" одна в одну частин.

Прикладом такої системи адресації може служити *доменна система імен (Domain Name System – DNS)*, яка застосовується в Інтернеті і має ієрархічну деревоподібну структуру, що і допускає більший ступінь вкладеності, тобто більшу кількість ієрархічних підрівнів.

Доменне ім'я може складатися з декількох частин, відділених один від одного крапками, наприклад, images.yandex.ru. Кожна з таких частин називається доменом.

Під *доменом* можна мати на увазі якусь сукупність комп'ютерів, які мають деякі схожі властивості.

Доменне ім'я записується таким чином: ліворуч знаходиться ім'я вузла, який входить у домен самого низького рівня в ієрархії, а праворуч – домен найвищого ієрархічного рівня (рис. 2.7.1). Тому крайній праворуч домен називається *доменом верхнього* або *першого рівня*. Наступний домен, що ліворуч, відділений крапкою, є дочірнім доменом стосовно домену першого рівня, тобто входить у нього як його складова частина. Цей домен називається *доменом другого рівня*. Домени, які є дочірніми для домену другого рівня, називаються *доменами третього рівня* і т.д.

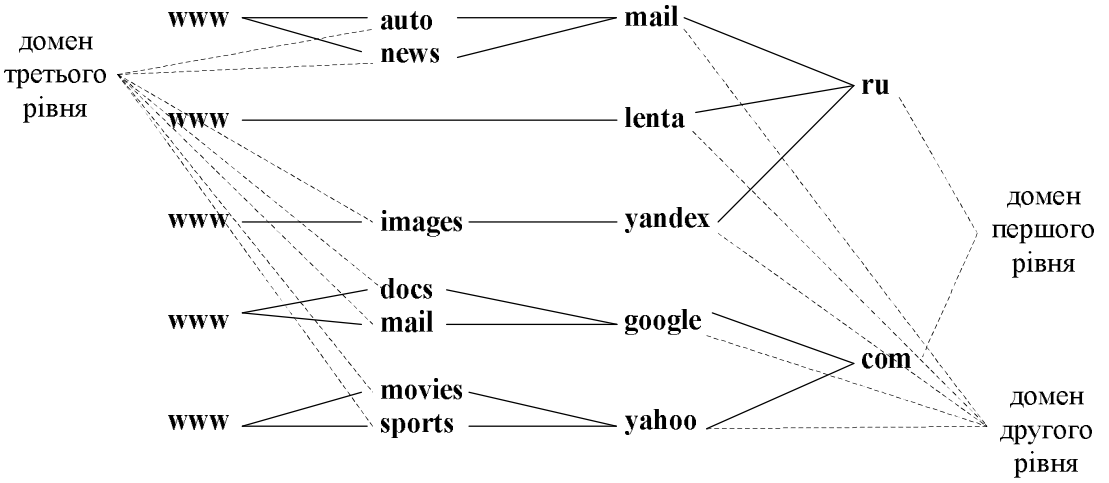


Рис. 2.7.1. Система ієрархії доменів

У адресі images.yandex.ru доменом першого рівня є домен “ru”, доменом другого рівня – “yandex”, слово “images” є ім’ям хоста.

Назви доменів першого рівня призначаються централізовано, відповідно до міжнародного стандарту. Імена доменів першого рівня можуть позначати країни або типи організацій і, як правило, являють собою дво- або трибуквені абревіатури (табл. 2.7.4).

Таблиця 2.7.4

Приклади доменів першого рівня

Домени першого рівня			
	Загальні[1]		**Регіональні[2]**
Ім’я	**Значення**	**Ім’я**	**Значення**
.com	Комерційні	.ru	Російська Федерація
.edu	Освітні	.ua	Україна
.gov	Урядові	.us	США
.int	Міжнародні	.jp	Японія
.mil	Військові	.de	Німеччина
.info	Інформаційні	.fr	Франція
.net	Мережеві	.au	Австралія
.org	Некомерційні	.it	Італія
[1] Призначені для позначення типів організацій. [2] Призначені для позначення країн і регіонів.			

Доменом другого рівня зазвичай є псевдонім організації, якій належить корпоративна мережа або хост-комп’ютер, для адресації яких використовується цей домен.

Домени третього й наступних рівнів є частиною доменів другого рівня, і на практиці зазвичай представляють якісь підмережі або дочірні хости, які продаються або безкоштовно передаються у використання іншим організаціям або фізичним особам. Дуже часто на таких хостах розміщуються домашні сторінки користувачів Інтернету.

Встановлення відповідності доменних імен мережевим адресам здійснюється централізовано за допомогою сервісу DNS.

Сервіс DNS – система забезпечення перетворення символічних імен і псевдонімів локальних мереж і вузлів у мережі Інтернет в IP-адреси, і навпаки.

Принцип роботи сервісу DNS заснований на використанні так званих DNS-серверів. Кожний домен повинен мати свій DNS-сервер, який зберігає таблицю відповідностей доменних імен і IP-адрес даного

домену, а також доменів, які є для нього дочірніми. У таблиці також присутній запис, що належить до батьківського домену. Таким чином, будь-який вузол може одержати відомості про шукану IP-адресу будь-якого вузла мережі. Припустимо, що ми набрали в браузері адресу uabs.edu.ua. Браузер запитує у сервера DNS: "яка IP-адреса у uabs.edu.ua"? Однак, DNS-сервер може нічого не знати не тільки про це ім'я, але навіть про всі домени .edu.ua. У цьому випадку сервер звертається до кореневого сервера – наприклад, 198.41.0.4. Цей сервер повідомляє: "У мене немає інформації про дану адресу, але я знаю, що 204.74.112.1 є відповідальним за зону .ua." Тоді DNS-сервер направляє свій запит до 204.74.112.1, але той відповідає: "У мене немає інформації про даний сервер, але я знаю, що 207.142.131.234 є відповідальним за зону .edu.ua.". Нарешті, той самий запит відправляється до третього DNS-сервера і отримує відповідь про IP-адресу, яка і передається клієнтові – браузеру.

Контрольні питання

1. Для чого необхідна адресація в комп'ютерних мережах?
2. Що таке IP-адреса? Яка її структура? Які можливі способи представлення IP-адрес?
3. Чим відрізняються версії 4 і 6 протоколу IP? Які переваги забезпечить версія 6 протоколу IP? Чому виникла необхідність у переході на версію 6 протоколу IP?
4. Що таке маска підмережі? Для чого вона потрібна?
5. У чому полягає сенс поділу IP-адреси на ідентифікатори мережі і вузла? Для чого це потрібно?
6. У чому відмінність між класовою та безкласовою IP-адресацією? Які їх переваги і недоліки?
7. Що таке класи IP-адрес? За якими правилами вони визначаються?
8. Як призначити IP-адреси в локальній мережі (без виходу до Інтернету)?
9. Як співвідносяться IP- та MAC-адреси?
10. Що таке доменна система імен і для чого вона використовується?

ЛІТЕРАТУРА: [17, 25, 42, 45, 49].

Тема 8. МАРШРУТИЗАЦІЯ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Мета теми – розглянути принципи маршрутизації пакетів у комп'ютерній мережі, ознайомитись зі статичною та динамічною маршрутизацією, розглянути алгоритми роботи динамічних протоколів маршрутизації.

Ключові поняття: маршрутизація в комп'ютерних мережах; динамічна маршрутизація; статична маршрутизація; протоколи маршрутизації; маршрутні протоколи; алгоритми маршрутизації.

Основи маршрутизації

Під терміном "*маршрутизація пакетів"* можна розуміти якийсь механізм, що дозволяє здійснити передачу пакета з одного вузла складеної мережі на інший.

Як вже говорилося раніше, локальна мережа може бути розділена на декілька підмереж за допомогою такого мережевого обладнання, як мости й комутатори. Однак, очевидно, що ці ж пристрої можуть використовуватися й для об'єднання двох і більше мереж у єдину складену мережу.

Мости й комутатори належать до пристроїв фізичного й канального рівня мережевої моделі OSI. З огляду на це об'єднана за їхньою допомогою мережа матиме ряд обмежень і недоліків, пов'язаних з базовими технологіями, на яких побудовані підмережі, що входять до неї.

Насамперед, топологія складеної мережі, побудованої з використанням мережевого обладнання першого й другого рівнів моделі OSI, не повинна містити петель, тобто між відправником і одержувачем завжди повинен існувати тільки один єдиний шлях або маршрут. Таке обмеження істотно знижує надійність мережі через відсутність резервних маршрутів пересилання даних.

Крім того, виникають проблеми, пов'язані із системою адресації, яка необхідна для забезпечення обміну даними між будь-якими вузлами складеної мережі. Система фізичних адрес, використовувана на нижніх рівнях мережевої моделі, у масштабах складеної мережі виявляється недостатньо гнучкою й зручною.

Виникає й ряд інших складностей, пов'язаних з різнорідністю об'єднаних мереж.

Вирішенням цих проблем стало використання *маршрутизаторів* – апаратних і програмних засобів, здатних виконувати функції третього мережевого рівня моделі OSI.

Мережеве обладнання перших двох і третього рівнів використовує різну інформацію в процесі переміщення від джерела до адресата, тобто виконує схожі завдання, але принципово різними способами.

Об'єднання різнорідних (гетерогенних) підмереж за допомогою маршрутизаторів (рис. 2.8.1) допускає наявність петель у топології мережі. Зазвичай, у складних складених мережах практично завжди існує декілька альтернативних маршрутів, якими можлива передача даних між двома вузлами (рис. 2.8.2). Крім того, великі складені

мережі можуть містити в собі мережі різних масштабів – від локальних до територіально-розподілених глобальних мереж.

Маршрутом пересилання пакета з одного вузла складеної мережі на інший є порядок проходження цим пакетом транзитних мереж, що з'єднують мережі, у яких розташовані джерело й адресат даного пакета.

Складені мережі, у яких необхідна маршрутизація пакета на мережевому рівні, повинні бути об'єднані між собою за допомогою маршрутизаторів. Тому *маршрутом* пересилання пакета мережею можна назвати послідовність маршрутизаторів, через які цей пакет буде переправлений у процесі досягання свого адресата.

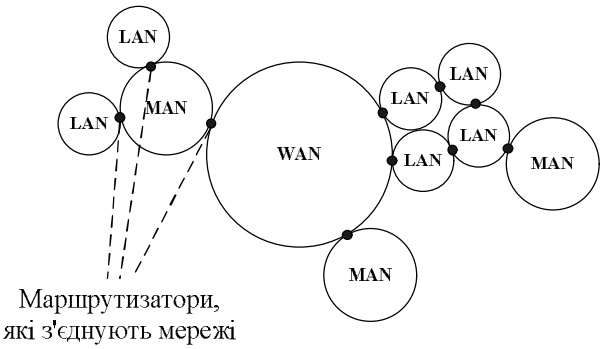


Рис. 2.8.1. Об'єднання гетерогенних мереж в складену

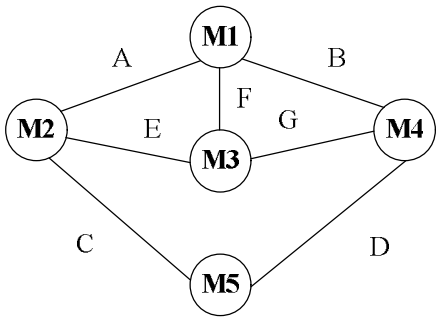


Рис. 2.8.2. Приклад RIP-системи

Маршрутизатор зазвичай передає пакет від одного каналу зв'язку до іншого. При такій передачі перед маршрутизатором стоять дві задачі: *визначення шляху* і *комутація*.

Виконуючи функцію комутації, маршрутизатор приймає пакет на одному інтерфейсі і направляє його на інший. При визначенні найкращого шляху маршрутизатор вибирає найбільш підходящий інтерфейс для відправки пакета. Вузлова частина адреси відноситься до конкретного порту на маршрутизаторі, який веде до наступного в даному напрямку маршрутизатора.

Коли додатку деякого хоста потрібно послати пакет у пункт призначення в іншій мережі, фрейм канального рівня приймається на одному з інтерфейсів маршрутизатора. На мережевому рівні досліджується заголовок фрейму для визначення мережі пункту призначення, а потім маршрутизатор звертається до таблиці маршрутизації, яка пов'язує мережі з вихідними інтерфейсами. Після читання адреси заголовок і трейлер пакета відкидаються, а сам пакет знову інкапсулюється в канальний фрейм для обраного інтерфейсу і ставиться в чергу (queue) для доставки до наступного переходу (hop).

Цей процес повторюється при кожній комутації з одного маршрутизатора на інший. На маршрутизаторі, підключеному до мережі, в якій знаходиться хост призначення, пакет інкапсулюється в канальний фрейм типу LAN-одержувача і передається на хост пункту призначення.

Для того, щоб мати можливість визначити оптимальний маршрут пересилання пакета, маршрутизатор повинен мати інформацію про всі існуючі й доступні в цей момент часу маршрути. Метод, заснований на такому представленні маршрутної інформації, називається *маршрутизацією за джерелом* і, зазвичай, використовується при тестуванні роботи мережі.

Однак, така інформація, особливо в складних і великих мережах, виявляється досить громіздкою й незручною для здійснення пошуку нею з метою вибору підходящого маршруту. Тому ні вузол, що відправив пакет, ні який-небудь проміжний маршрутизатор на шляху його проходження не зберігають інформацію про весь маршрут пакета повністю. Вузол-відправник, а також кожний маршрутизатор знають лише адресу маршрутизатора, на яку потрібно направити пакет, щоб він був доставлений за призначенням. Інакше кажучи, маршрутизатор знає, що певний пункт призначення може бути досягнутий за оптимальним шляхом за рахунок відправлення пакета певному маршрутизатору, який знає адресу наступного на шляху до кінцевого пункту призначення маршрутизатора.

Таким чином, процес маршрутизації полягає у визначенні наступного вузла в шляху проходження пакета й пересилання пакета цьому вузлу. Такий вузол називають *хопом* (від англ. *hop* – стрибок). Дійсно, передача пакета складеною мережею відбувається свого роду стрибками від маршрутизатора до маршрутизатора.

Принципи роботи засобів маршрутизації

Основні засоби маршрутизації функціонують таким чином. Хост застосовує операцію логічного “І” до IP-адреси відправника (найчастіше це його власна IP-адреса) і маски мережі, яка відповідає цій адресі, а також до IP-адреси та до відповідної маски мережі одержувача. Якщо отримані при цьому результати збігаються, це означає, що обидві IP-адреси знаходяться в одній і тій самій мережі, тому для визначення MAC-адреси пристрою одержувача можна застосувати трансляцію запиту ARP. А якщо отримані результати не збігаються, це означає, що одержувач знаходиться в іншій мережі, і для передачі пакета на хост одержувача необхідно звернутися до маршрутизатора. Дійшовши висновку, що потрібно використовувати маршрутизатор, хост відправника перевіряє наявність у своїй конфігурації IP-адреси

шлюзу, яка застосовується за замовчуванням. Потім він визначає MAC-адресу шлюзу, який застосовується за замовчуванням (маршрутизатора), за допомогою широкомовної розсилки запиту ARP. Отримавши MAC-адресу маршрутизатора, хост формує пакет, використовуючи IP-адресу кінцевого одержувача хоста, але як MAC-адресу вказує MAC-адресу маршрутизатора. Після отримання пакета маршрутизатор перевіряє пакет і виявляє, що пакет призначений йому, після чого перевіряє в пакеті IP-адресу одержувача.

Потім маршрутизатор переглядає таблицю (яка називається *таблицею маршрутизації*), у якій перераховані всі віддалені мережі, відомі йому в даний час, і намагається знайти в цій таблиці маршрут до мережі одержувача. Якщо маршрут до віддаленої мережі знайдений, маршрутизатор вводить MAC-адресу пристрою, який знаходиться в кінці наступного транзитного переходу (або наступного маршрутизатора, через який проходить даний маршрут, або найбільш віддаленого хоста), у пакет і відправляє його. А якщо не вдається знайти маршрут до віддаленої мережі, маршрутизатор повертає відправнику ICMP-повідомлення про те, що одержувач недосяжний.

Розглянемо цей процес на прикладі. Візьмемо комп'ютер з наступними параметрами протоколу IP:

- IP-адреса – 192.168.5.200;
- маска підмережі – 255. 255. 255. 0;
- основний шлюз – 192.168.5.1.

При запуску протоколу IP на комп'ютері виконується операція логічного "І" між його власними IP-адресою і маскою підмережі, у результаті якої всі біти IP-адреси, відповідні нульовим бітам маски підмережі, також стають нульовими:

- IP-адреса – 11000000 10101000 00000101 11001000;
- маска підмережі – 11111111 11111111 11111111 00000000;
- ідентифікатор мережі – 11000000 10101000 00000101 00000000.

Ця проста операція дозволяє комп'ютеру визначити ідентифікатор власної мережі (у нашому прикладі – 192.168.5.0).

Тепер припустимо, що комп'ютерові треба відправити IP-пакет за адресою 192.168.5.15. Щоб вирішити, як це потрібно зробити, комп'ютер виконує операцію логічного "І" з IP-адресою комп'ютера одержувача і власною маскою підмережі. Легко зрозуміти, що отриманий в результаті ідентифікатор мережі призначення буде співпадати з ідентифікатором власної мережі комп'ютера-відправника. Так, наш комп'ютер визначить, що комп'ютер-одержувач знаходиться в одній з ним мережі, і виконає наступні операції:

- за допомогою протоколу ARP буде визначена фізична MAC-адреса, відповідна IP-адресі комп'ютера-одержувача;
- за допомогою протоколів канального й фізичного рівня з цією MAC-адресою буде надіслана потрібна інформація.

Тепер подивимося, що зміниться, коли нашому комп'ютерові треба відправити пакет за адресою 192.168.10.20. Комп'ютер виконає аналогічну процедуру визначення ідентифікатора мережі призначення. У результаті буде отримана адреса 192.168.10.0, яка не співпадає з ідентифікатором мережі комп'ютера-відправника. Так буде встановлено, що комп'ютер-одержувач знаходиться у віддаленій мережі, і алгоритм дій комп'ютера-відправника зміниться:

- буде визначено MAC-адресу не комп'ютера-одержувача, а маршрутизатора;
- за допомогою протоколів канального й фізичного рівня з цією MAC-адресою на маршрутизатор буде надіслана потрібна інформація.

Незважаючи на те, що IP-пакет у цьому випадку не доставляється безпосередньо за призначенням, протокол IP на комп'ютері-відправникові вважає своє завдання виконаним (згадайте, що і ми при відправленні листа всього лише кидаємо його в поштову скриньку). Подальша доля IP-пакета залежить від правильного налаштування маршрутизаторів, які об'єднують мережі 192.168.5.0 і 192.168.10.0.

До речі, у даному прикладі легко продемонструвати, наскільки важливе правильне налаштування маски підмережі в параметрах IP-адресації. Нехай ми зробили помилку і вказали для комп'ютера 192.168.5.200 маску підмережі, яка дорівнює 255.255.0.0. У цьому випадку при спробі послати пакет за адресою 192.168.10.20 наш комп'ютер вважатиме, що комп'ютер призначення знаходиться в його власній мережі (адже ідентифікатори мереж при такій масці збігаються!), і буде намагатися відправити пакет самостійно. У результаті цей пакет не потрапить до маршрутизатора і не буде доставлений за призначенням.

Розглянемо приклад таблиці маршрутизації, яка знаходиться на комп'ютері з встановленою операційною системою Windows XP (рис. 2.8.3).

Як видно, у таблиці визначено декілька маршрутів з різними параметрами. Читати кожний запис в таблиці маршрутизації потрібно таким чином: щоб доставити пакет в мережу з адресою з поля "Сетевой адрес" і маскою з поля "Маска сети", потрібно з інтерфейсу з IP-адресою з поля "Интерфейс" послати пакет з IP-адресою з поля "Ад-

рес шлюза", а "вартість" такої доставки буде дорівнювати числу з поля "Метрика".

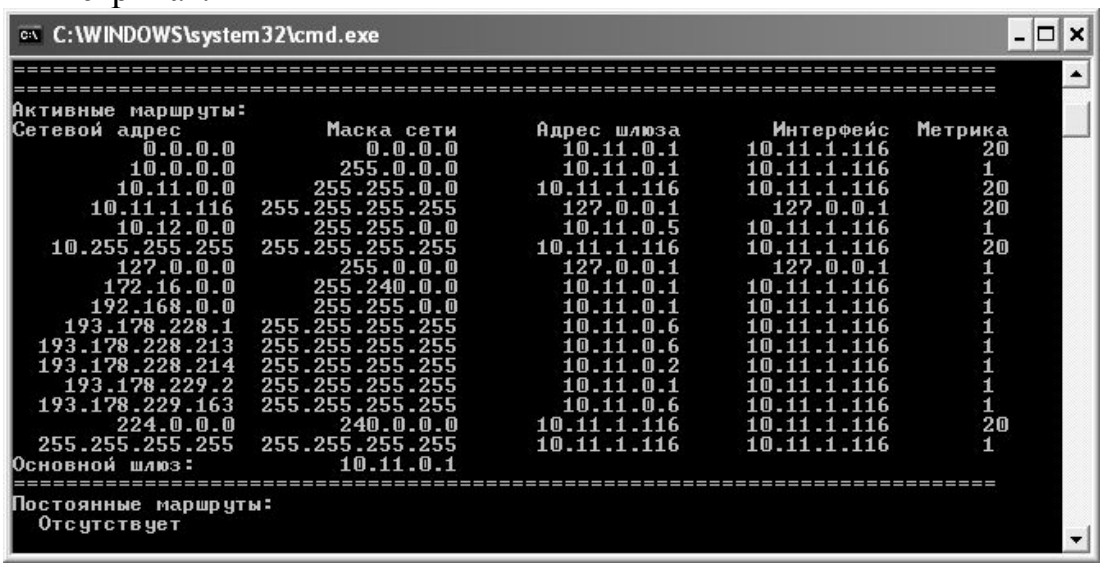


Рис. 2.8.3. Таблиця маршрутизації в ОС Windows XP

Залежно від використовуваного алгоритму маршрутизації таблиця маршрутів може заповнюватися вручну адміністратором або за допомогою спеціальних протоколів збору маршрутної інформації. При цьому своя таблиця маршрутів, навіть найелементарніша, повинна бути на кожному хості.

Вибір того або іншого маршруту з таблиці відбувається на основі застосовуваного даним маршрутизатором алгоритму маршрутизації, який базується на різних критеріях.

Порівняння динамічної та статичної маршрутизації

Статична маршрутизація (static routing) виконується вручну. Її здійснює мережевий адміністратор, вносячи зміни в конфігурацію маршрутизатора. Адміністратор повинен змінювати цю інформацію про маршрути кожного разу, коли змінюється мережева топологія. Статична маршрутизація зменшує кількість переданої службової інформації, оскільки в цьому випадку не надсилається інформація про зміни в маршрутному розкладі (у разі використання протоколу RIP це потрібно робити кожні 30 секунд).

У великих мережах, які містять велику кількість з'єднаних одна з одною підмереж, вручну прописувати маршрути доставки пакетів на всіх маршрутизаторах досить важко. До того ж такі маршрути є статичними, тобто при кожній зміні конфігурації мережі потрібно буде проробляти велику роботу, перероблюючи систему IP-маршрутизації. Щоб уникнути цього, потрібно налаштувати маршрутизатори так, щоб

вони обмінювалися один з одним інформацією про маршрути. Для цього в мережах використовують динамічні протоколи маршрутизації.

Динамічна маршрутизація (dynamic routing) виконується по-іншому. Після того, як мережевий адміністратор введе конфігураційні команди для початку динамічної маршрутизації, маршрутна обстановка змінюється автоматично при кожному отриманні з мережі інформації про зміни в її топології. При цьому обмін інформацією між маршрутизаторами про зміни в топології мережі є частиною процесів зміни мережі.

Статична маршрутизація має кілька переваг. Вона дозволяє адміністраторові вказати, яка службова інформація буде передаватися по мережі. З міркувань безпеки адміністратор може приховати деякі частини мережі. Динамічна маршрутизація має тенденцію до повної відкритості всієї інформації про мережу.

Протоколи маршрутизації та маршрутні протоколи

Часто змішують поняття маршрутного протоколу (routed protocol) і протоколу маршрутизації (routing protocol).

Маршрутний протокол (або протокол, який маршрутизується) – це будь-який мережевий протокол, який у своїй адресі мережевого рівня містить достатньо інформації для того, щоб направити пакет від вузла до вузла, спираючись на схему адресації. Маршрутний протокол визначає формат і характер використання полів всередині пакета. При цьому пакет зазвичай направляється від однієї кінцевої системи до іншої. Прикладом маршрутного протоколу є IP.

Протокол маршрутизації (або протокол, який маршрутизує) – це протокол, який підтримує маршрутний протокол, надаючи йому механізми спільного використання інформації з маршрутизації. Повідомлення протоколів маршрутизації переміщається між маршрутизаторами. Протокол маршрутизації дозволяє маршрутизаторам обмінюватися інформацією один з одним з метою підтримки таблиць маршрутизації та внесення до них змін. Прикладами протоколів маршрутизації типу TCP/IP є протоколи: Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP) та Open Shortest Path First (OSPF).

Протоколи маршрутизації

Динамічна маршрутизація дозволяє позбавитися багатьох обмежень статичної маршрутизації. Основна ідея динамічної маршрутизації полягає в тому, що для передачі інформації між маршрутизаторами в мережевій топології застосовується спеціальний протокол, який на-

зивається *протоколом маршрутизації*. Розглянемо, для чого призначені всі протоколи маршрутизації:

1. Вони дозволяють зменшити обсяг робіт, які виконуються мережевим адміністратором, оскільки вводять в таблиці маршрутизації маршрути до всіх мереж.
2. За наявності більше одного маршруту до деякої мережі вони виконують одну з таких дій:

- поміщають в таблицю найкращий маршрут;
- вводять у таблицю кілька маршрутів і забезпечують розподіл навантаження по цих маршрутах.

3. Дозволяють автоматично видаляти з таблиці недійсні маршрути при виникненні відмови каналу.
4. Після отримання інформації про найкращий маршрут вводять дані про нього в таблицю.
5. Усувають маршрутні цикли з максимально можливою оперативністю.

Ці цілі є однаковими для всіх протоколів маршрутизації, незалежно від використовуваного алгоритму маршрутизації.

Протоколи маршрутизації зазвичай класифікуються за типом застосовуваних у них алгоритмів. Нижче зазначені три основні алгоритми, які застосовуються в протоколах маршрутизації, разом з коротким описом кожного з них.

Дистанційно-векторний алгоритм. Цей алгоритм належить до числа найбільш широко застосовуваних на сьогодні алгоритмів маршрутизації. Цей алгоритм визначає напрямок (вектор) і відстань для всіх зв'язків у мережі. Маршрутизацію на основі дистанційно-векторного алгоритму іноді жартома називають "маршрутизацією з чуток". По суті, маршрутизатор, у якому застосовується дистанційно-векторний протокол, повідомляє всім безпосередньо підключеним до нього (або, як прийнято їх називати, сусіднім) маршрутизаторам: "У мене є інформація про всі наявні тут мережі!". Кожен з сусідніх маршрутизаторів відповідає: "передай мені цю інформацію, щоб я міг включити її в свою таблицю. Так, до речі, я також знаю про всі наявні тут мережі!". І такий процес відбувається у всій розподіленій мережі. Насправді жоден з маршрутизаторів не має інформації "про всі наявні тут мережі" (безумовно, крім тих, до яких кожен з них безпосередньо підключений). Просто так передбачено алгоритмом, що маршрутизатор завжди повинен діяти виходячи з того, що в ньому містяться відомості про всі мережі. А якщо один з маршрутизаторів володіє помилковою інформацією, він передає ці помилкові відомості всім іншим маршрутизаторам, не враховуючи того, що вони фактично

можуть виявитися недостовірними. З цієї причини для дистанційно-векторних протоколів потрібні складні алгоритми, які дозволяють маршрутизатору "поставити під сумнів" будь-які прийняті ним відомості про оновлення маршрутів, щоб запобігти виникненню великомасштабних маршрутних циклів. З числа IP-протоколів маршрутизації, до категорії дистанційно-векторних протоколів належать протоколи RIP і протокол IGRP (Interior Gateway Routing Protocol – протокол маршрутизації внутрішнього шлюзу). Протокол EIGRP також належить до типу дистанційно-векторних протоколів (просто є більш розвинутим у порівнянні з іншими протоколами цього типу), але компанія Cisco визначає його як "збалансований гібридний протокол".

Алгоритм маршрутизації з урахуванням стану каналів. Протоколи маршрутизації з урахуванням стану каналів засновані на використанні алгоритму SPF (Shortest Path First – вибір найкоротшого шляху) Дейкстри (Dijkstra) і діють трохи інакше, ніж дистанційно-векторні протоколи. По суті протоколи маршрутизації з урахуванням стану каналів формують "схему" розподіленої мережі, тому спочатку дозволяють отримати краще уявлення про те, де що знаходиться, у порівнянні з дистанційно-векторними протоколами. Завдяки такій перевазі протоколи маршрутизації з урахуванням стану каналів є найбільш розвиненими і складними, але у зв'язку з цим їх також набагато складніше зрозуміти і реалізувати належним чином. Прикладом такого IP-протоколу маршрутизації є OSPF.

Збалансований гібридний алгоритм. Таку назву використовує компанія Cisco Systems для позначення алгоритму маршрутизації, який застосовується у власному протоколі EIGRP. Застосування для даних алгоритмів назви "збалансований гібридний" засноване на тому, що вони вміщують у собі властивості і дистанційно-векторних алгоритмів маршрутизації, і алгоритмів маршрутизації з урахуванням стану каналів. Наприклад, хоча по суті в основі протоколу EIGRP лежить дистанційно-векторний алгоритм, цей протокол передбачає передачу додаткової інформації про топологію для формування "схеми" розподіленої мережі, як передбачено алгоритмом маршрутизації з урахуванням стану каналів.

Проведемо просту аналогію, яка дозволяє зрозуміти відмінності між основними трьома типами алгоритмів маршрутизації. Припустимо, що мережевий пакет – це мандрівник, який заблукав у пустелі та який ходить колами у пошуках води й раптово виявляє на своєму шляху розвилку доріг. Якщо б цей мандрівник діяв на основі дистанційно-векторного протоколу, то прочитав би покажчик з написом "До

води веде ця дорога", і пішов услід за ним, не думаючи про те, що хтось міг просто побавитися і переставити покажчик. А якщо б цей мандрівник керувався протоколом з урахуванням стану каналів, то спочатку зайнявся б складанням докладної схеми доріг і (в кінцевому підсумку) знайшов би правильний маршрут. З іншого боку, якби мандрівник діяв у відповідності зі збалансованим гібридним протоколом, то він не тільки б склав би схему, а й намагався швидше знайти правильний маршрут.

Протоколи маршрутизації поділяються не тільки за своїми алгоритмами, але і за своїм призначенням: вони можуть належати або до категорії *протоколів внутрішнього шлюзу (Interior Gateway Protocol – IGP)*, або до категорії *протоколів зовнішнього шлюзу (Exterior Gateway Protocol – EGP)*. Протоколи IGP зазвичай здатні підтримувати належним чином тільки мережі обмежених розмірів (хоча після невеликого налаштування деякі з них набувають здатність підтримувати досить великі мережі) і тому вони, як правило, набагато простіше в порівнянні з протоколами EGP, здатними підтримувати дуже великі мережі. Протоколи IGP призначені для маршрутизації трафіку усередині *автономних систем (Autonomous System – AS)*. Термін "автономна система" – це просто хитромудрий спосіб позначення розподіленої мережі, яка знаходиться під управлінням одного адміністративного органу. До категорії автономних систем належать всі локальні мережі, а також велика частина корпоративних розподілених мереж. Але сама мережа Internet являє собою сукупність мереж, яка складається з безлічі автономних систем. Протоколи EGP, з іншого боку, призначені для підтримки величезних мереж. Основне призначення протоколів EGP полягає в маршрутизації трафіку між автономними системами.

Контрольні питання

1. З якою метою мережі з'єднують між собою?
2. Які основні функції маршрутизатора?
3. Які поля містить таблиця маршрутизації?
4. Які алгоритми маршрутизації Вам відомі?
5. У чому різниця між маршрутним протоколом та протоколом маршрутизації?
6. У чому різниця між дистанційно-векторними протоколами і протоколами стану зв'язків?
7. У чому різниця між статичною і динамічною маршрутизацією?

ЛІТЕРАТУРА: [2, 15, 17, 25, 38, 51, 53].

Тема 9. МЕТОДИКА ПРОЕКТУВАННЯ МЕРЕЖІ ТА СКС

Мета теми – ознайомитися з основними етапами проектування мереж; розглянути основи проектування структурованих кабельних систем (СКС); ознайомитися з вимогами та рекомендаціями міжнародного стандарту ISO/IEC 11801:2002; розглянути структуру та топологію СКС.

Ключові поняття: структурована кабельна система, міжнародний стандарт ISO/IEC 11801:2002, топологія СКС, структура СКС, технічні приміщення СКС.

Етапи проектування мережі

Будь-яке проектування, як відомо, являє собою сильно спрощене моделювання дійсності, яка ще не настала. Саме тому передбачити всі можливі фактори, врахувати всі потреби, які можуть виникнути в майбутньому, практично неможливо. Отже, навіть найдокладніші керівництва з проектування мають не дуже велику цінність.

Однак загальні підходи до проектування локальних комп'ютерних мереж все-таки можуть бути сформульовані, деякі корисні принципи такого проектування пропонуються і з успіхом використовуються.

При створенні нової мережі для якого-небудь підприємства бажано враховувати наступні фактори:

1. Потрібний розмір мережі (на даний момент, у найближчому майбутньому і в далекій перспективі).
2. Структуру, ієрархію і основні частини мережі (по підрозділах підприємства, а також по кімнатах, поверхах і будівлях підприємства).
3. Основні напрями та інтенсивність інформаційних потоків у мережі (на даний момент, у найближчому майбутньому і в далекій перспективі).
4. Характер інформації (дані, відео, звук, зображення), яка передається мережею, бо це безпосередньо позначається на необхідній швидкості передачі.
5. Технічні характеристики обладнання (комп'ютерів, адаптерів, кабелів, повторювачів, концентраторів, комутаторів) і його вартість.
6. Можливості монтажу кабельної системи у приміщеннях і між ними, а також заходи щодо забезпечення цілісності кабелю.
7. Обслуговування мережі та контроль її працездатності та безпеки.
8. Вимоги до програмних засобів за допустимим розміром мережі, швидкістю, гнучкістю, розмежуванням прав доступу, вартості, за можливостями контролю обміну інформацією тощо.
9. Необхідність підключення до глобальних або до інших локальних мереж.

Таким чином, проектування мережі можна розділити на декілька етапів:

1. Визначення розміру і структури мережі;
2. Визначення, для вирішення яких прикладних задач буде використовуватися мережа;
3. Вибір мережі з централізованим управлінням або однорангової мережі, виходячи з задач, які необхідно вирішувати;
4. Вибір мережевої операційної системи;
5. Вибір топології мережі та методу доступу;
6. Вибір мережевого апаратного забезпечення: комп'ютер для файл-сервера (або файл-серверів, якщо їх декілька), комп'ютери для робочих станцій, мережеві адаптери тощо.

Цілком можливо, що після вивчення всіх факторів з'ясується, що можна обійтися без мережі, уникнувши тим самим солідних витрат на апаратуру і програмне забезпечення, встановлення, експлуатацію, підтримку та ремонт мережі, зарплату обслуговуючому персоналу тощо.

Мережа в порівнянні з автономними комп'ютерами породжує безліч додаткових проблем: від простих механічних (комп'ютери, підключені до мережі, важче переміщувати з місця на місце) до складних інформаційних (необхідність контролювати спільно використовувані ресурси, запобігати зараженню мережі вірусами). До того ж користувачі мережі вже не так незалежні, як користувачі автономних комп'ютерів, їм треба дотримуватися певних правил, підкорятися встановленим вимогам, яким їх необхідно навчити.

Нарешті, мережа гостро ставить питання про безпеку інформації, захист від несанкціонованого доступу, адже з будь-якого комп'ютера мережі можна зчитувати дані з загальних мережевих дисків. Захистити один комп'ютер або навіть декілька набагато простіше, ніж цілу мережу. Тому приступати до монтажу мережі доцільно тільки тоді, коли без мережі робота стає неможливою, непродуктивною, коли відсутність міжкомп'ютерного зв'язку уповільнює роботу та стримує розвиток справи.

Вибір розміру і структури мережі

Під *розміром мережі* в даному випадку розуміють кількість об'єднаних у мережу комп'ютерів і відстань між ними. Треба чітко уявляти собі, скільки комп'ютерів (мінімально і максимально) потребує підключення до мережі. У будь-якому випадку необхідно залишити можливість для подальшого збільшення кількості комп'ютерів в мережі, хоча б відсотків на 20-50. До речі, зовсім не обов'язково раз і назавжди включати в мережу всі комп'ютери підприємства. Можливо, є сенс залишити деякі з них автономними, наприклад, з міркувань безпеки

інформації на їх дисках. Кількість підключених до мережі комп'ютерів сильно впливає як на її продуктивність, так і на складність її обслуговування. Розмір мережі також визначає вартість необхідних програмних засобів. Тому помилки в даному випадку можуть мати досить серйозні наслідки.

Необхідна довжина ліній зв'язку мережі також відіграє важливу роль в проектуванні мережі. Наприклад, якщо відстані дуже великі, може знадобитися використання дорогого обладнання. До того ж із збільшенням відстані різко зростає значимість захисту ліній зв'язку від зовнішніх електромагнітних перешкод. Від відстані залежить і швидкість передачі інформації мережею. Доцільно при виборі відстаней закладати невеликий запас (хоча б 10 %) для врахування непередбачених обставин. Подолати обмеження по довжині іноді можна шляхом вибору структури мережі, розбиття її на окремі частини.

Під *структурою мережі* розуміють спосіб поділу мережі на частини (сегменти), а також спосіб з'єднання цих сегментів між собою. Мережа підприємства може включати в себе робочі групи комп'ютерів, мережі підрозділів, опорні мережі, засоби зв'язку з іншими мережами. Для об'єднання частин мережі можуть використовуватися повторювачі, концентратори, комутатори, мости та маршрутизатори. Причому в ряді випадків вартість цього обладнання може навіть перевищити вартість комп'ютерів, мережевих адаптерів і кабелю, тому вибір структури мережі дуже важливий.

В ідеалі структура мережі повинна відповідати структурі будівлі або комплексу будівель підприємства. Робочі місця групи співробітників, які займаються одним завданням (наприклад, бухгалтерія, відділ продажів, інженерна група), повинні розміщуватися в одній або поруч розташованих кімнатах. Тоді можна комп'ютери цих співробітників об'єднати в один сегмент, в єдину робочу групу і встановити поблизу їх кімнат сервер, з яким вони працюватимуть, а також концентратор або комутатор, що зв'язує всі їхні машини. Так само робочі місця співробітників підрозділу, що займається комплексом близьких завдань, краще розташувати на одному поверсі будівлі, це спростить їх об'єднання в сегмент і подальше його адміністрування. На цьому ж поверсі зручно розташувати комутатори, маршрутизатори і сервери, з якими працює даний підрозділ.

Як і в інших випадках, при виборі структури розумно залишати можливості для подальшого розвитку мережі. Наприклад, краще купувати комутатори або маршрутизатори з кількістю портів дещо більшою, ніж потрібно в даний момент (хоча б на 10-20 %). Це дозволить за потребою легко включити в мережу один або кілька сегментів.

Адже будь-яке підприємство завжди прагне до зростання, і це зростання не повинне кожного разу приводити до необхідності проектувати мережу підприємства заново.

Визначення задач, які будуть вирішуватися

На цьому етапі необхідно з'ясувати, для чого слід використовувати мережу. Може виявитися так, що витратиться дуже багато коштів на побудову високошвидкісної мережі, можливості якої будуть використовуватися тільки на 5 відсотків.

Декілька типових використань мережі описані в табл. 2.9.1.

Таблиця 2.9.1

Мережі та їх характеристика

Застосування	Особливості
Мережа для невеликої фірми	Колективне використання одного-двох принтерів, файлів на дисках файл-сервера, модему, передача файлів і повідомлень від однієї робочої станції до іншої. Невелика кількість робочих станцій, мала протяжність мережі
Мережа для великої фірми	Загальна протяжність мережі значна, у ній використовуються десятки і сотні робочих станцій. Пред'являються підвищені вимоги до продуктивності і надійності мережі
Мережа для роботи з великою базою даних і великою кількістю користувачів	Аналогічно попередній мережі, але додатково підключені потужні міні-комп'ютери або робочі станції, які використовуються як СУБД-сервери. Підвищені вимоги до надійності, продуктивності і стійкості до відмов

Склад програмного забезпечення, яке планується використовувати в мережі, і кількість користувачів сильно впливає на вимоги, що пред'являються до файл-сервера.

Вибір мережевої операційної системи

Після того як визначилися з вирішуваними в мережі задачами, слід вибрати мережеву операційну систему (ОС).

Мережеві ОС можуть бути розділені на дві групи: *масштабу відділу* і *масштабу підприємства*. ОС для відділів або робочих груп забезпечують набір мережевих сервісів, включаючи мережеве використання файлів, додатків і принтерів. Вони також повинні забезпечувати властивості відмовостійкості, наприклад, працювати з RAID-масивами, підтримувати кластерні архітектури. Мережеві ОС відділів зазвичай простіші у встановленні і управлінні у порівнянні з мережевими ОС підприємства, у них менше функціональних властивостей,

вони менше захищають дані та мають слабші можливості по взаємодії з іншими типами мереж, а також гіршу продуктивність.

Мережева операційна система масштабу підприємства перш за все повинна володіти основними властивостями будь-яких корпоративних продуктів, у тому числі:

- масштабованістю, тобто здатністю однаково добре працювати в широкому діапазоні різних кількісних характеристик мережі;
- сумісністю з іншими продуктами, тобто здатністю працювати в складному гетерогенному середовищі інтермережі в режимі plug-and-play.

Критеріями для вибору ОС масштабу підприємства є наступні характеристики:

- органічна підтримка багатосерверної мережі;
- висока ефективність файлових операцій;
- можливість ефективної інтеграції з іншими ОС;
- наявність централізованої масштабованої довідкової служби;
- гарні перспективи розвитку;
- ефективна робота віддалених користувачів;
- різноманітні сервіси: файл-сервіс, принт-сервіс, безпека даних і відмовостійкість, архівування даних, служба обміну повідомленнями, різноманітні бази даних та інші;
- різноманітні програмно-апаратні хост-платформи: IBM SNA, DEC NSA, UNIX;
- різноманітні стеки протоколів: TCP/IP, IPX/SPX, NetBIOS, AppleTalk;
- підтримка різноманітних операційних систем кінцевих користувачів: UNIX, Windows, Mac;
- підтримка мережевого обладнання стандартів Ethernet, Token Ring, FDDI.

Зазвичай, жодна з існуючих мережевих ОС не відповідає в повному обсязі перерахованим вимогам, тому вибір мережевої ОС, як правило, здійснюється з урахуванням виробничої ситуації і досвіду.

Останнім часом спостерігається стійка тенденція до скорочення кількості фірм, які виробляють мережеві програмні засоби. Причому навіть постачальники, що залишаються на цьому ринку, намагаються мінімізувати кількість своїх продуктів. У результаті вибір у користувача не такий вже й великий. Найчастіше вибирати доводиться між Novell і Microsoft. Всі інші фірми або взагалі припинили виробництво нових мережевих продуктів, або їх частка на ринку незрівнянно менша, ніж у цих двох гігантів.

Вибираючи між продуктами компаній Microsoft та Novell, необхідно мати на увазі, що традиційно перевагами продуктів Novell (мережеві ОС NetWare) вважаються:

- більш досконала архітектура мережевої ОС;
- універсальність і функціональна повнота програмних засобів;
- спрощене адміністрування мережі;
- більш висока захищеність від вірусів і несанкціонованого доступу;
- підтримка різних типів користувачів на різних комп'ютерних платформах.

Головною перевагою продуктів Microsoft вважається краща сумісність з користувачами на базі ОС Microsoft Windows.

Ціни на новітні продукти компаній Microsoft і Novell приблизно однакові. Утім вартість експлуатації ОС NetWare виявляється зазвичай помітно нижчою, ніж вартість експлуатації Windows Server.

Вибір топології мережі та методу доступу

При організації комп'ютерної мережі виключно важливим є вибір топології, тобто компонування мережевих пристроїв та кабельної інфраструктури. Потрібно вибрати таку топологію, яка забезпечила б відмінну й ефективну роботу мережі, зручне управління потоками мережевих даних. Бажано також, щоб мережа по вартості створення і супроводу вийшла недорогою, але в той же час залишалися можливості для її подальшого розширення і, бажано, для переходу до більш високошвидкісних технологій зв'язку.

Мережа Ethernet зараз найпопулярніша у світі (більше 90 % ринку), приблизно такою вона і залишиться у найближчі роки. Цьому значною мірою сприяло те, що з самого початку характеристики, параметри, протоколи мережі були відкриті, у результаті чого величезна кількість виробників в усьому світі стали випускати апаратуру Ethernet, повністю сумісну між собою. Технологія Ethernet використовує метод доступу CSMA/CD.

Вибір обладнання

При виборі мережевого обладнання треба враховувати безліч чинників, зокрема:

1. Рівень стандартизації обладнання та його сумісність з найбільш поширеними програмними засобами.
2. Швидкість передачі інформації і можливість її подальшого збільшення.
3. Можливі топології мережі та їх комбінації (шина, кільце, пасивна зірка, пасивне дерево).

4. Метод управління обміном у мережі (CSMA/CD, повнодуплексний або маркерний метод).
5. Дозволені типи кабелю мережі, максимальну його довжину, захищеність від перешкод.
6. Вартість і технічні характеристики конкретних апаратних засобів (мережевих адаптерів, повторювачів, концентраторів, комутаторів тощо).

Усім цим часто нехтують, а дарма: замінити програмне забезпечення порівняно просто, а от заміна апаратури, особливо прокладання кабелю, обходиться часом дуже дорого, а іноді буває просто неможливою.

На сьогодні для організації локальних мереж у переважній більшості випадків використовується неекранована вита пара UTP. Більш дорогі варіанти на основі екранованої витої пари, оптоволоконного кабелю або бездротових з'єднань застосовуються на підприємствах, де в цьому дійсно існує гостра необхідність. Наприклад, оптоволокно може використовуватися для зв'язку між віддаленими сегментами мережі без втрати швидкості.

Ще одна важлива задача – це вибір комп'ютерів. Якщо для робочих станцій або невиділених серверів зазвичай використовують ті комп'ютери, які вже є на підприємстві, то виділений сервер бажано купувати спеціально для мережі. Краще, якщо це буде швидкодіючий спеціалізований комп'ютер-сервер, спроектований з урахуванням специфічних потреб мережі (такі сервери випускаються усіма найбільшими виробниками комп'ютерів).

Вимоги до сервера:

- максимально швидкий процесор (для нової серверної операційної системи Windows Server 2008 компанії Microsoft процесор повинен мати мінімальну тактову частоту 1 ГГц, але рекомендовано використовувати процесор з частотою 2 ГГц і вище). Для великих мереж застосовують і багатопроцесорні сервери (іноді до 32 процесорів);
- великий обсяг оперативної пам'яті (фірма Microsoft рекомендує для своєї операційної системи Windows Server 2008 обсяг пам'яті не менше 512 МБ, такі ж вимоги фірми Novell для NetWare 6.5). Великий обсяг пам'яті сервера навіть важливіше швидкодії процесора, оскільки дозволяє ефективно використовувати кешування дискової інформації, зберігаючи в пам'яті копії тих областей диска, з якими проводиться найбільш інтенсивний обмін;
- швидкі жорсткі диски великого обсягу (мінімальні вимоги до вільного місця на жорсткому диску фірми Microsoft для операційної

системи Windows Server 2008 – 10 ГБ, а рекомендується – 40 ГБ і вище).

Вимоги до комп'ютерів, які використовуються як робочі станції, визначаються, перш за все, виходячи з тих задач, які будуть вирішуватися на цих робочих станціях.

Для будь-якої мережі вкрай критична ситуація перебоїв в системі електроживлення. Незважаючи на те, що багато мережевих програмних засобів використовують спеціальні заходи запобігання цьому, як і проти інших відмов апаратури (наприклад, дублювання дисків), проблема дуже серйозна. Іноді відключення живлення може повністю і надовго вивести з ладу мережу.

В ідеалі захищеними від відключення живлення повинні бути всі сервери мережі (бажано і робочі станції). Простіше всього цього домогтися, якщо сервер в мережі всього один. Джерело безперебійного живлення при збої живлення переходить на живлення підключеного комп'ютера від акумулятора й подає спеціальний сигнал комп'ютеру, який за короткий час завершує всі поточні операції і зберігає дані на диску. При виборі джерела безперебійного живлення треба, перш за все, звертати увагу на максимальну потужність, яку воно забезпечує, і на час підтримання ним номінального рівня напруги. Вартість пристрою досить висока (до декількох тисяч доларів). Тому доцільно одне джерело безперебійного живлення застосовувати для двох-трьох серверів.

Найстійкіші до відмов живлення ноутбуки. Вбудований акумулятор і низьке споживання енергії забезпечують їх нормальну роботу без зовнішнього живлення протягом однієї-двох годин і навіть більше. Якщо ще врахувати низький рівень випромінювань і високу якість зображення моніторів цих комп'ютерів, то варто серйозно розглянути можливість використання ноутбуків як робочих станцій, а, ймовірно, і не надто потужного, невиділеного сервера. Тим більше що багато ноутбуків мають вбудовані мережеві адаптери досить непоганої якості. Особливо зручне застосування ноутбуків у тимчасових мережах з безліччю серверів. Застосування зовнішніх джерел безперебійного живлення в подібних випадках стає занадто дорогим задоволенням.

Крім перерахованих проблем проектувальнику мережі доводиться вирішувати завдання, пов'язані з вибором мережевих адаптерів, повторювачів, концентраторів, комутаторів і маршрутизаторів, але про це вже досить сказано в попередніх розділах. Варто тільки відзначити, що продуктивність мережі та її надійність визначаються найбільш низькоякісним її компонентом. При покупці дорогих концентраторів або комутаторів не варто економити, наприклад, на мережевих адаптерах.

Вірно і зворотне. Бажано, щоб всі компоненти обладнання максимально повно відповідали один одному.

Проектування структурованої кабельної системи

Сьогодні розвиток і діяльність будь-якої організації неможливі без існування повноцінної і надійної структурованої кабельної системи. Структуровані кабельні системи (СКС) містять у собі комп'ютерні, телефонні, телевізійні мережі, а також кабелі охоронної та пожежної сигналізації, систем контролю доступу та інших систем безпеки.

Проектування і монтаж СКС здійснюється на етапі будівництва – у цьому основна відмінність СКС від простого комплексу мереж. При цьому при проектуванні СКС спочатку закладається величезна пропускна здатність і потужність, тому канали СКС здатні витримати навіть дуже велике навантаження.

Структурованою кабельною системою (СКС) будемо називати кабельну систему, яка має наступні чотири чіткі ознаки:

- стандартизовані структуру і топологію;
- стандартизовані компоненти (кабелі, роз'єми, комутаційні пристрої, комутаційні шнури);
- стандартизовані електромагнітні характеристики ліній і каналів зв'язку, які можуть бути створені за допомогою СКС (загасання, смуга пропускання частот, затримка сигналів та ряд інших);
- стандартизовані методи управління (адміністрування) кабельної системи.

Відзначимо, що термін "стандартизований" не означає тут "однаковий", а визначає лише, що всі різні СКС будуються за однаковими принципами і правилами, які задані національними або міжнародними стандартами в галузі інформаційних технологій.

Кабельну систему, яка не володіє хоча б одною з перерахованих ознак, будемо називати *винятковою кабельною системою (ВКС)*. Винятковою не в тому сенсі, що вона – видатна, а в тому – що вона єдина у своєму роді.

В англомовній літературі для СКС використовують еквівалентні терміни "generic cabling" і "structured cabling", а для ВКС – "proprietary cabling" (приватна кабельна система).

Завдяки перерахованим вище чотирьом характерним ознакам СКС здобувають, у порівнянні з ВКС, істотні переваги:

- універсальність;
- високу адаптивну здатність до змін зовнішніх умов ("гнучкість");
- низькі трудовитрати при експлуатації;
- високу економічну ефективність.

Універсальність. Ця перевага полягає в тому, що одні й ті ж кабелі і роз'єми можуть бути використані для з'єднання між собою активних блоків різних радіоелектронних систем: локальних мереж, систем телефонного зв'язку, відеоспостереження, охоронної сигналізації, телебачення та ін.

Гнучкість. Суть цієї переваги полягає в тому, що простими і швидкими перемиканнями комутаційних шнурів СКС пристосовується:

- до змін організаційної структури підприємства (створення та ліквідація підрозділів, збільшення або скорочення чисельності персоналу);
- до передислокації співробітників і підрозділів;
- до зміни типів обладнання та його постачальників.

Низькі трудовитрати на експлуатацію. Дана перевага витікає з того, що відпадає необхідність в утриманні бригади монтажників, необхідної при наявності ВКС для перекладки кабелів і перестановки розеток, а також з того, що експлуатацію СКС здійснює нечисленний і спеціальний персонал (не потрібні окремі фахівці по кабельних проводках телефонних, охоронних, комп'ютерних та інших систем).

Висока економічна ефективність. Дана перевага не так очевидна, як попередні, але є найважливішою. Зазвичай витрати на експлуатацію СКС (50 %) і переробку будівлі (25 %) значно перевищують початкові витрати на фінансування (14 %) та будівництво (11 %), але інтеграція систем на основі СКС може істотно знизити витрати на експлуатацію будівлі протягом терміну її життя. Так, СКС дозволяє знизити витрати в порівнянні з ВКС – на будівництво на 14 %, на час праці – на 49 % і на експлуатацію – на 34 %.

Основною перешкодою широкого впровадження СКС є їх висока вартість, що робить прийнятним це рішення для відносно масштабних локальних мереж рівня підприємства. Дійсно, стандарти на СКС передбачають проведення, разом з іншими, комплексу дорогих будівельних робіт.

Основними стандартами на СКС є:

- Міжнародний стандарт ISO/IEC 11801 "Information technology – Generic cabling for customer premises" ("Інформаційна технологія – структурована кабельна система для будівлі і території замовника");
- Європейський стандарт EN 50173 "Information technology – Generic cabling systems" ("Інформаційна технологія – Структуровані кабельні системи");
- Американський стандарт EIA/TIA-568B "Commercial Building Telecommunications Wiring Standard".

Стандарти на СКС періодично (приблизно раз на п'ять років) переглядаються у зв'язку з розвитком апаратних засобів локальних ме-

реж (включаючи удосконалення мідних і оптоволоконних кабелів). На сьогоднішній день діють версії стандартів ISO/IEC 11801:Ed. 2.1 2008-05 (включає друге видання стандарту (2002 р.) і Додаток 1 2008 року – специфікації каналів класів Ea і Fa) та EIA/TIA-568B.

Слід зауважити також, що американський, європейський і міжнародний стандарти дуже близькі один до одного в технічному сенсі: більшість їхніх вимог до СКС співпадають, а незначна різниця в термінах і конкретні цифри не носять принципового характеру, відображаючи лише традиції і локальний технічний рівень кабельних систем.

Вимоги та рекомендації міжнародного стандарту ISO/IEC 11801:2002

Міжнародний стандарт ISO/IEC 11801 "Information technology – Generic cabling for customer premises" ("Інформаційна технологія – Структурована кабельна система для будівель і території Замовника") у другому виданні офіційно опублікований у вересні 2002 року.

Стандарт містить 13 розділів, 9 додатків (3 нормативних – A, B, C і 6 інформативних – D, E, F, G, H, I) і бібліографічний список інших нормативних документів з 74 назв. Обсяг документа – 136 сторінок.

Стандарт (як видання) охороняється авторським правом, на його поширення потрібна ліцензія ISO/IEC.

До цифр і рекомендацій, що належать до СКС, які публікуються в численних статтях і на різних сайтах Інтернету, необхідно ставитися обережно, оскільки вони дуже часто визначаються особистим сприйняттям стандарту і досвідом авторів і не повною мірою відповідають оригіналу. Безумовно, фахівець у сфері СКС повинен мати на своєму робочому столі оригінал міжнародного стандарту в чинній редакції.

Стандарт ISO/IEC 11801:2002 корисний для трьох груп фахівців.

Він забезпечує:

- *користувачів і власників СКС*, по-перше, незалежною від програм універсальною кабельною системою, здатною підтримувати широкий спектр апаратури і, по-друге, "гнучкою" кабельною системою, модифікації якої легкі й економічні;
- *будівельників (проектувальників, інженерів, архітекторів)* керівництвом, яке дозволяє пристосувати будинок до кабельної системи навіть до того моменту, коли стануть відомі конкретні вимоги специфічних додатків. Причому це справедливо як на етапі початкового проектування будівлі, так і на етапі його реконструкції;
- *розробників радіоелектронної апаратури (а також стандартизаторів у цій області)* кабельною системою, яка підтримує всі відомі види апаратури, а крім того, є основою для розробки апаратури наступних поколінь.

Стандарт ISO/IEC 11801:2002 визначає кабельну систему як мультивендорну, яку можна створити, використовуючи компоненти як одного, так і різних постачальників. При цьому він спирається на промислові стандарти IEC, що визначають вимоги до електричних і оптичних кабелів і коннекторів; на стандарти з інсталяції й тестування кабельних систем; на стандарти додатків і керівництва за специфічними додатками.

У цілому стандарт ISO/IEC 11801: 2002 специфікує вимоги до кабельної системи, які охоплюють:

- структуру, топологію і мінімальну конфігурацію СКС;
- інтерфейси на інформаційних розетках;
- електромагнітні характеристики і параметри окремих кабельних ліній і каналів;
- інсталяцію кабельної системи та варіанти її реалізації;
- електромагнітні характеристики компонентів кабельної системи, які необхідні для досягнення максимальних відстаней, визначених стандартом;
- процедури сертифікації та встановлення відповідності кабельної системи даному стандарту.

Структура кабельної системи

На відміну від ВКС структурована кабельна система проектується і будується з цілком визначеного та обмеженого ряду функціональних компонентів.

Їх усього чотири види:

- кабелі (електричні та оптичні);
- розподільчі пристрої (кросові блоки і комутаційні (патч) панелі);
- інформаційні з'єднувачі (гнізда, виделки);
- точки консолідації.

Ніяких інших функціональних елементів СКС не містить. Зазвичай, для побудови реальної кабельної системи потрібно багато інших додаткових виробів, таких, як шафи та стійки, кабельні канали і лотки, монтажні інструменти і пристрої, спеціалізовані вимірювальні прилади тощо. Однак ці додаткові компоненти не є функціональними, хоча і визначають, зрештою, деякі товарні якості СКС як продукту. Структурна схема СКС наведена на рис. 2.9.1.

На рисунку визначені:

- РПТ – розподільчий пристрій території (Campus Distributor – CD);
- РПБ – розподільчий пристрій будівлі (Building Distributor – BD);
- РПП – розподільчий пристрій поверху (Floor Distributor – FD);
- ТК – точка консолідації (Consolidation Point – CP);
- ІР – інформаційна розетка (Telecommunication Outlet – TO).

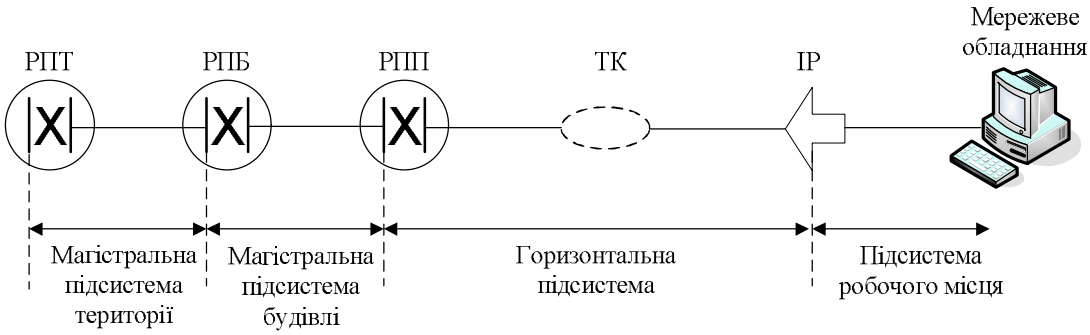


Рис. 2.9.1. Структурна схема СКС

У загальному випадку СКС включає в себе три підсистеми:

- магістральну підсистему території (МПТ);
- магістральну підсистему будівлі (МПБ);
- горизонтальну підсистему (ГП).

Зрозуміло, що за відсутності у підприємства території (одна будівля) буде відсутня, відповідно, і магістральна підсистема території. Відзначимо, що кабелі зовнішніх ліній зв'язку, шнури робочого місця, шнури обладнання не входять до складу СКС: вони входять до складу тих інженерних систем, які підключаються до СКС і можуть бути замінені при зміні інженерної системи. Призначення функціональних елементів структурної схеми СКС зрозуміло з їхніх назв.

Розподільчі пристрої всіх рангів забезпечують можливість конфігурувати кабельну систему, щоб підтримувати різні топології (шина, зірка, кільце) активних інженерних систем. З'єднання підсистем СКС при створенні активних інженерних систем (ЛВМ та ін.) може бути здійснене через активні пристрої (наприклад, концентратор), або пасивним способом за допомогою комутаційних шнурів або кросових перемичок.

Пристрій, що називається *точкою консолідації (ТК)*, являє собою панель з інформаційними гніздами, на яких з одного боку приєднані стаціонарні кабелі горизонтальної підсистеми. У ці гнізда вмикаються інформаційні вилки, якими оконцовані так звані "кабелі точки консолідації", що йдуть, у свою чергу, через мобільні перегородки до інформаційних розеток, закріплених на цих перегородках. Кабелі точки консолідації можуть бути переміщені в просторі разом з цими мобільними перегородками у так званому "відкритому офісі". ТК може бути корисною у відкритому офісі, де необхідно переміщати інформаційні розетки при зміні дислокації робочих місць.

Розглянемо більш детально елементний склад підсистем СКС:

- *магістральна підсистема території* включає в себе магістральні кабелі території, механічне закінчення кабелів (роз'єми) в РПТ та

РПБ і комутаційні з'єднання в РПТ. Магістральні кабелі території з'єднують в єдину мережу зв'язку окремо розташовані на одній території будинки (їх РПБ). На практиці ця підсистема досить часто має фізичну кільцеву топологію, що додатково забезпечує збільшення надійності за рахунок наявності резервних кабельних трас. Із цих же міркувань ця підсистема іноді реалізується за подвійною кільцевою топологією. Якщо СКС монтується автономно тільки в одному будинку, то магістральна підсистема території відсутня. У будинках з більшими розмірами до МПТ належать ті кабелі, які мають довжину понад 500 м, хоча фактично не виходять за межі будинку;

- *магістральна підсистема будівлі,* яка називається в деяких СКС вертикальною або вторинною підсистемою, містить прокладені між РПБ і РПП внутрішні магістральні кабелі, механічне закінчення кабелів (роз'єми) в РПБ та РПП, а також комутаційні з'єднання в РПБ. Кабелі розглянутої підсистеми фактично зв'язують між собою окремі поверхи будинку і/або просторово рознесені приміщення в межах одного будинку. Якщо СКС обслуговує один поверх, то МПТ може бути відсутньою;
- *горизонтальна підсистема* утворена горизонтальними кабелями між РПП і розетковими модулями інформаційних розеток робочих місць, самими інформаційними розетками, а також комутаційним обладнанням у РПП, до якого підключаються горизонтальні кабелі. До складу ГП входить також більша частина комутаційних шнурів і/або перемичок у РПП. При побудові горизонтальної проводки допускається використання однієї точки консолідації на тракт, у якій відбувається зміна типу кабелю, що прокладається (наприклад, перехід на плоский кабель для прокладки під килимовим покриттям з еквівалентними передатними характеристиками). Не допускається включення активних елементів і адаптерів до складу СКС.

Підсистема робочого місця забезпечує підключення мережевого обладнання на робочих місцях. Застосовуване для її реалізації обладнання цілком і повністю залежить від конкретного додатку. Вона не є частиною СКС і виходить за рамки дії стандарту ISO/IEC 11801:2002, хоча цей нормативний документ накладає на її параметри й характеристики певні обмеження.

Топологія СКС

В основу будь-якої повномасштабної СКС покладена деревоподібна топологія, яку іноді називають також *структурою ієрархічної зірки*. Функції вузлів структури виконує комутаційне обладнання різного

виду, яке може мати два основні різновиди: індивідуальні інформаційні розетки, що експлуатуються користувачами кабельної системи, і панелі різних видів, що утворюють групове комутаційне поле, з якими працює обслуговуючий персонал. Комутаційне обладнання з'єднується між собою електричними й волоконно-оптичними кабелями різних видів.

Усі кабелі, які входять у технічні приміщення, обов'язково заводяться на згадані вище комутаційні панелі, на яких за допомогою шнурів, здійснюються всі підключення й перемикання, у процесі поточної експлуатації кабельної системи. Стандарти дозволяють також організацію резервних трактів передачі сигналів. Усе це, у комбінації з використаною деревоподібною топологією, у частині кабельної системи, що стосується СКС, забезпечує гнучкість і надійність СКС, а також можливість легкої переконфігурації й адаптування кабельної системи під конкретний додаток (рис. 2.9.2).

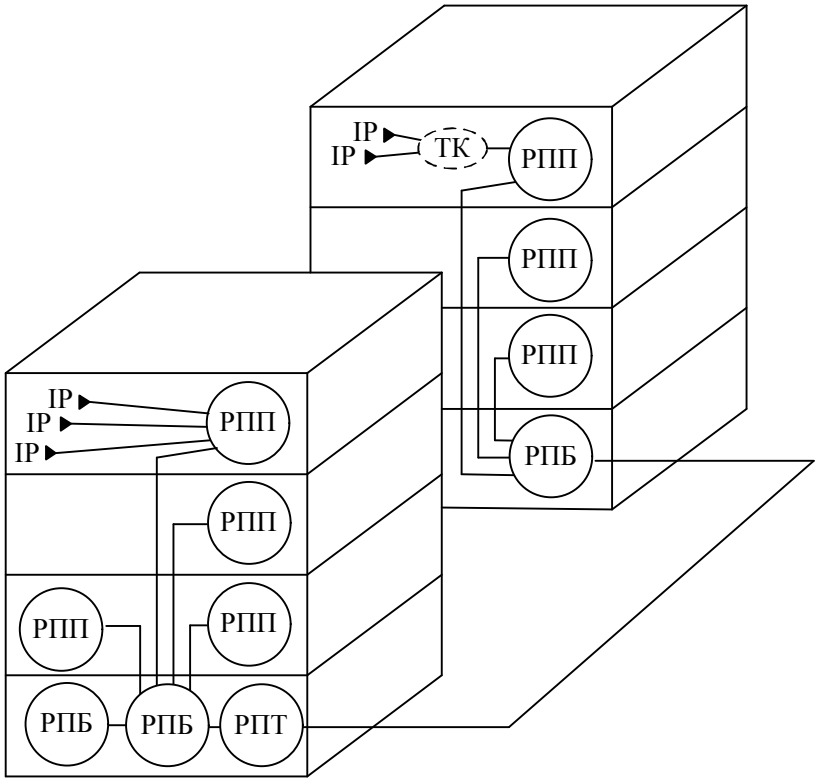


Рис. 2.9.2. Приклад структури СКС із прив'язкою до будівель

Технічні приміщення

Стандартом ISO/IEC 11801:2002 введені такі терміни, які визначають приміщення, необхідні при створенні СКС:

- *телекомунікаційна кімната (telecommunications room).* Це кімната, у якій розташовується пасивне комутаційне і з'єднуюче обладнання

розподільчих пристроїв. Вона повинна мати прямий доступ до "вищої" підсистеми СКС і повинна забезпечувати для елементів СКС все необхідне: відповідні площу, електроживлення, кліматичні умови, освітлення та ін. (У вітчизняній літературі таке приміщення часто називають "кросова");

- *кімната обладнання (equipment room)*. Це кімната, у якій окрім пасивних розподільчих пристроїв СКС ще перебуває активне обладнання інженерних систем, підключених до СКС (сервери та маршрутизатори ЛВС, телефонні станції та ін.). Кімнати обладнання експлуатуються відмінним від телекомунікаційних кімнат чином, що пояснюється складністю, великим обсягом і дорожнечею активного обладнання (у вітчизняній літературі таке приміщення часто називають "апаратна").

Якщо в приміщенні розташовано більше одного РПБ, то з огляду на великі розміри і важливість такого приміщення, воно також набуває більш високого статусу і вважається кімнатою обладнання. Її облаштування і експлуатація також проводяться відповідним чином.

Контрольні питання

1. Які основні етапи проектування мережі?
2. При створенні нової мережі які фактори повинні бути враховані?
3. Що таке СКС та ВКС?
4. Які переваги СКС Вам відомі?
5. Які підсистеми входять до СКС?
6. Які типи технічних приміщень Вам відомі?

ЛІТЕРАТУРА: [19, 22, 24, 28, 29, 37].

Тема 10. БЕЗПЕКА КОМП'ЮТЕРНИХ МЕРЕЖ

Мета теми – ознайомитись із основними загрозами, які існують для інформаційних систем та розглянути методи захисту від них.

Ключові поняття: мережевий екран, антивірус, шифрування інформації, системи виявлення і попередження вторгнень, сканери вразливостей.

Основи захисту інформації у комп'ютерних мережах

Мережеві технології у відриві від комплексного захисту інформації, яка передається мережевими каналами зв'язку, розглядати неможливо. Якщо раніше перенесення небезпечного програмного забезпечення (ПЗ) відбувалося в основному на таких носіях як дискети, оптичні диски тощо, то в умовах стрімкого розвитку Інтернету на перше місце виходить розповсюдження шкідливого програмного забез-

печення за допомогою комп'ютерної мережі. У першу чергу, через Інтернет.

У той же час на даному етапі розвитку інформаційних технологій атаки організуються не одинаками, створена ціла індустрія з багатомільйонним оборотом. Створюються "*бот-мережі"* (комп'ютери, на яких запущене автономне ПЗ – і які управляються віддалено), які в подальшому можуть продаватися. За допомогою заражених комп'ютерів можуть бути організовані *DDos-атаки*, розсилка спаму (небажаної пошти) або ж перебір можливих паролів на віддаленому сервері. Зважаючи на вищесказане, до організації захисту інформації потрібно підходити комплексно, не обмежуючись єдиним інструментом.

Розглядаючи безпеку передачі даних у мережі організації, слід виділити наступні рішення:

- антивіруси;
- мережеві екрани;
- системи виявлення і попередження вторгнень;
- сканери вразливостей;
- рішення, що попереджують витік інформації;
- контентні фільтри;
- інструменти резервного копіювання і відновлення інформації.

У той же час багато рішень пропонують захист в комплексі, тобто наприклад, мережеві екрани інтегрують в собі ще й захист від вірусів, а системи виявлення і попередження вторгнень є, як правило, міжмережевими екранами. Однак, напевно говорити, що дана система є міжмережевим екраном, до якої було інтегровано функції системи виявлення і попередження вторгнень, або навпаки, не можна без конкретного аналізу розвитку даної системи забезпечення захисту інформації. Розуміючи, що і захист інформації потребує комплексного підходу, і системи, як правило, інтегрують в собі декілька рішень захисту інформації, вважаємо за доцільне розглянути кожну із вищенаведених систем окремо, як закінчену систему. Це дозволить сформувати більш чітке уявлення щодо функцій, які виконує та чи інша система у комплексному захисті інформації організації.

Антивірусні рішення

Антивірусна програма (або просто *антивірус*) – це програма, яка призначена для знаходження небажаного ПЗ (сюди віднесемо комп'ютерні віруси, троянські програми, програми-шпигуни тощо), для лікування заражених файлів, а також попередження зараження інформаційної системи.

Часто все небажане ПЗ називають вірусами, що є не зовсім правильним. *Комп'ютерний вірус* – це різновид комп'ютерних програм, особливістю яких є здатність до розмноження (*самореплікація*). Також до небажаного ПЗ належать *троянські програми* – небажані програми, які проникають до системи під виглядом корисних (кодеку, різного роду корисного ПЗ тощо), та *шпигунське ПЗ* – це програмне забезпечення, яке інсталюється в інформаційну систему для повного або часткового контролю над нею без відповідної згоди на це користувача даної системи. Даний вид ПЗ визначають як несанкціоновано встановлений.

З початку створення антивірусних програмних засобів пройшло досить багато часу. На початкових етапах еволюціонування антивірусів існував поділ антивірусних програм на ті, що виявляли віруси під час сканування, ті що знаходилися постійно в оперативній пам'яті комп'ютера, не даючи, таким чином, провести зараження інформаційної системи. Також додатково потрібно було встановлювати ПЗ, яке покликане протидіяти шпигунським, троянським програмам тощо. Наприклад, Євгенієм Касперським у 1992 році була зроблена наступна класифікація антивірусних рішень:

- *сканери (або "поліфаги")* – виявляють наявність вірусу по базі сигнатур. Ефективність даних програм вимірюється актуальністю сигнатур, які зберігаються в базі даних;
- *ревізори* – запам'ятовують стан файлової системи, що дозволяє в подальшому робити аналіз наступних змін;
- *монітори* – виявляють потенційно небезпечні операції, видаючи запит на дозвіл або заборону такої операції;
- *вакцини* – змінюють кінцевий файл таким чином, щоб вірус думав, що файл вже заражений (у сучасних умовах з неймовірною кількістю вірусів даний підхід неактуальний).

На сьогодні всі сучасні антивіруси забезпечують постійний захист як від вірусів, так і від іншого небажаного ПЗ. Більше того, широко розповсюджені рішення, які дозволяють встановлювати більше одного антивірусного засобу (як правило, у складі міжмережевого екрану вже є вбудований антивірус, однак можна ще встановити інший, на вибір користувача). Самостійно встановлювати два і більше антивіруси в одну систему категорично забороняється, оскільки антивірусні рішення будуть сприйматися один одним, як комп'ютерний вірус.

Перші антивірусні програми з'явилися одразу після створення перших вірусів. Сьогодні розробкою даного виду ПЗ займаються такі виробники, як Kaspersky, Symantec, McAfee, Microsoft та багато інших. На ринку пропонується найрізноманітніше антивірусне ПЗ, від безкоштовних до дорогих корпоративних рішень (рис. 2.10.1).

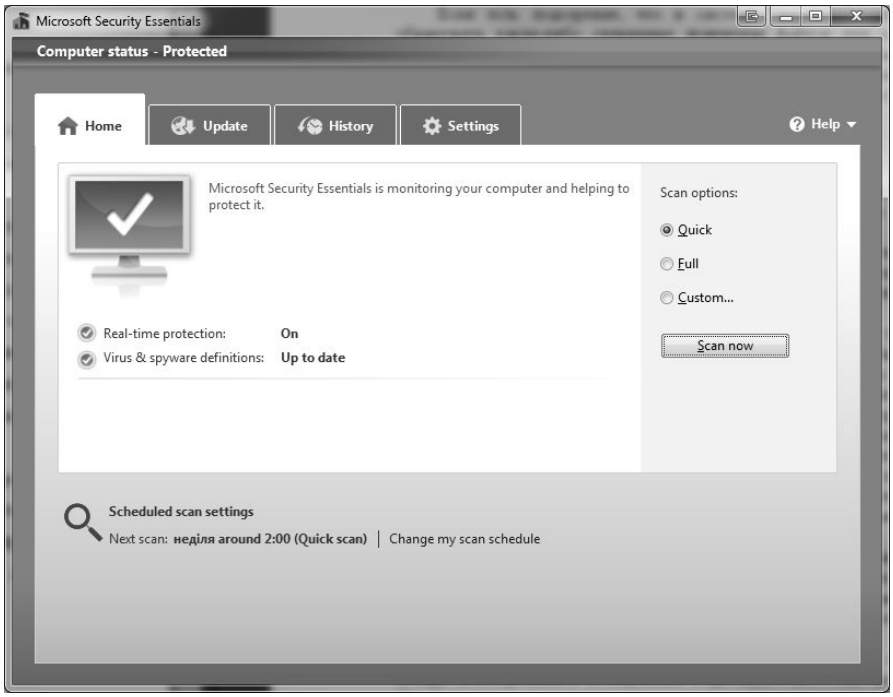


Рис. 2.10.1. Головне вікно безкоштовного антивірусу від Microsoft

Усі антивіруси можна розділити на:

- продукти для домашніх користувачів: власне антивіруси, комбіновані продукти (крім антивірусу присутній мережевий екран, антиспам тощо);
- корпоративні продукти: серверні антивіруси, антивіруси для робочих станцій.

Якщо говорити про класифікацію антивірусних програм, то можна її робити відповідно до визначального фактора. Наприклад, якщо вибрати ціну, то можна виділити: безкоштовні антивіруси, умовно безкоштовні, платні тощо.

Для виявлення і знешкодження небажаного ПЗ антивірусні програми використовують різні методи:

- відповідність вірусу в описі бази наявних сигнатур. Антивірусна програма шукає відповідність опису вірусу в базі сигнатур, яку має у своєму розпорядженні. Недоліком даного підходу можна назвати те, що таким методом не можна віднайти небажане ПЗ, опис якого не було додано до бази сигнатур;
- віднаходження неадекватної поведінки програм. Відслідковується поведінка програм, які працюють у системі, й у випадку небезпечної дії програми (наприклад, зміни виконуючого файлу) антивірус повідомляє про це користувача. Перевагою такого методу є можливість віднаходити небажане ПЗ, яке ще не було додано до бази да-

них сигнатур. Недоліком є ймовірність невірного спрацювання при певних режимах роботи користувача (наприклад, встановлення поновлень для ПЗ);

- емуляція поведінки ПЗ. Перед передачею прав на виконання безпосередньо ПЗ антивірус намагається провести емуляцію початку виконання. Якщо програма буде вести себе по іншому, вона буде вважатися шкідливою для системи. Даний метод також має недоліки у вигляді невірних спрацювань;
- "білий список". Дозволяється використовувати лише те ПЗ, яке безпосередньо дозволено в системі. Таким чином, у системі не буде виконуватися навіть ПЗ, яке не несе у собі загрози у вигляді вірусів чи іншого ПЗ. Даний підхід, як правило, використовують при корпоративному управлінні антивірусним ПЗ.

Хоча на комп'ютері, особливо на комп'ютері, який взаємодіє з іншими за допомогою мережі, повинно бути встановлене антивірусне ПЗ, слід чітко усвідомлювати, що жоден антивірус не зможе надати 100% захисту від небажаного ПЗ.

Мережеві екрани

Найбільш важливим засобом захисту мереж є мережеві екрани (або міжмережеві екрани, файрволи чи брандмауери) та проксі-сервери. Основна функція мережевого екрану – екранування мережевого трафіка з метою недопуску несанкціонованого доступу між комп'ютерними мережами. Проксі-сервери використовуються для обробки запитів користувачів із внутрішньої мережі та транслювання їх до зовнішньої мережі, і навпаки. У таких запитах, як правило, розрізняють мережі, що користуються довірою, та такі, що не користуються (наприклад, мережа Інтернет).

Мережевий екран – це програмне або апаратне рішення, яке здійснює контроль і фільтрацію мережевих пакетів, що проходять через нього на різних рівнях моделі OSI у відповідності до заданих правил.

Мережеві екрани надзвичайно популярні завдяки тим перевагам, які вони у собі несуть:

- вони є засобом реалізації корпоративних політик безпеки;
- мережеві екрани надають можливість обмежувати доступ до певних служб (наприклад, до служби telnet, яка непотрібна звичайним користувачам);
- мережевий екран можна використовувати як засіб аудиту. Збирати інформацію можна не лише про трафік, який пройшов, але і про той, який був заблокований, таким чином попереджаючи можливі майбутні атаки на систему.

Утім мережеві екрани, будучи лише ланкою у загальній системі захисту інформаційної системи, мають наступні недоліки:

- мережеві екрани не можуть блокувати небажану інформацію, яка потрапляє до інформаційної системи через авторизовані канали. Таким чином, якщо шпигунське ПЗ надійшло до системи через дозволений канал, воно не зможе бути зупинене мережевим екраном;
- ефективність мережевих екранів визначається ефективністю правил, які покладено в основу функціонування мережевого екрану. Тому потрібно підійти з усією відповідальністю до формулювання правил фільтрації трафіка;
- мережеві екрани не зможуть попередити атаки користувачів, які користуються авторизованими каналами інформації;
- мережеві екрани не зможуть протидіяти атакам, якщо є можливість пустити інформаційний потік в обхід екрану.

Розподіл мережевих екранів можна провести відповідно до класифікаційної ознаки, наприклад, відповідно до місця знаходження мережевого екрану в мережі, у залежності від розташування механізму контролю в моделі OSI чи в залежності від можливості слідкування за активними з'єднаннями.

Однією із найбільш поширених класифікацій є класифікація мережевих екранів відповідно до охвату територій, що контролюються:

1. *Прикладний шлюз* або *традиційний мережевий екран*. Це програмне або апаратне рішення, яке контролює як вхідні, так і вихідні потоки даних між підключеними мережами. Фактично при встановленні з'єднання користувача із мережею зовні проходять два з'єднання: одне із мережевим екраном, а інше – мережевого екрану з мережею зовні. Даний вид мережевих екранів ще називають *проксі-серверами* або *проксі-шлюзами*. У випадку здійснення атаки на систему користувача фактично атака буде здійснюватися на проксі-сервер. Утім поряд із перевагами в захисті інформації, проксі-сервери мають і недоліки, а саме: зменшення швидкодії, оскільки кожне з'єднання являє собою два з'єднання, та зменшення прозорості, коли деяке ПЗ не може повноцінно функціонувати в мережі.

2. *Пакетний фільтр* або *персональний мережевий екран.* Даний тип мережевих екранів встановлюється на кінцеві системи, і тому захищають вони лише систему, на якій встановлені, а не цілі мережі. Мережеві екрани цього типу здійснюють фільтрацію трафіка, базуючись на наступній інформації:

- IP-адреса джерела;
- IP-адреса одержувача;
- протокол, який використовується;
- вихідний порт;

- порт призначення;
- тип повідомлення.

Ефективність мережевих екранів вимірюється правильністю побудови правил, що в них покладені, тому при побудові правил потрібно дотримуватися наступних інструкцій:

- побудова правил повинна здійснюватися від найбільш конкретних до загальних. Оскільки перевірка йде за правилами до першої відповідності, то неправильна побудова правил може створити умови, коли більш загальний набір правил перекриє більш конкретні правила;
- розміщення правил, які використовуються найчастіше, повинно бути у верхній частині списку. Оскільки перевірка йде до першого збігу, то розміщення активних правил у кінці списку може суттєво зменшити швидкодію роботи інформаційної системи.

Сканери вразливостей

Сканери вразливостей – це програмні або апаратні рішення, які призначені для діагностики і моніторингу мережевих комп'ютерних систем. Вони дозволяють сканувати мережі, інформаційні системи та прикладні програми на предмет виявлення потенційних загроз у системі організації безпеки, оцінювати і знешкоджувати вразливості.

Типи сканерів вразливостей:

- сканери портів;
- сканери, які досліджують топологію комп'ютерної мережі;
- сканери, які досліджують вразливості мережевих сервісів;
- CGI-сканери, які дозволяють виявити вразливі скрипти.

Роботу сканера вразливостей можна розподілити на наступні кроки:

1. Виявлення активних IP-адрес, відкритих портів, активних операційних систем та прикладних програм.
2. Створення звіту з безпеки.
3. Спроба виявлення рівня можливого втручання до операційної системи чи прикладної програми.
4. Можливе використання вразливості для створення збою в системі (лише для шкідливих сканерів).

Говорячи про сканери вразливостей, слід зауважити, що вони можуть слугувати як інструментом виявлення загроз, так і інструментом злому інформаційної системи, тому четвертий крок використовують сканери, які створені для здійснення атаки на інформаційну систему.

До сканерів вразливостей належать наступні рішення: Microsoft Baseline Security Analyzer (MBSA), Security Administrator's Integrated Network Tool (SAINT), сканер вразливостей (веб-сервіс) (QualysGuard),

сканер для дослідження мережевих вразливостей (X-scan), оцінка вразливостей на рівні прикладних програм (ISS Internet Scanner) та інші.

Системи виявлення і попередження вторгнень

Система виявлення вторгнень (Intrusion Detection System) – це програмне або апаратне рішення, яке націлене на виявлення фактів неавторизованого доступу в інформаційну систему чи мережу та несанкціонованого керування ними, як правило, через Інтернет.

Архітектура систем виявлення вторгнень складається з:

- сенсорної підсистеми, яка направлена на збір даних в області інформаційної безпеки;
- підсистеми аналізу, яка виявляє підозрілі дії на основі даних, що були отримані із сенсорів;
- сховища, необхідного для зберігання первинної інформації, а також результатів аналізу;
- консолі керування даною системою.

Основними видами систем виявлення вторгнень є:

- мережева, яка відслідковує вторгнення, перевіряючи мережевий трафік, а також слідкує за декількома хостами. Мережева система виявлення вторгнень отримує доступ до мережевого трафіка, підключаючись до концентратора чи комутатора;
- система, основана на протоколі. Система, яка аналізує комунікаційні протоколи з пов'язаними системами чи користувачами. Для веб-сервера дана система виявлення вторгнень, як правило, слідкує за HTTP та HTTPS протоколами. Дана система повинна бути налаштованою так, щоб могла проглядати пакети ще до їх відправки в мережу;
- система, основана на прикладних протоколах. Система, яка слідкує і аналізує дані, які передаються з використанням специфічних протоколів прикладних програм;
- вузлова. Система, яка розташована на хості, відслідковує вторгнення, використовуючи аналіз системних викликів, модифікації файлів та інших джерел;
- гібридна. Система, яка включає більше одного підходу у розробці систем виявлення вторгнень.

Крім того, системи виявлення вторгнень можна розділити на пасивні і активні. У пасивній системі отримана в результаті аналізу інформація записується до спеціального архіву, а також відсилаються повідомлення адміністратору системи.

Якщо система виявлення вторгнень є активною, то вона має назву *система попередження вторгнень (Intrusion Prevention system – IPS)*. Даний тип систем не лише веде збір інформації щодо дій в системі,

але і здійснює активні дії, направлені на попередження можливих вторгнень до інформаційної системи. Дані дії можуть виконуватися як в автоматичному режимі, так і в ручному.

Системи виявлення і попередження вторгнень досить близькі за своєю сутністю з мережевими екранами. Більше того, деякі мережеві екрани виконують роль систем виявлення і попередження вторгнень. Основна ж відмінність між даними системами виявляється в тому, що мережевий екран відсікає неавторизований трафік, пропускаючи авторизований, та не займається слідкуванням за вторгненнями, які можуть бути всередині самої мережі. Система ж виявлення вторгнень навпаки пропускає трафік та аналізує його, подаючи сигнали у випадку підозрілої активності. Щодо наявних систем виявлення вторгнень можна назвати наступні: Snort NIDS, Endian Firewall, Tripwire, Untangle та інші.

Рішення попередження витоку інформації

Попередження витоку інформації (Data Leak Prevention – DLP) – це технології, які попереджують втечу конфіденційної інформації із інформаційної системи назовні, а також технічні засоби для попередження такого витоку.

Системи даного типу будуються на аналізі потоків даних, які пересікають периметр інформаційної системи. Якщо в інформаційному потоці віднаходиться конфіденційна інформація, то спрацьовує система захисту і потік блокується.

Розпізнавання інформації, витік якої є небажаним, може відбуватися двома основними методами: аналізом формальних ознак (наприклад, грифу документа, спеціально створених міток, порівнянням хеш-функції) та аналізом самого контенту. У першому випадку виключені неправильні спрацювання, однак потрібен час на проведення індексації документів, введення до них міток тощо. У другому випадку можливі невірні спрацювання, і якість системи буде залежати від правильності налаштованих фільтрів. Як правило, гарна система попередження витоку інформації повинна включати обидва методи перевірки контенту.

Системи попередження витоку інформації включають до свого складу компоненти мережевого рівня і модулі хоста. Компоненти мережевого рівня контролюють трафік, який перетинає кордони інформаційної системи через мережу. Компоненти мережевого рівня повинні бути встановлені на проксі-серверах, серверах електронної пошти, а також окремих серверах. Компоненти рівня хоста встановлюються на комп’ютери співробітників і контролюють шляхи запису інформації на носії, відслідковують встановлення неавторизованого ПЗ тощо.

Основною задачею систем попередження витоку інформації є недопущення витоку інформації з інформаційної системи. Крім основної задачі дана система повинна ще виконувати ряд другорядних задач:

- архівування повідомлень, які пересилаються. Архіви можуть знадобитися для подальшого розслідування можливих справ;
- попередження передачі зовні не лише конфіденційної інформації, але й іншої, яка є небажаною для компанії (наприклад, значних об'ємів, що може знизити продуктивність каналів чи збільшити оплату за використання Інтернету);
- попередження витоку інформації не лише зовні, а й із зовнішнього середовища до інформаційної системи;
- попередження використання співробітниками службових інформаційних ресурсів в особистих цілях;
- оптимізація загрузки каналів передачі інформації;
- контроль присутності співробітників на робочому місці.

Шифрування інформації

Шифрування – це спосіб перетворення відкритої інформації в закриту, і навпаки. Шифрування поділяється на процес зашифровування і розшифрування. При шифруванні інформації формується *ключ* – секретна інформація, яка використовується криптографічним алгоритмом шифрування. Використання криптографії при передачі важливої інформації практикувалося досить давно. Існують докази, що давні римляни використовували шифрування при передачі інформації кур'єрами на полі бою. Шифрування залишається одним з основних механізмів забезпечення захисту інформації завдяки тому, що за допомогою шифрування можна одразу забезпечити вирішення декількох задач в області захисту інформації. До цих задач належать:

- збереження конфіденційності. Інформація, яка була зашифрована залишається недоступною для сторонніх осіб (за умови належного зберігання ключа і використання крипостійкого алгоритму);
- збереження цілісності. Неможливо провести зміну даних несанкціоновано, оскільки для її зміни зашифровану інформацію потрібно спочатку розшифрувати;
- неможливість відмови від авторства. Завдяки наявності цифрового підпису й асиметричних методів шифрування інформації є можливість однозначно ідентифікувати автора повідомлення.

Шифрування інформації використовується в сучасному світі постійно: при авторизації користувачів на Інтернет порталах, при пересиланні електронної пошти і використанні цифрового підпису. Бази даних користувачів і їх паролі обов'язково повинні зберігатися в зашифрова-

ному вигляді, та навіть звичайний текст документа MS Word можна зашифрувати вбудованими засобами і встановити на нього пароль.

Існують два основні алгоритми шифрування інформації: *симетричний* і *асиметричний*, – у кожного є свої переваги і недоліки, а також область, де їх можна застосовувати. При використанні симетричного методу шифрування ключ для шифрування і для розшифровки інформації співпадає, тому він повинен зберігатися в секреті (рис. 2.10.2).

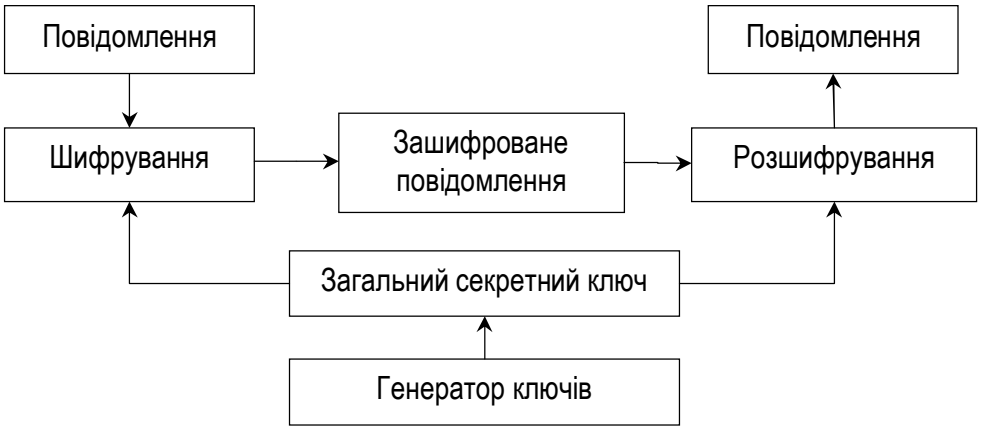


Рис. 2.10.2. Використання симетричного методу шифрування

До переваг симетричного методу шифрування можна віднести простоту реалізації та швидкість роботи симетричних алгоритмів. Однак, існують і недоліки, у першу чергу, проблема розповсюдження ключів, оскільки для розшифровки повідомлення потрібно мати ключ, аналогічний тому, яким дане повідомлення було зашифроване. Окрім того, за допомогою симетричних методів шифрування неможливо вирішити задачу щодо авторства повідомлення, оскільки неможливо однозначно виявити автора зашифрованої інформації.

Для вирішення задач, згаданих вище, використовуються асиметричні методи шифрування інформації. В асиметричних методах використовується пара ключів: один для шифрування, інший для розшифровки повідомлення. Ключ, за допомогою якого шифрується повідомлення, не є секретним, оскільки за допомогою нього не можна розшифрувати повідомлення, тому він називається *відкритим*. Разом із відкритим ключем формується секретний, який повинен зберігатися в секреті, оскільки він використовується для розшифровки повідомлень. Одним із відомих методів асиметричного шифрування є RSA, який використовує операції з великими простими числами та їх множенням. Загальний принцип роботи асиметричного методу шифрування наведений на рис. 2.10.3.

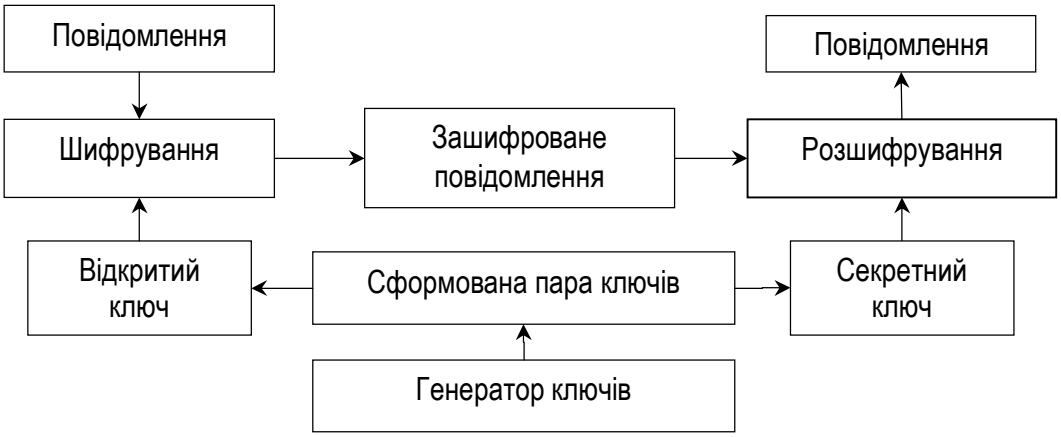


Рис. 2.10.3. Використання асиметричного алгоритму шифрування

Асиметричний метод шифрування вирішує недоліки, які існують при використанні симетричних методів, однак у асиметричних методів існує один значний недолік, а саме низька швидкодія. Для усунення цього одного недоліку асиметричних методів використовують досить простий і у той же час зручний спосіб: основне повідомлення шифрується за допомогою швидкого симетричного методу, а його ключ – за допомогою асиметричного алгоритму, таким чином можна шифрувати значні обсяги інформації і передавати її. У той же час гарантується достовірність авторства.

Контрольні питання

1. Які існують види небажаного ПЗ і чим вони відрізняються?
2. Які основні методи виявлення небажаного ПЗ притаманні антивірусним програмам?
3. Які переваги та недоліки у сфері захисту інформації притаманні мережевим екранам?
4. Які основні принципи роботи сканерів вразливостей?
5. Яке призначення систем виявлення і попередження вторгнень?
6. Яке призначення рішень попередження витоку інформації?
7. Які основні алгоритми шифрування інформації Ви знаєте, у чому їх переваги і недоліки?

ЛІТЕРАТУРА: [21, 27].

3. МЕТОДИЧНІ ВКАЗІВКИ ЩОДО ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ

Лабораторна робота № 1
Тема “РОЗРОБКА ПЛАНУ ПРИМІЩЕНЬ КОМЕРЦІЙНОГО БАНКУ І ПЛАНУ КОМП’ЮТЕРНОЇ МЕРЕЖІ”

Мета роботи: отримати навички проектування плану приміщень комерційних банків і плану комп’ютерної мережі з використанням інструментального засобу Microsoft Office Visio 2007.

Методичні вказівки

Короткий опис роботи з інструментальним засобом Microsoft Office Visio 2007

Інструментальний засіб Microsoft Office Visio 2007 призначений для створення різного виду документів (креслень): схеми комп’ютерних мереж, планів офісних приміщень, блок-схем тощо.

Створення документа. Існує багато типів документів Microsoft Office Visio 2007, але для створення всіх документів можна скористатися трьома основними діями:

1. Вибір та відкриття шаблону.
2. Перетаскування і з’єднання фігур.
3. Додавання тексту до фігур.

Для вибору і відкриття шаблону необхідно *(дія 1)*:

- відкрити програму Visio 2007;
- у списку категорій шаблонів вибрати елемент “блок-схема”;
- у діалоговому вікні блок-схеми у області готових шаблонів двічі клацнути на елемент *Простая блок-схема* (рис. 3.1.1).

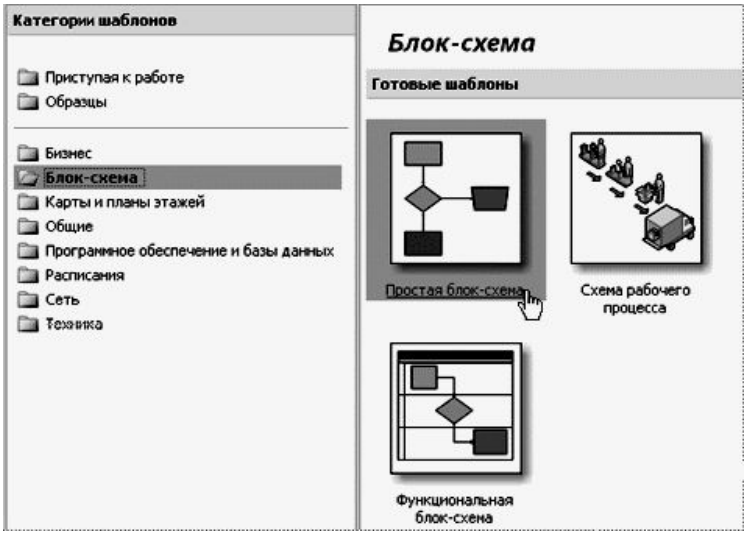


Рис. 3.1.1. Категорії шаблонів

Після відкриття шаблону будуть відкриті необхідні колекції фігур, які називаються наборами елементів. До наборів елементів, які відкриваються разом із шаблоном *Простая блок-схема*, належать стрілки, фонові малюнки, фігури простої блок-схеми (рис. 3.1.2).

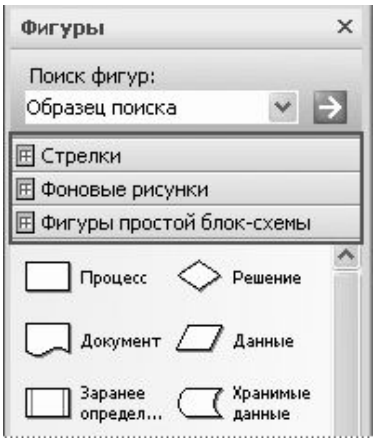
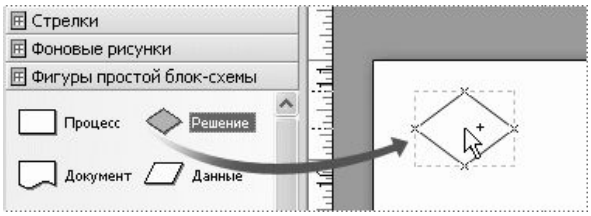


Рис. 3.1.2. Колекція фігур

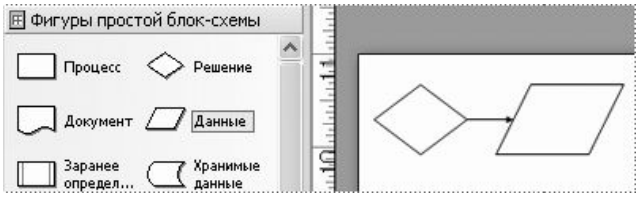
Для перетаскування та з'єднання фігур необхідно *(дія 2)* перетягнути фігури з наборів елементів у порожній документ і з'єднати їх один з одним. Є багато способів зробити це, але найчастіше використовують найшвидший спосіб – автоз'єднання. Для цього слід перетягнути нову фігуру з колекції в документ і розташувати поруч із тією, з якою необхідно зробити з'єднання. Процедура автоз'єднання представлена в табл. 3.1.1.

Таблиця 3.1.1

Процедура автоз'єднання

Дія	Візуалізація дії
1. Перетягніть першу фігуру із набору елементів фігур простої блок-схеми на сторінку документу і відпустіть кнопку миші	
2. Перетягніть другу фігуру у верхню частину першої. З'являться блакитні стрілки. При цьому кнопка миші повинна залишатися натиснутою	
3. Утримуючи натиснутою кнопку миші, перетягніть вказівник миші на блакитну стрілку, яка показує місце, куди необхідно помістити другу фігуру	

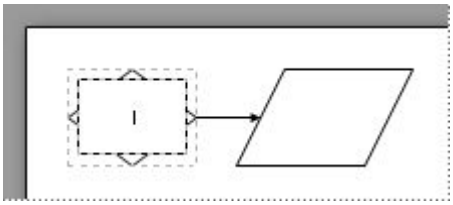
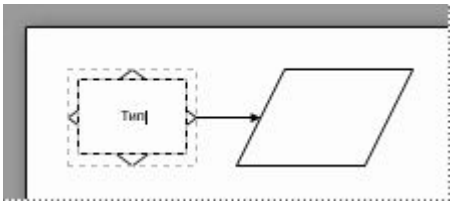
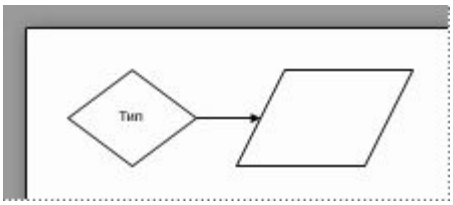
Продовж. табл. 3.1.1

Дія	Візуалізація дії
4. Відпустіть кнопку миші. Тепер фігури з'єднані і перша фігура показує на другу	

При додаванні тексту в фігурі *(дія 3)* необхідно провести процедуру, представлену в табл. 3.1.2.

Таблиця 3.1.2

Процедура додавання тексту в фігуру

Дія	Візуалізація дії
1. Двічі клацніть на фігуру	
2. Введіть текст	
3. Після завершення вводу тексту клацніть на пустому місці сторінки документа	

Процедура створення робочих місць. Для створення планів окремих офісів, включаючи стіни, електрообладнання, плани секцій необхідно:

1. У меню *Файл* послідовно вибрати команди *Создать*, *Карты и планы этажей*, а потім – команду *План рабочих мест*.
2. Створити структуру стін для плану офісів одним із наступних способів:
   - скористатися фігурами приміщень. Для цього слід перетягнути на сторінку документа одну з фігур *Комната*. Далі за необхідності змінити розмір приміщення, перетягнувши керуючі маркери ◇ і маркери виділення ■ на окремі стіни;

- скористатися фігурами стін. Для цього слід перетягнути фігури *Стена* на сторінку документа. При необхідності слід змінити розмір стіни, перетягнувши кінцеву точку (або). Для з'єднання стін необхідно перетягнути кінцеву точку однієї стіни до будь-якої точки іншої стіни. Коли стіни будуть приклеєні, кінцеві точки стануть червоними.

3. Додати фігури вікон і дверей. Для цього необхідно:
   - перетягнути на сторінку документа фігури вікон і дверей і помістити їх на стіни. Слід зазначити, що двері та вікна автоматично будуть повернені для вирівнювання уздовж стін і приклеєні до них; оберуть товщину стін; будуть переміщатися зі стінами при зміні їх положення;
   - для зміни напрямку відкриття дверей і вікон слід виділити відповідну фігуру або фігури. Необхідно клацнути на них правою кнопкою миші, а потім у контекстному меню вибрати потрібну команду напрямку відкриття. Як показано на наступному малюнку, вікно або двері на стіні будуть вирівняні уздовж стіни, а двері або вікно на вигнутій стіні будуть повернені для вирівнювання уздовж стіни (рис. 3.1.3).

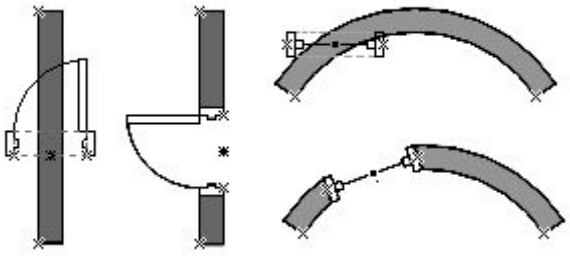


Рис. 3.1.3. Зміна положення дверей і вікон

4. Додати фігури, що позначають різне електрообладнання. Для цього необхідно:
   - з набору елементів *Офисное оборудование* перетягнути на стіни фігури електрообладнання. Коли з'явиться червоний квадрат , який позначає приклеєну до стіни фігуру, відпустити кнопку миші;
   - для зміни орієнтації електрообладнання щодо стіни слід клацнути правою кнопкою миші фігуру, а потім у контекстному меню вибирати команду *Изменить ориентацию*.
5. Додати секції, офісні меблі і обладнання, перетягнувши відповідні фігури на сторінку документа.

Приклад робочого місця представлений на рис. 3.1.4.

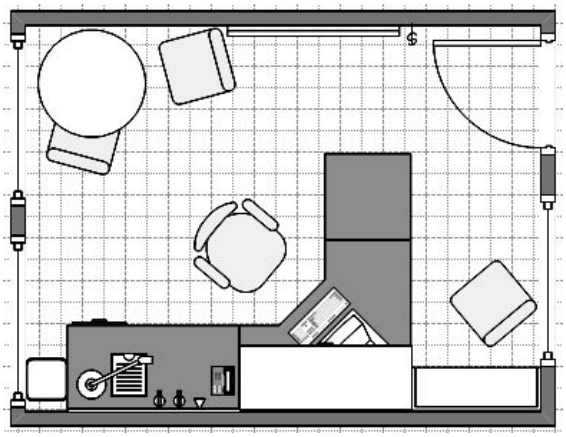


Рис. 3.1.4. Приклад робочого місця

При проектуванні комп'ютерних мереж в офісних приміщеннях використовують кабельні лотки та пластикові короби. *Кабельний лоток* – це відкрита конструкція, призначена для монтажу дротів і кабелів. *Короб кабельний* – конструкція із пластмаси для монтажу кабельних мереж усередині приміщення. Пластикові короби поділяються на кілька основних видів:

- *кабельний канал (кабель-канал)* – має просту конструкцію, він досить дешевий, деякі моделі дозволяють встановлювати розетки всередині кабель-каналу;
- *парапетні короби* – встановлюються на рівні робочого місця, внутрішній простір такого короба розділений на секції, він має подвійну стінку, і практично всі види парапетного короба підтримують монтаж розеток;
- *короб на підлогу* – короб для монтажу на підлогу, має посилену конструкцію та стійку до стирання поверхню.

Вимоги до серверної кімнати

Серверна кімната – приміщення для великого телекомунікаційного або серверного обладнання. Розміри серверної повинні відповідати вимогам до розташовуваного в ній обладнання. Якщо такі дані на момент вибору приміщення відсутні, розрахунки ведуться, виходячи із площі робочих місць, що обслуговуються: на кожні її 10 м^2 приймаються 0,07 м^2 для серверної. Мінімальна площа апаратної приймається 14 м^2.

Серверна кімната повинна розташовуватися в приміщенні, яке не має зовнішніх стін будинку. Для забезпечення катастрофостійкості приміщень критичного електронного, електричного або механічного обладнання та комп'ютерів дані приміщення не допускається розміщати у підвальних поверхах або нижче очікуваного рівня поводкових

вод, і на верхніх поверхах будинку, оскільки вони сильніше інших страждають у випадку пожежі.

Конструкція стін приміщення повинна бути герметичною, при цьому стіни та двері повинні мати вогнестійкість не менш 45 хвилин, а міжповерхові перекриття, окрім цього, повинні мати гідроізоляцію. Ширина дверей у серверну повинна бути не менш 910 мм, висота – 2000 мм. Конструкція дверей має певні обмеження: полотно повинно відкриватися назовні на 180 градусів, а дверна коробка не повинна мати порогу. При використанні в серверній великогабаритного обладнання передбачається встановлення двостулкових дверей. Для забезпечення герметичності в конструкції дверей повинна бути ущільнювальна прокладка, а для підвищення рівня захисту від злому необхідно передбачити протиз'ємне пристосування.

У серверній не повинно бути вікон. Обов'язковою умовою в цьому приміщенні є наявність фальшпідлоги, що витримує навантаження від обладнання, що встановлюється, і працюючих з ним людей. Рекомендована відстань між плитою на підлозі та фальшпідлогою – 400 мм, при цьому просвіт між фальшпідлогою і фальшстелею повинен бути не менш 2440 мм. Фальшпідлогу рекомендується робити з легкознімних модулів. Матеріал, із якого вона виготовлена, повинен бути міцним, зносостійким, мати низьку займистість і електричний опір відносно землі від 1 до 20 Ом. Використання килимових покриттів у таких приміщеннях суворо заборонене. Перекриття під фальшпідлогою повинне бути герметизованим або пофарбованим.

Нумерація (маркування) розеток

Усі розетки в комп'ютерній мережі повинні бути пронумеровані. Причому номер розетки повинен бути зазначений (приклеєний, підписаний) безпосередньо поруч із розеткою. Для кожного користувача комп'ютерної мережі повинні бути зарезервовані 2 розетки: комп'ютерна – для підключення комп'ютера користувача до комп'ютерної мережі та телефонна – для підключення телефону. Правила нумерації розеток не регламентуються, але слід підкреслити, що кожна розетка повинна мати свій унікальний номер, а пошук фізичного розташування розетки не повинен бути складним. Пропонується наступна складена нумерація розеток – 01-01-К01:

- перша і друга цифри – номер поверху;
- третя та четверта цифри – номер кімнати;
- п'ятий символ – тип розетки (К – комп'ютерна, Т – телефонна);
- шоста і сьома цифри – порядковий номер розетки.

Приклад нумерації розеток зображений на рис 3.1.6.

Типи кабельних сегментів

При проектуванні комп'ютерної мережі необхідно враховувати характеристики кабельних сегментів. *Кабельний сегмент* – відрізок кабелю або ланцюг відрізків кабелів, електрично (оптично) з'єднаних один з одним, що забезпечують з'єднання двох або більше вузлів мережі. Особливо важливо враховувати довжину кабельного сегмента. В табл. 3.1.3 надані основні характеристики кабельних сегментів.

Таблиця 3.1.3

Характеристики кабельних сегментів

Стандарт	Швидкість передачі даних	Тип кабелю, що використовується	Максимальна довжина сегмента
Ethernet 10Base-2	10 Мбіт/с	тонкий коаксіальний	185 м.
Ethernet 10Base-5	10 Мбіт/с	товстий коаксіальний	500 м.
Ethernet 10Base-F	10 Мбіт/с	волоконно-оптичний	2 км
Ethernet 10Base-T	10 Мбіт/с	вита пара	100 м.
Ethernet 100Base-FX	100 Мбіт/с	волоконно-оптичний	2000 м.
Ethernet 100Base-T	100 Мбіт/с	вита пара	100 м.
Ethernet 100Base-T2	100 Мбіт/с	UTP 3	100 м.
Ethernet 100Base-T4	100 Мбіт/с	UTP5, STP	100 м.
Ethernet 1000Base-CX	1000 Мбіт/с	STP	25 м.
Ethernet 1000Base-LX	1000 Мбіт/с	волоконно-оптичний	одномод. 5000 м. багатомод. 550 м.
Ethernet 1000Base-T	1000 Мбіт/с	UTP 5	100 м.

Завдання до роботи

Необхідно спроектувати план поверху комерційного банку та план комп'ютерної мережі. Вихідними даними для цього є: кількість кімнат на поверсі комерційного банку, робочі місця користувачів комп'ютерної мережі та розподіл робочих місць у комерційному банку (табл. 3.1.4).

На основі вихідних даних необхідно спроектувати план одного поверху комерційного банку, враховуючи, що одна з кімнат поверху комерційного банку повинна бути серверною кімнатою з одним робочим місцем для адміністратора мережі (серверна кімната входить у перелік кімнат з вихідних даних). Також необхідно врахувати всі вимоги щодо розташування серверної кімнати (двері, вікна тощо).

Таблиця 3.1.4

Вихідні дані

Вихідні дані							
№ кімнати	Кількість робочих місць	№ кімнати	Кількість робочих місць	№ кімнати	Кількість робочих місць	№ кімнати	Кількість робочих місць
Варіант № 1		**Варіант № 2**		**Варіант № 3**		**Варіант № 4**	
1	7	1	1	1	4	1	4
2	6	2	6	2	8	2	8
3	9	3	7	3	10	3	8
4	5	4	10	4	3	4	3
5	5	5	5	5	5	5	5
6	2	6	7	6	4	6	8
7	1			7	1	7	1
Варіант № 5		**Варіант № 6**		**Варіант № 7**		**Варіант № 8**	
1	5	1	5	1	25	1	30
2	8	2	7	2	5	2	3
3	10	3	12	3	1	3	2
4	5	4	1	4	7	4	1
5	5	5	9	5	15	5	1
6	3	6	5	6	3	6	4
7	1	7	1				
Варіант № 9		**Варіант № 10**		**Варіант № 11**		**Варіант № 12**	
1	1	1	3	1	1	1	10
2	7	2	1	2	3	2	5
3	10	3	5	3	10	3	1
4	12	4	7	4	7	4	8
5	3	5	9	5	14	5	9
6	4	6	5	6	5	6	4
7	6	7	8	7	6	7	4
8	2	8	1				

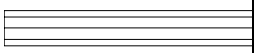
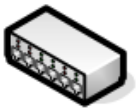
При проектуванні поверху офісного будинку необхідно визначити робочі місця для персоналу, оснащені офісними меблями й персональними комп'ютерами. Також необхідно визначити можливе місце розташування для монтажу кабелю комп'ютерної мережі – місця для коробів, лотків і т.д.; визначити місце розташування для мережевого обладнання; визначити місце розташування телефонних і комп'ютерних розеток на робочих місцях користувачів і пронумерувати їх.

План виконання роботи

1. Визначити форму периметру зовнішніх несучих стін будинку.
2. Спроектувати план поверху офісного будинку, тобто визначити розташування кімнат на поверсі офісного будинку. Необхідно також підписати номери кімнат. Варто пам'ятати, що на поверсі повинні бути присутніми коридори для переміщень, серверна кімната, місця для комунікацій. Приклад зображений на рис. 3.1.5.
3. Показати розміри кімнат. Це необхідно для визначення порядку довжин кабельних сегментів від серверної до офісних кімнат.
4. Ґрунтуючись на вихідних даних, визначити робочі місця користувачів комп'ютерної мережі. Для цього необхідно використовувати рекомендовані елементи Microsoft Office Visio 2007: столи, стільці, комп'ютери і т.д. (табл. 3.1.5).

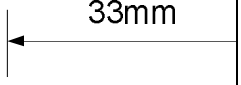
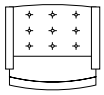
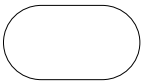
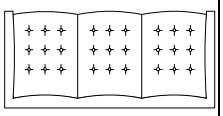
Таблиця 3.1.5

Рекомендовані елементи Visio

Піктограма	Назва об'єкта	Піктограма	Назва об'єкта
	"Кабельный лоток" (Tray track)		"Персональный компьютер" (PC)
	"Переходник к кабельному лотку" (Track comer)		"Коммутатор" (Switch)
	"Концовка кабельного лотка" (Track end-bevel)		"Маршрутизатор" (Router)
	"Кабельный короб" (Cable tray/spacer)		"Файловый сервер" (File server)

	“Стена” (Wall)		“Сервер баз данных” (Database server)

Продовж. табл. 3.1.5

Піктограма	Назва об’єкта	Піктограма	Назва об’єкта
	“Двойная дверь” (Double door)		“Веб сервер” (Web server)
	“Окно” (Window)		“Почтовый сервер” (Email server)
	“Горизонтальные размеры” (Dimensioning horizontal)		“Кресло с 2-мя ручками” (2-arm seat module)
	“Вертикальные размеры” (Dimensioning vertical)		“Стол” (Racetrack table)
	“Небольшое растение” (Small plant)		“Диван” (Sofa)
	“Перегородка” (Panel)		“Офисный стул” (Desk chair)
	“Круговая перегородка” (Curved panel)		

5. Визначити місце розташування коробів, лотків, телефонних і комп’ютерних мережевих розеток. Короби, лотки й розетки необхідно пронумерувати. Приклад зображений на рис. 3.1.6.
6. Заповнити кабельний журнал, у якому необхідно вказати відповідність мережевого обладнання, порту мережевого обладнання, мережевої комп’ютерної розетки, номера кімнати й ім’я комп’ютера. Приклад кабельного журналу представлено в табл. 3.1.6 (журнал

заповнений відповідно до проекту комп'ютерної мережі, представленого на рис. 3.1.6).

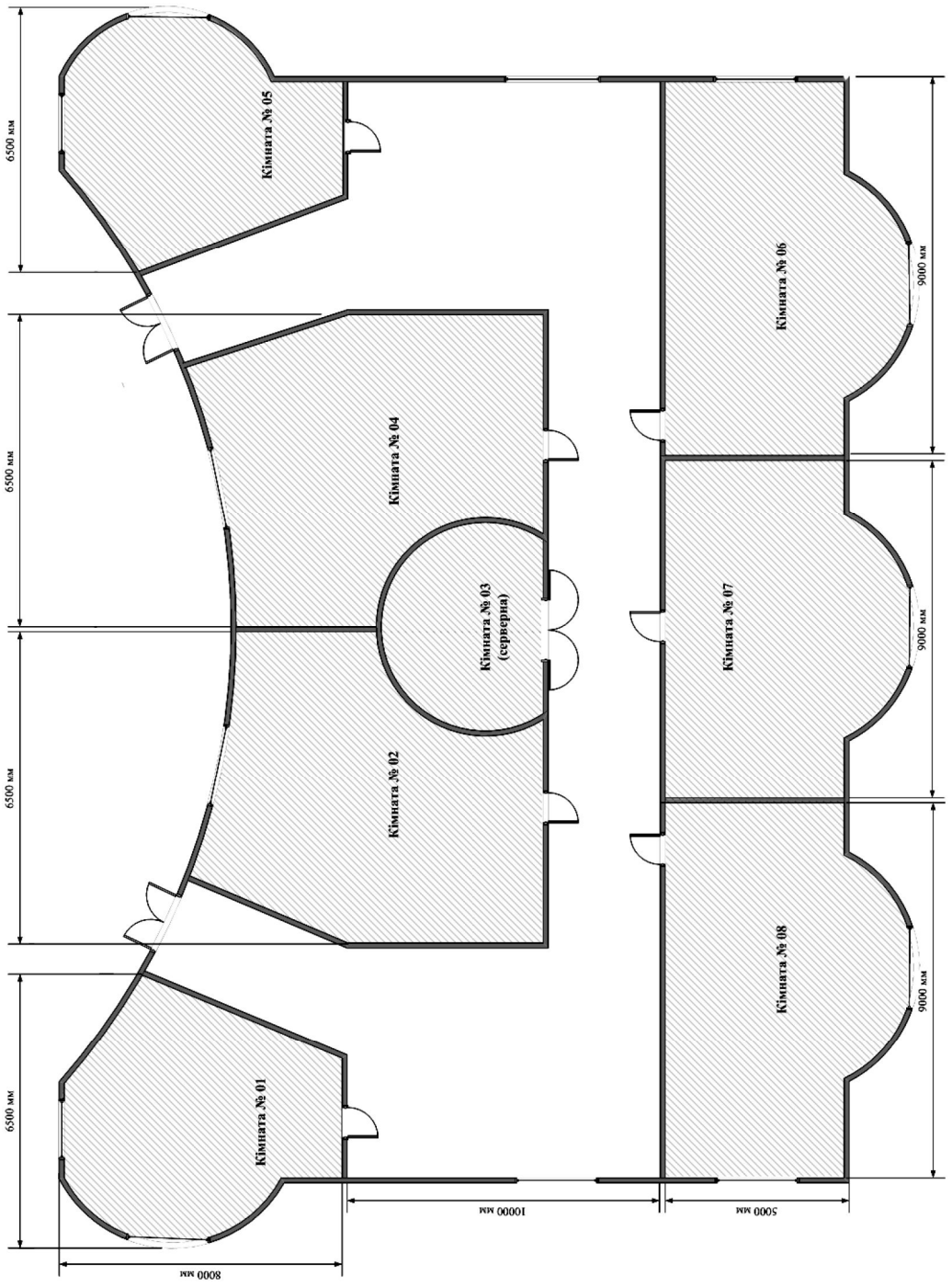


Рис. 3.1.5. План поверху комерційного банку

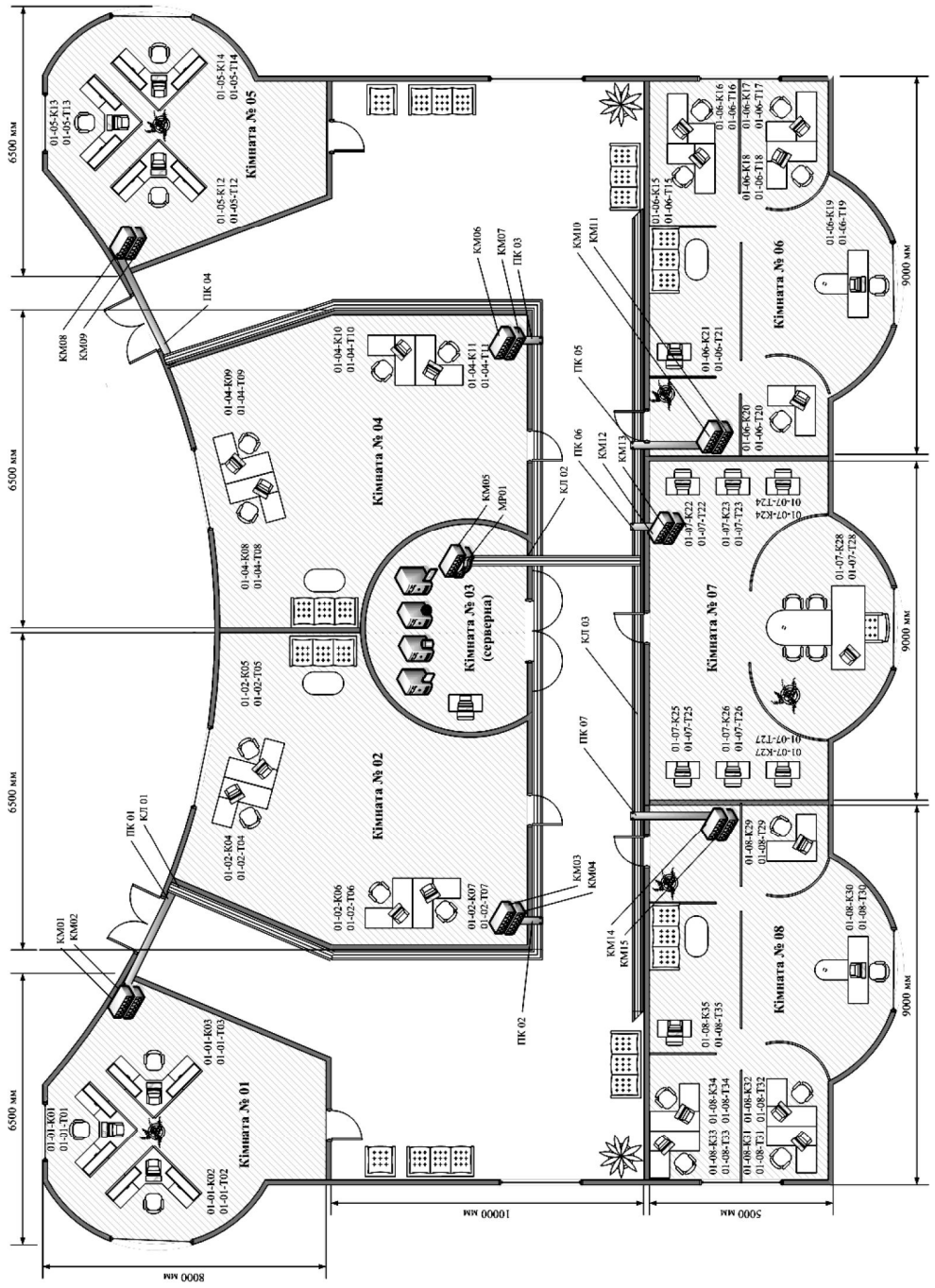


Рис. 3.1.6. План кімнат, меблів і елементів комп'ютерної мережі на поверсі комерційного банку

Таблиця 3.1.6

Приклад кабельного журналу

№	Назва пристрою	№ порту	№ розетки	Ім'я комп'ютера	№ кімнати
	КМ01	01	01-01-К01	01-01-01	01
		02	01-01-К02	01-01-02	
		03	01-01-К03	01-01-03	
	КМ02	01	01-01-Т01	01-01-01	
		02	01-01-Т02	01-01-02	
		03	01-01-Т03	01-01-03	
	КМ03	01	01-02-К04	01-02-04	02
		02	01-02-К05	01-02-05	
		03	01-02-К06	01-02-06	
		04	01-02-К07	01-02-07	
	КМ04	01	01-02-Т04	01-02-04	
		02	01-02-Т05	01-02-05	
		03	01-02-Т06	01-02-06	
		04	01-02-Т07	01-02-07	
	МР01	01	01-05-К36	01-05-36	03
	КМ05	01	01-05-Т36	01-05-36	
	КМ06	01	01-04-К08	01-04-08	04
		02	01-04-К09	01-04-09	
		03	01-04-К10	01-04-10	
		04	01-04-К11	01-04-11	
	КМ07	01	01-04-Т08	01-04-08	
		02	01-04-Т09	01-04-09	
		03	01-04-Т10	01-04-10	
		04	01-04-Т11	01-04-11	
	КМ08	01	01-05-К12	01-05-12	05
		02	01-05-К13	01-05-13	
		03	01-05-К14	01-05-14	
	КМ09	01	01-05-Т12	01-05-12	
		02	01-05-Т13	01-05-13	
		03	01-05-Т14	01-05-14	
	КМ10	01	01-06-К15	01-06-15	06
		02	01-06-К16	01-06-16	
		03	01-06-К17	01-06-17	
		04	01-06-К18	01-06-18	
		05	01-06-К19	01-06-19	
		06	01-06-К20	01-06-20	
		07	01-06-К21	01-06-21	

Продовж. табл. 3.1.6

№	Назва пристрою	№ порту	№ розетки	Ім'я комп'ютера	№ кімнати
	КМ11	01	01-06-Т15	01-06-15	
		02	01-06-Т16	01-06-16	
		03	01-06-Т17	01-06-17	
		04	01-06-Т18	01-06-18	
		05	01-06-Т19	01-06-19	
		06	01-06-Т20	01-06-20	
		07	01-06-Т21	01-06-21	
	КМ12	01	01-07-К22	01-07-22	07
		02	01-07-К23	01-07-23	
		03	01-07-К24	01-07-24	
		04	01-07-К25	01-07-25	
		05	01-07-К26	01-07-26	
		06	01-07-К27	01-07-27	
		07	01-07-К28	01-07-28	
	КМ13	01	01-07-Т22	01-07-22	
		02	01-07-Т23	01-07-23	
		03	01-07-Т24	01-07-24	
		04	01-07-Т25	01-07-25	
		05	01-07-Т26	01-07-26	
		06	01-07-Т27	01-07-27	
		07	01-07-Т28	01-07-28	
	КМ14	01	01-08-К29	01-08-29	08
		02	01-08-К30	01-08-30	
		03	01-08-К31	01-08-31	
		04	01-08-К32	01-08-32	
		05	01-08-К33	01-08-33	
		06	01-08-К34	01-08-34	
		07	01-08-К35	01-08-35	
	КМ15	01	01-08-Т29	01-08-29	
		02	01-08-Т30	01-08-30	
		03	01-08-Т31	01-08-31	
		04	01-08-Т32	01-08-32	
		05	01-08-Т33	01-08-33	
		06	01-08-Т34	01-08-34	
		07	01-08-Т35	01-08-35	

Питання до захисту роботи

1. Перерахуйте основні етапи створення документа у Visio 2007.
2. Назвіть основні вимоги до створення серверної кімнати.
3. Яким чином нумеруються комп'ютерні і телефонні розетки у комп'ютерній мережі?
4. Перерахуйте основні характеристики типів кабельних сегментів.
5. З якою метою необхідно вказувати розміри кімнат на плані поверху?
6. Що таке кабельний лоток і пластиковий короб?
7. Що входить до робочого місця користувача комп'ютерної мережі?

ЛІТЕРАТУРА: [16, 20, 23, 28, 29].

Лабораторна робота № 2
Тема "ПРОЕКТУВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ КОМЕРЦІЙНОГО БАНКУ НА ОСНОВІ ТЕХНОЛОГІЙ FAST ETHERNET, TOKEN RING І FDDI"

Мета роботи: отримати навички проектування комп'ютерних мереж на основі технологій Fast Ethernet, Token Ring і FDDI.

Методичні вказівки

Дана лабораторна робота повинна бути виконана в інструментальному середовищі, яке підтримує проектування комп'ютерної мережі з використанням реального обладнання, підтримувати різні технології побудови комп'ютерних мереж, а також проводити моделювання роботи комп'ютерної мережі та здійснювати виміри технічних параметрів роботи комп'ютерної мережі під час моделювання її роботи.

Як інструментальне середовище проектування комп'ютерної мережі пропонується використовувати NetCracker Professional.

Короткий огляд графічного інтерфейсу

Основні команди меню "File" (Файл)

Це меню призначене для виконання команд, які управляють файлами проекту мережі (табл. 3.2.1).

Таблиця 3.2.1

Основні команди меню "Файл"

Опція меню	Іконка	Опис
[1]New		Створює новий проект і відкриває вікно Site, помічене вершиною (Top)
[1]Open		Відкривається існуючий файл проекту NetCracker

Продовж. табл. 3.2.1

Опція меню	Іконка	Опис
[2]Close		Закривається файл проекту
2Save		Зберігається файл проекту
[2]Save As		Зберігає існуючий проектний файл і призначає нове ім'я файлу або зберігає новий проектний файл
[2]Print		Відображає вибране вікно сайту у тому вигляді, як воно буде надруковано
[2]Print		Друкує проектний файл на встановленому принтері
[1] MRU1,MRU2, MRU3, MRU4		Відкриває чотири останні використані (MRU) проектні файли
[1] Exit		Вихід із програмного середовища

[1] Ця команда відображається, коли проект закритий і не відображається у вікні проектної області.

[2] Ця команда відображається, коли проект відкритий і відображається у вікні проектної області.

Основні команди меню "Edit" (Редагування)

Це меню призначене для використання команди редагування зображенн пристроїв, які поміщені до проектної області (табл. 3.2.2).

Таблиця 3.2.2

Основні команди Меню "Edit"

Опція меню	Іконка	Опис
Cut		Вирізає вибраний об'єкт
Copy		Копіює вибраний об'єкт до буфера обміну
Paste		Вставляє елемент, скопійований до буфера обміну, в проектну область вікна
Delete		Видаляє вибраний об'єкт
Duplicate		Дублює вибраний об'єкт, враховуючи усі вказані параметри налаштування і властивості
Replicate		Копіює вибраний об'єкт вказану кількість разів
Select All		Вибирає всі об'єкти у робочому вікні Site

Основні команди меню “View” (Вид)

Меню “Вид” (табл. 3.2.3) призначене для зміни виду поточного вікна на дисплеї, відображення або приховання інструментальних панелей, браузерів і областей вікон, вибору типу браузера для відображення, визначення характеристики типу пакета.

Таблиця 3.2.3

Основні команди Меню “View”

Опція меню	Підменю	Іконка	Опис
Zoom			Змінює розмір вікна дисплею
	Zoom in		Збільшує масштаб параметрів зображення
	Zoom out		Зменшує масштаб параметрів зображення
	Zoom to page		Відображає проект в одному вікні
	Zoom 1:1		Відображає вибраний зміст вікна у 100 %-му масштабі
	Zoom one side		Змінює розмір вікна в одному напрямку
	Zoom undo change		Повертається до попередніх параметрів налаштування дисплею
Bars			Відображає або приховує інструментальні панелі
	Standard		Відображає або приховує інструментальну панель *Standard*
	Zoom		Відображає або приховує інструментальну панель *Zoom*
	Drawing		Відображає або приховує інструментальну панель *Drawing*
	Modes		Відображає або приховує інструментальну панель *Modes*
	Control		Відображає або приховує інструментальну панель *Control*
	Database		Відображає або приховує інструментальну панель *Database*
	Browser Pane		Відображає або приховує інструментальну панель браузера
	Image Pane		Відображає або приховує область вікна зображення

Продовж. табл. 3.2.3

Опції меню	Підменю	Іконка	Опис
Status bar			Відображає або приховує рядок стану
Image Pane			Визначає розмір і рівень значків пристрою в області вікна зображення
	Large icons		Відображає великі значки пристрою в області вікна зображення
	Small icons		Відображає маленькі значки пристрою в області вікна зображення
	List		Відображає значки пристрою в області вікна зображення в форматі списку
Full Screen			Відображає вікно Site у його максимальному виді та без інтерфейсу прикладної програми NetCracker
Legends			Відображає діалог легенд
Database Browser			Відображає бази даних браузера NetCracker
Project Hierarchy			Відображає ієрархію браузера NetCracker
Compatible Components			Відображає вид пошуку браузера NetCracker

Основні команди меню "Sites" (Сайти)

Дане меню (табл. 3.2.4) призначене для визначення характеристики дисплея рівня сайту, зміни назви (імені) сайту, визначення, яким чином ділити окремий сайт для друку на багатьох сторінках, зміни (заміни) режиму Netcracker, вибору інструмента для малювання.

Таблиця 3.2.4

Основні команди Меню "Sites"

Опції меню	Підменю	Іконка	Призначення
Site Setup			Відображає діалог налаштування сайту
Modes			Змінює вибраний режим
	Standard		Стандартний режим, який використовується для більшості функцій вибору, враховуючи переміщення. Вид курсору 

Продовж. табл. 3.2.4

Опції меню	Підменю	Іконка	Призначення
	Draw		Активізує режим *Activates Draw* і надає можливість вибору інструментальних засобів із панелі *Draw* або підменю *Sites* > *Draw*. Вид курсору +
	Link		Активізує режим зв'язків пристроїв. Для створення зв'язку між пристроями у проектній області вікна необхідно вибрати відповідні пристрої. Вид курсору 
	Set Traffic		Активізує режим *Set Traffic*. Для того щоб визначити трафік між двома пристроями, необхідно вибрати відповідні пристрої і потім вибрати тип трафіка у діалозі профілів. Вид курсору 
	Set Voice Call		Активізує режим *Set Calls*. Щоб визначити запити між двома пристроями виберіть відповідні пристрої, а потім виберіть тип запиту у діалозі профілів. Вид курсору 
	Set Data Call		Активізує режим *Set Calls*. Запити між двома пристроями можуть визначатися шляхом вибору відповідних пристроїв, а потім вибору типу запиту у діалозі профілів 
	Break/Restore		Активізує режим *Break/Restore*. Для того, щоб розривати та відновлювати зв'язки і пристрої, необхідно вибрати відповідний зв'язок або пристрій. Коли об'єкти (зв'язки або пристрої) розірвані, трафік/запити направляються за неправильною адресою. Щоб використовувати інструмент розриву/відновлення не повинно виконуватися моделювання роботи мережі. Рух трафіку/запиту за неправильною адресою може бути розглянутий лише під час виконання моделювання. Вид курсору 
	Trace Path		Активізує режим *Trace*. Щоб прослідкувати за шляхом між двома генераторами трафіка/запиту, необхідно вибрати ці два генератори. Шлях повинен бути позначений червоним кольором в тому ж самому сайті або між сайтами в багатошарових проектах. Якщо є багато шляхів, які доступні між пристроями, відстеження шляху відбувається для кожного типу відношення. Вид курсору 
	Say Info		Активізує режим *Say Notes*. Вид курсору 

Продовж. табл. 3.2.4

Опції меню	Підменю	Іконка	Призначення
Draw			Допускає вибір і виведення інструментальних засобів анотування проекту. Інструментальні засоби можуть бути вибрані, коли програма знаходиться в режимі *Draw*
	Pointer		Виберіть інструмент *Pointer* для того, щоб вибрати об'єкти і функції в той час, коли додаток знаходиться в режимі *Draw*. Інструмент *Pointer* виглядає так, як стандартний інструмент. Ця команда можлива лише тоді, коли додаток знаходиться в режимі *Draw*
	Line		Інструмент *Line* використовується для відображення (малювання) прямих ліній
	Rectangle		Інструмент *Rectangle* використовується для розміщення у вікні проекту порожніх прямокутників
	Round Rectangle		Інструмент *Round Rectangle* використовується для розміщення у вікні проекту прямокутника із закругленими краями
	Ellipse		Інструмент *Ellipse* використовується для розміщення у вікні проекту еліпсів
	Circle		Інструмент *Circle* використовується, щоб розмістити коло у вікні проекту
	Filled Rectangle		Інструмент *Filled Rectangle* використовується для розміщення у вікні проекту заповненого прямокутника
	Filled Round Rectangle		Інструмент *Filled Round Rectangle* використовується для розміщення у вікні проекту заповненого закругленого прямокутника
	Filled Ellipse		Інструмент *Filled Ellipse* використовується для розміщення у вікні проекту заповненого еліпса
	Filled Circle		Інструмент *Filled Circle* використовується для розміщення у вікні проекту заповненого кола
	Text		Інструмент *Text* використовується для додавання та редагування тексту
	Image		Інструмент *Image* використовується для звернення до діалогу огляду і вибору зображення, яке вставляють у проектну область вікна

Основні команди меню "Control" (Контроль)

Дане меню використовується для управління анімацією (табл. 3.2.5).

Таблиця 3.2.5

Основні команди Меню “Control”

Команди	Іконка	Опис
Start		Запуск анімації
Stop		Зупинка анімації
Pause		Пауза. Пакети/запити залишаються видимими, але не рухаються
Animation faster		Збільшити швидкість анімації
Animation slower		Зменшити швидкість анімації
Set Animation Default		Встановити параметри анімації для значень за замовчуванням, що були вибрані у діалозі параметрів
Animation setup		Відображає діалог налаштування анімації, який визначає інтенсивність пакетів/запитів, їх швидкодію і розмір
Quiet		Відключення звуку

Створення нового проекту NetCracker Professional

Для створення нового проекту в NetCracker Professional необхідно:

1. Запустити додаток NetCracker Professional.
2. У меню *File* вибрати команду *New*.
3. Розгорнути вікно сайту, натискаючи на кнопку збільшення вікна, а потім натиснути на кнопку *Zoom to page*.
4. У вікні *Devices* вибрати необхідне обладнання, наприклад, комутатори *(Switches),* робочі станції *(Workstation),* мережеві адаптери *(LAN adapters),* маршрутизатори *(Routers)* тощо.
5. Розмістити вибране обладнання на визначені місця.
6. З’єднати вибране обладнання і робочі станції лініями зв’язку, використовуючи інструмент *Link devices*.

Створення вигинів у кабельних сегментах

Для створення вигину кабельного сегмента необхідно:

1. Якщо виконується команда анімації, натиснути клавішу *Pause* для переходу до стану паузи. Утримуючи кнопку CTRL клавіатури, двічі клацнути кнопкою миші безпосередньо на зв’язку.
2. На зв’язку з’являється маркер захоплення (чорний квадрат). Натискаючи та утримуючи кнопку миші на захопленні, необхідно перетягнути її до нового місця розташування, а потім відпустити ліву кнопку миші. Зв’язок з’являється у точці, яка була обрана. Курсор

повинен бути поміщений точно на зв'язку, коли відбувається натискання на кнопку миші, щоб з'явилися маркери захоплення (точки вигину) (рис. 3.2.1).

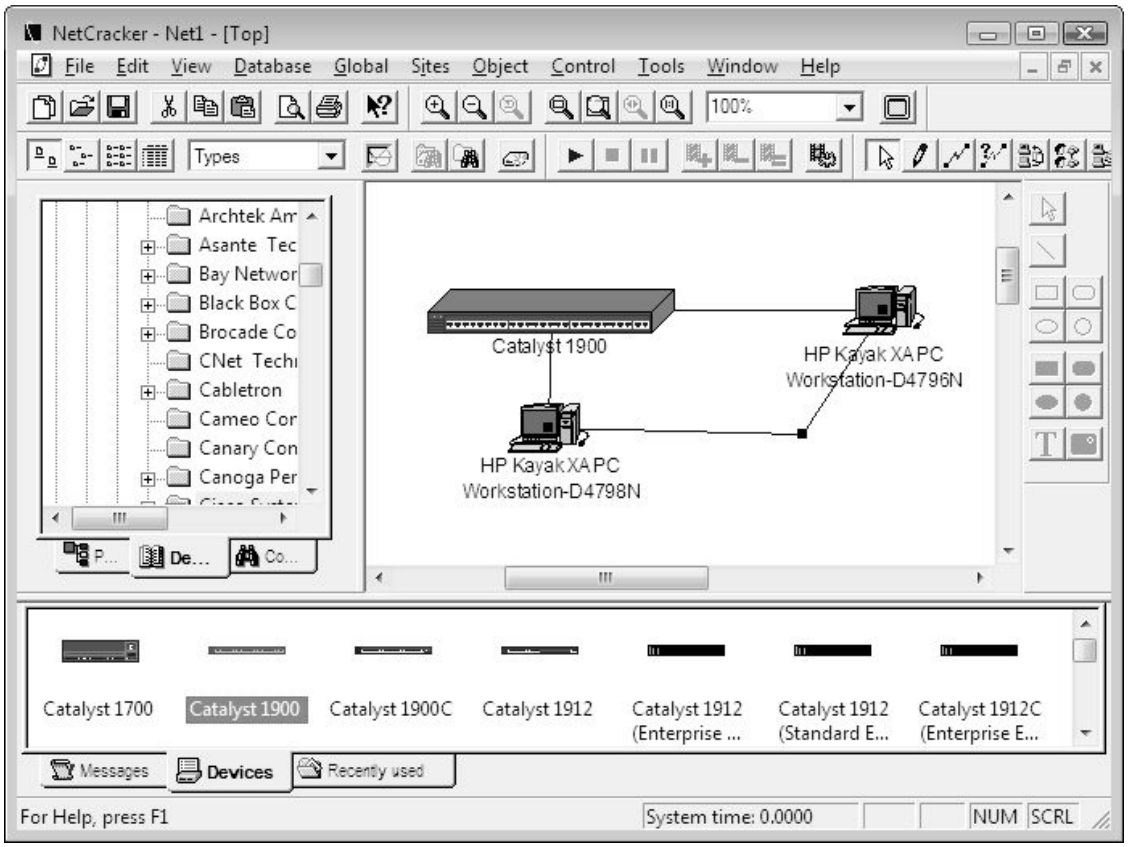


Рис. 3.2.1. Створення вигину у кабельному сегменті

Встановлення фону для проекту комп'ютерної мережі

Встановлення фону головного вікна проекту (Site) необхідне для більш точного розміщення мережевого обладнання і робочих станцій. Як фон може виступати план приміщення, для якого проектується комп'ютерна мережа.

Для встановлення фону в головному вікні проекту необхідно:

1. Натиснути правою кнопкою миші на головному вікні проекту і вибрати *Site Setup.* З'явиться вікно (рис. 3.2.2), у якому необхідно вибрати закладку "*Background*" (Фон).
2. Встановити прапорець "*Map*" (Мапа) у режим "включений" і вибрати необхідний фон, вказавши каталог *(Browse)*, у якому знаходиться фоновий файл. Необхідно відмітити, що фоновий файл повинен бути у форматі .gif.

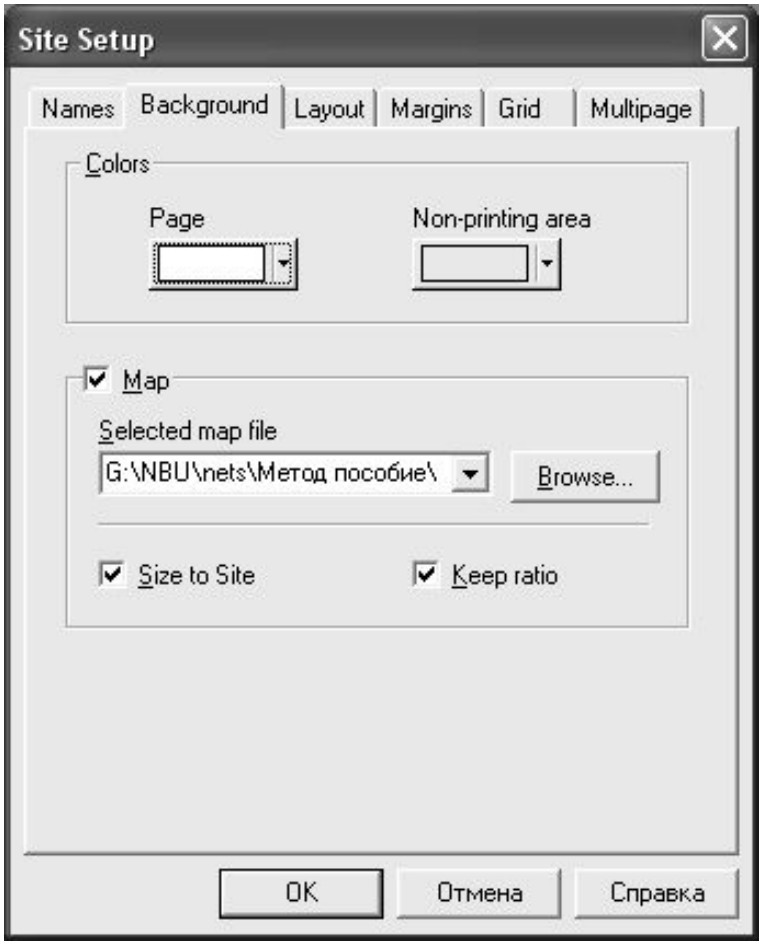


Рис. 3.2.2. Встановлення фону в головному вікні проекту

Встановлення зв'язків між пристроями

Для встановлення зв'язків між пристроями комп'ютерної мережі необхідно:

1. На інструментальній панелі *Modes* вибрати іконку *Link* (див. табл. 3.2.4).
2. Помістити курсор на одному з елементів, що з'єднуються (наприклад, на робочій станції), і виділити його лівою кнопкою миші, потім помістити курсор на іншому елементі, що з'єднується (наприклад, на комутаторі), і виділити його лівою кнопкою миші. З'явиться діалогове вікно помічника зв'язку (рис. 3.2.3).
3. Необхідно вибрати кнопку *Link,* потім ввести значення відстані між обладнанням і натиснути кнопку *Close* для того, щоб створити зв'язок і закрити діалогове вікно.

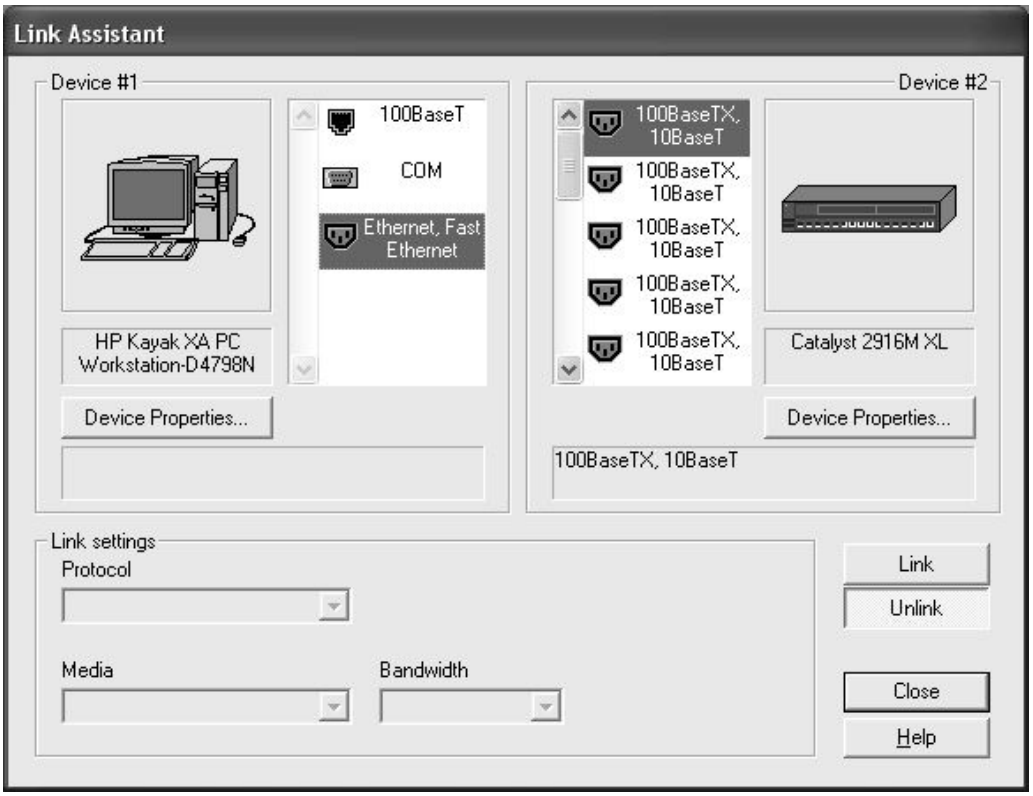


Рис. 3.2.3. Встановлення зв'язків між робочою станцією і вікно помічника зв'язку

Завдання до роботи

Необхідно спроектувати три комп'ютерні мережі банку з використанням технологій Ethernet (Fast Ethernet), Token Ring і FDDI. Мережі повинні бути спроектовані на основі плану приміщення, який був розроблений у лабораторній роботі № 1. Розташування мережевого обладнання, кабельних лотків, комп'ютерів і серверів повинно бути аналогічним плану розташування, спроектованого в попередній лабораторній роботі. Для проведення моделювання роботи комп'ютерних мереж, піктограми Visio-комп'ютерів, мережевого обладнання, серверів повинні бути замінені на аналогічні елементи Netcracker Professional. Персональні комп'ютери та сервери кожної з мереж повинні бути оснащені мережевими адаптерами. Мережеві адаптери та мережеве обладнання кожної мережі повинні підтримувати єдину для даної мережі технологію.

Дані про використовуване мережеве обладнання необхідно занести в таблицю.

Слід також відзначити, що у всіх мережах підтримується IP-телефонія, яка забезпечується комутаторами третього рівня компанії Cisco Systems. Трафік IP-телефонії йде по виділених кабельних сегментах і відділений від трафіка комп'ютерної мережі.

Також при проектуванні комп'ютерних мереж в Netcracker Professional відповідно до технології необхідно дотримуватися припустимих довжин кабельних сегментів (див. лекції).

План виконання роботи

Для кожної із трьох мереж, що проектуються, необхідно здійснити наступні дії:

1. Створити новий проект в інструментальному середовищі NetCracker Professional і зберегти його в окрему папку.
2. Встановити план приміщення банку як фон в головному вікні проекту. Фоном повинен бути рисунок плану приміщення комерційного банку, сформований в пакеті Microsoft Office Visio у лабораторній роботі № 1 (рис. 3.2.4).
3. Здійснити вибір екземпляра персонального комп'ютеру і необхідного мережевого адаптера. Мережевий адаптер необхідно розмістити в персональному комп'ютері (робочій станції).
4. Засобами NetCracker Professional здійснити дублювання необхідної кількості персональних комп'ютерів з встановленими мережевими адаптерами (див. табл. 3.2.2).
5. Здійснити вибір необхідного мережевого обладнання і серверів. Усе обладнання повинно підтримувати відповідну мережеву технологію і має бути сумісним між собою в рамках технології.
6. Занести інформацію про вибране мережеве обладнання (робочі станції, мережеві адаптери, комутатори і маршрутизатори) у таблицю (див. приклад – табл. 3.2.6).
7. Встановити зв'язки між мережевим обладнанням, персональними комп'ютерами і серверами. Зв'язки повинні розташовуватися відповідно до встановлених кабельних лотків і пластикових коробів.
8. Задати довжини кабельних сегментів у комп'ютерній мережі (рис. 3.2.5–3.2.7).

Таблиця 3.2.6

Приклад мережевого обладнання, яке застосовується при проектуванні комп'ютерної мережі

Тип	Назва в NetCracker	Компанія-виробник
Мережевий адаптер	3Com EtherLink 10/100 PCI	3Com
Робочі станції	HP Kayak XA PC Workstation-D4798N	Hewlett Packard
Комутатори	Catalyst 2924C XL (Standard Edition)	Cisco Systems
Маршрутизатори	Cisco 7513	Cisco Systems

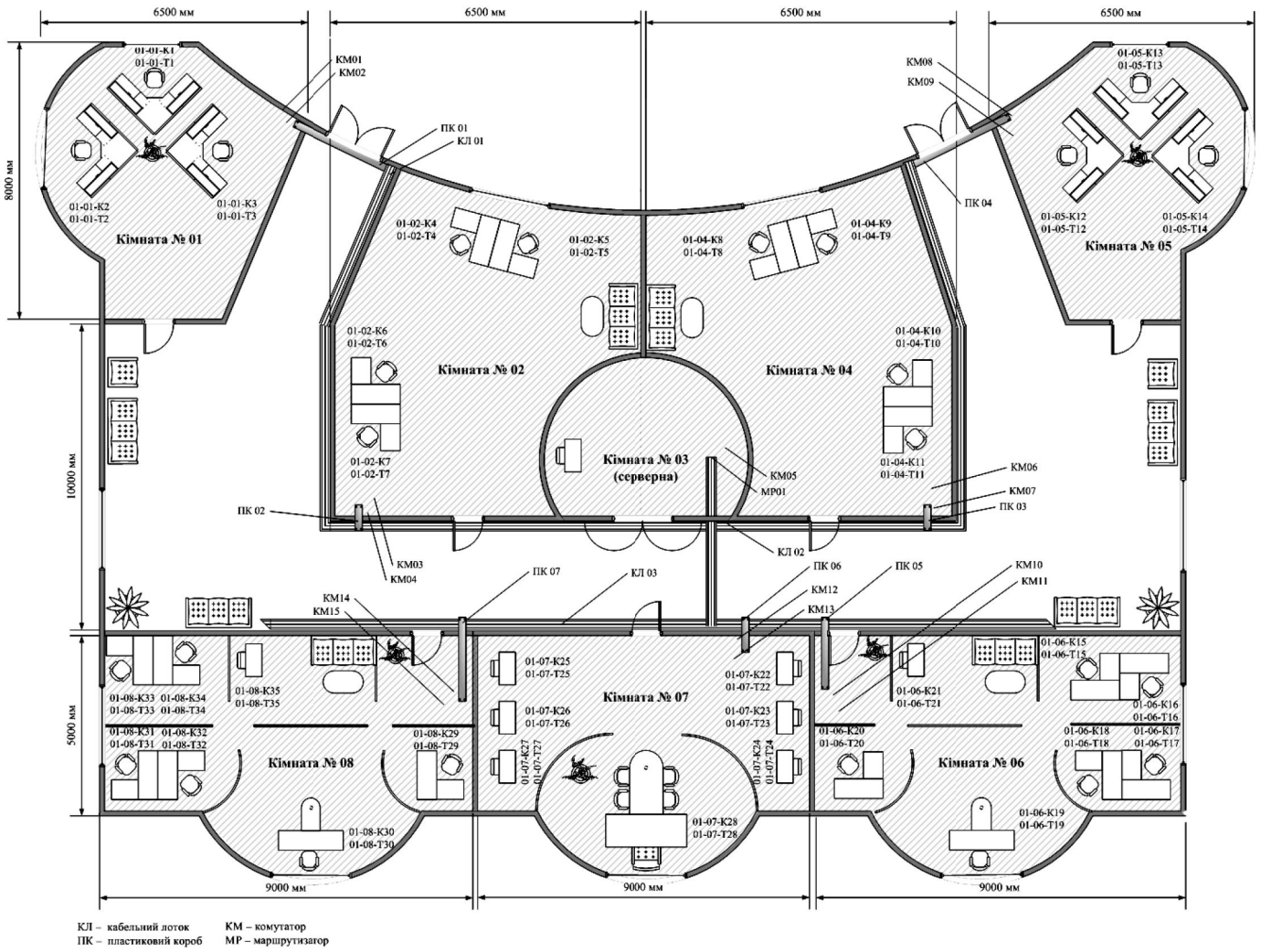


Рис. 3.2.4. Приклад фону головного вікна проекту

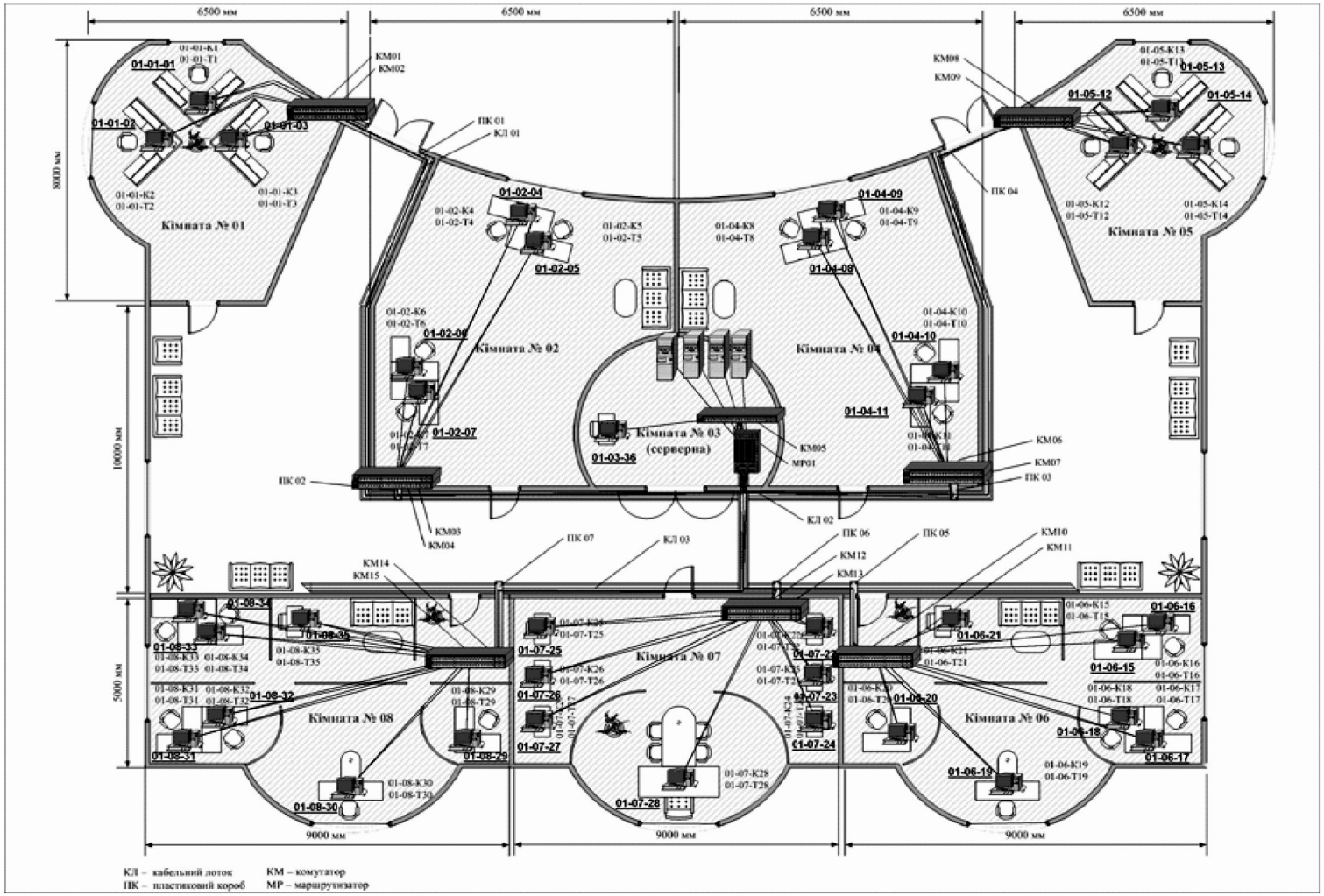


Рис. 3.2.5. Проект комп’ютерної мережі на основі технології Fast Ethernet

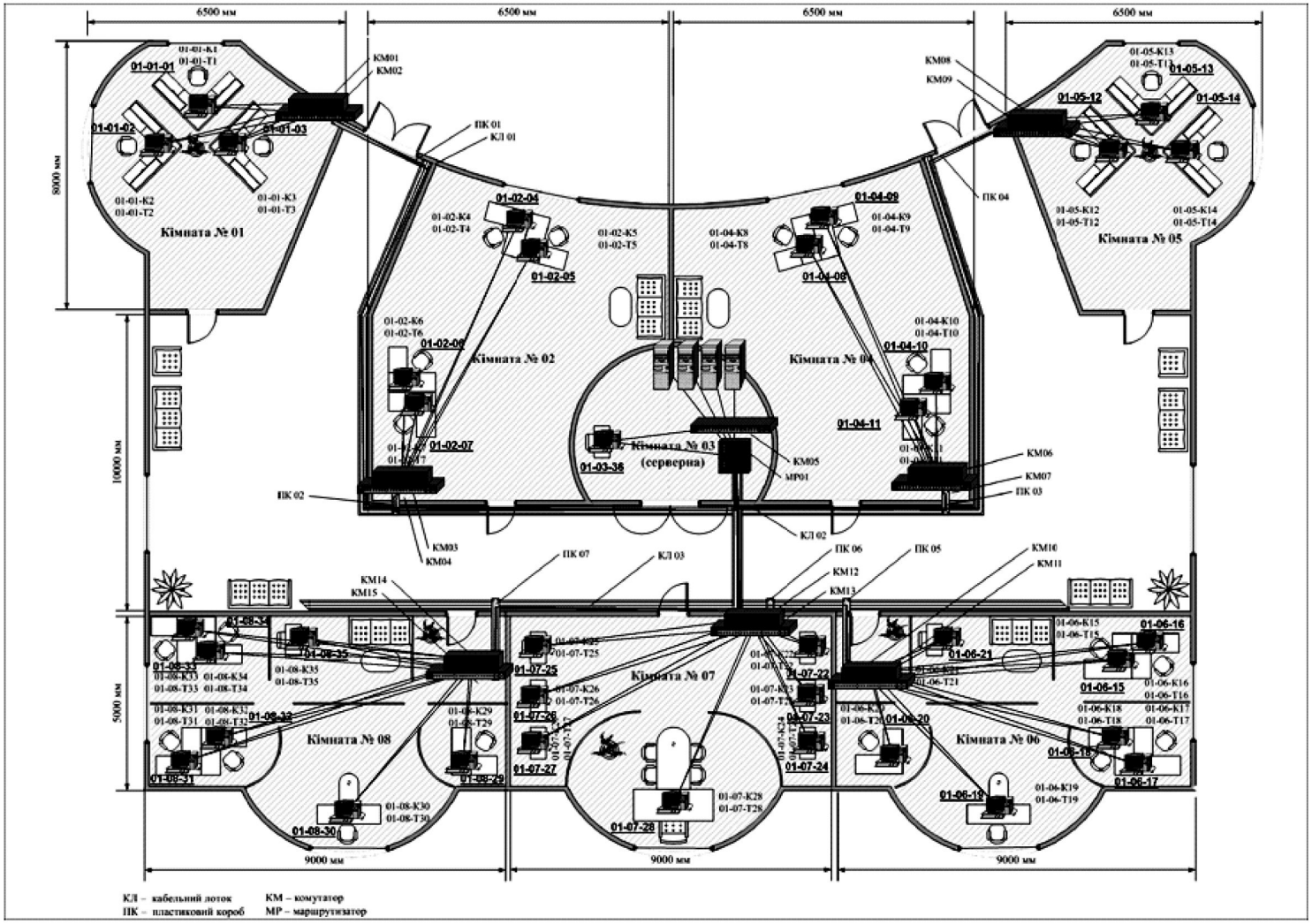


Рис. 3.2.6. Проект комп'ютерної мережі на основі технології Token Ring

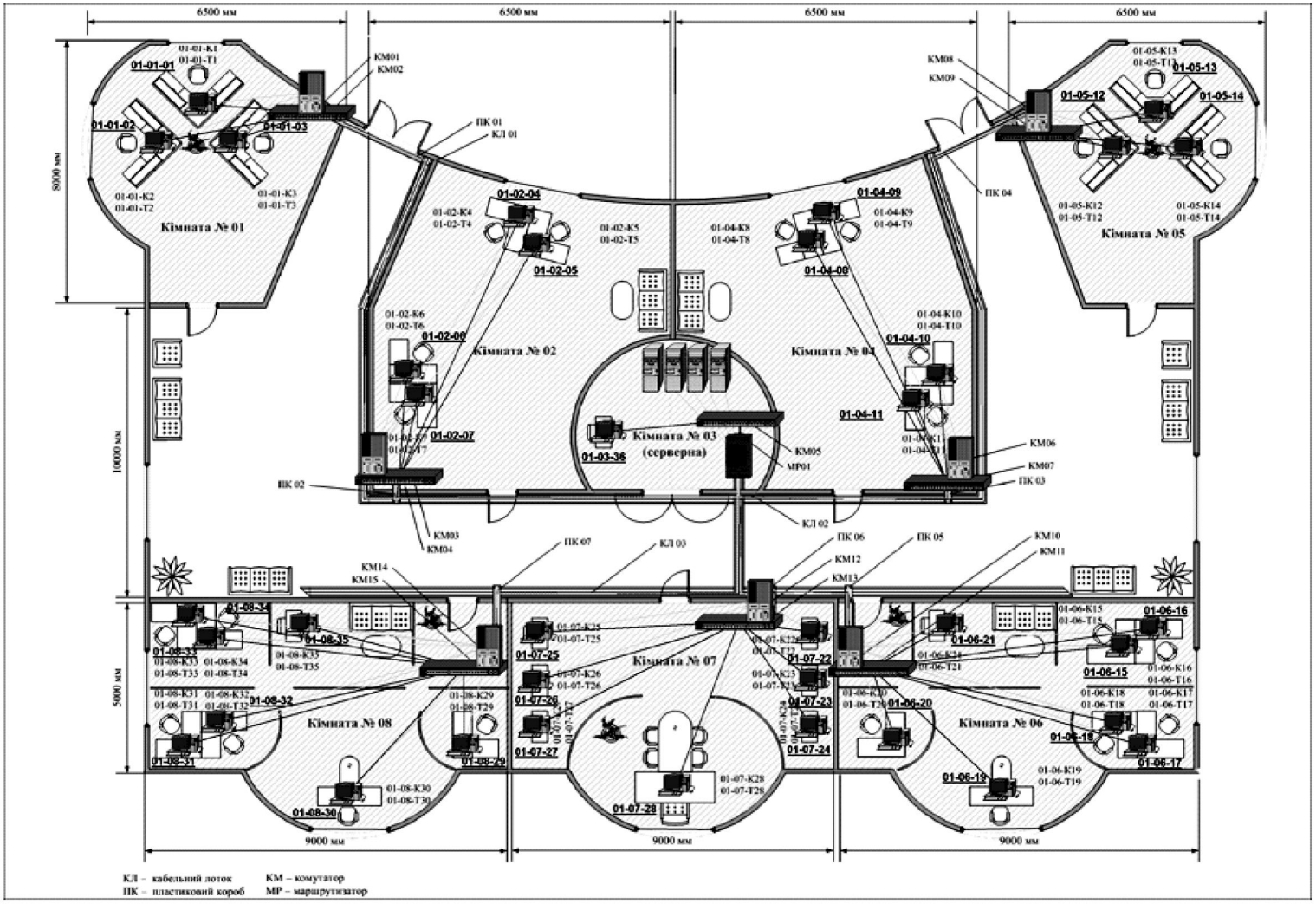


Рис. 3.2.7. Проект комп'ютерної мережі на основі технології FDDI

Питання для захисту роботи

1. Якими характерними рисами характеризується технологія Fast Ethernet?
2. Чи існують відмінності між обладнанням технології Fast Ethernet і Token Ring? Якщо так, то яка їх сутність?
3. Яку топологію мають комп'ютерні мережі, побудовані на основі технології FDDI?
4. Яким чином можна встановити зв'язки між обладнанням у середовищі NetCracker Professional?
5. Яким чином у NetCracker Professional можна створити вигин кабельного сегмента?
6. Яким чином встановлюються мережеві адаптери в робочі станції в середовищі NetCracker Professional?
7. Яким чином можна задати фон у головному вікні проекту NetCracker Professional?

ЛІТЕРАТУРА: [2, 5, 17, 31, 32, 33].

Лабораторна робота № 3
Тема "ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ РОБОТИ КОМП'ЮТЕРНИХ МЕРЕЖ КОМЕРЦІЙНОГО БАНКУ, СПРОЕКТОВАНИХ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ FAST ETHERNET, TOKEN RING І FDDI"

Мета роботи: одержати навички імітаційного моделювання роботи комп'ютерних мереж, спроектованих на основі технологій Fast Ethernet, Token Ring і FDDI.

Методичні вказівки

Дана лабораторна робота може бути виконана в інструментальному середовищі NetCracker Professional або в іншому подібному інструментальному середовищі.

Запуск процесу моделювання роботи мережі

Для запуску імітаційного моделювання роботи мережі необхідно:

1. Вибрати головне вікно проекту *(Top)* у меню *Windows* і позиціонувати його в робочий простір для детального розгляду.
2. Запустити процедуру імітаційного моделювання роботи комп'ютерних мереж, натискаючи кнопку *Start* на інструментальній панелі *Control.* Після чого активізується робота комп'ютерної мережі (пакети почнуть переміщатися по мережі).
3. Для налаштування імітаційного моделювання необхідно уточнити ряд параметрів. Для відображення вікна з налаштуванням параме-

трів (рис. 3.3.1) необхідно натиснути кнопку *Animation Setup* на панелі інструментів.

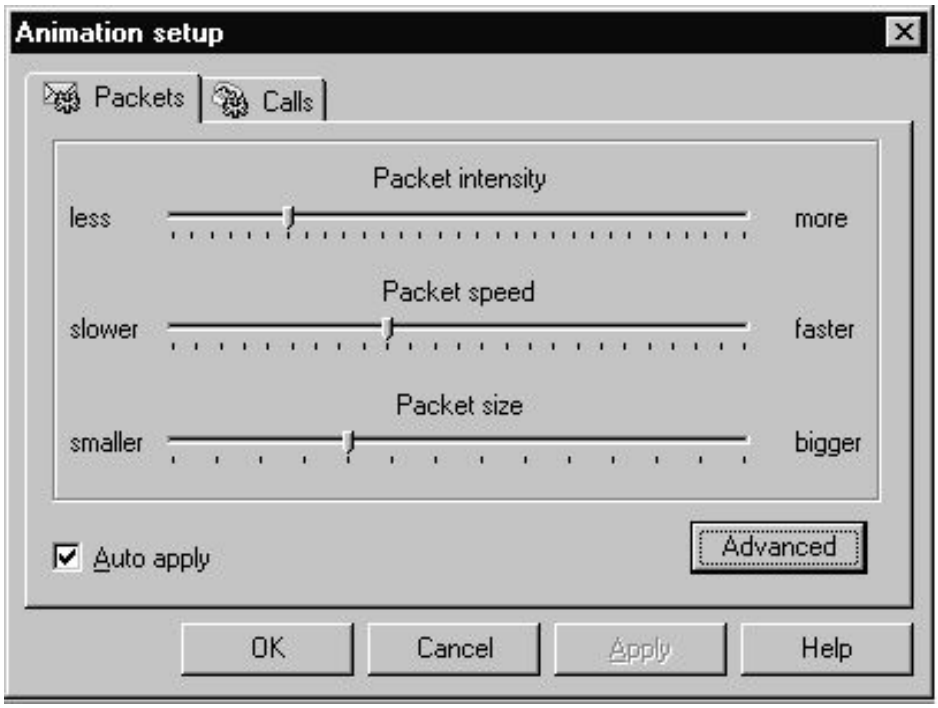


Рис. 3.3.1. Вікно налаштування параметрів імітаційного моделювання

Призначення типів трафіка в мережі

Для того, щоб призначити відповідні типи трафіка для комп'ютерної мережі, необхідно:

1. Вибрати кнопку *Set Traffics* на панелі інструментів NetCracker Professional.
2. Виділити, натискаючи лівою кнопкою миші, мережеве обладнання (робоча станція, комутатор, маршрутизатор) (джерело), від якого повинен відбуватися рух пакетів у мережі.
3. Виділити, натискаючи лівою кнопкою миші, мережеве обладнання (приймач), до якого повинні рухатися пакети, що йдуть від джерела.
4. У діалоговому вікні *Profiles* (рис. 3.3.2), яке з'явилося, указати тип трафіка, переданого від джерела до приймача типу, наприклад, *Small office*.
5. Дії 2-4 повторити для тих ділянок мережі, у яких необхідно промоделювати роботу.

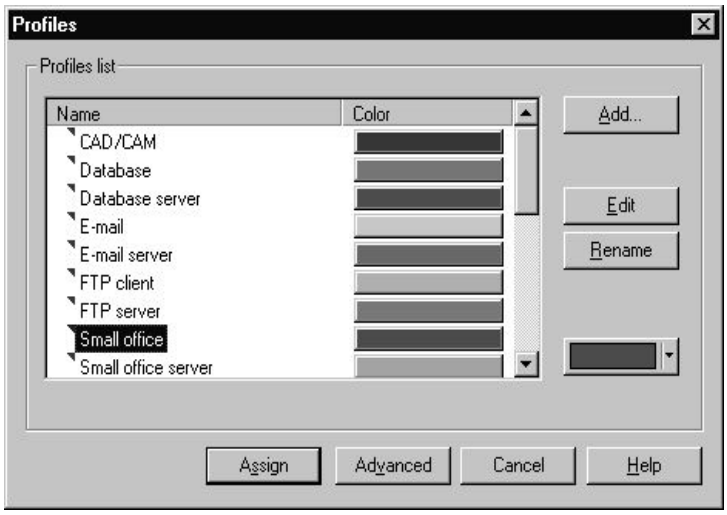


Рис. 3.3.2. Діалогове вікно профілів мережевого трафіка

Порушення й відновлення зв'язків, поломка та ремонт пристроїв

Для штучного порушення роботи мережі (зв'язків і обладнання) необхідно:

1. Натиснути на кнопку *Break/Restore* на панелі інструментів NetCracker Professional.
2. Вказівником миші в режимі *Break/Restore* натиснути на зв'язок або на обладнання.
3. Поява червоного спалаху (рис. 3.3.3) означає, що у точці її появи відбувся розрив зв'язку комп'ютерної мережі або вийшло з ладу мережеве обладнання.

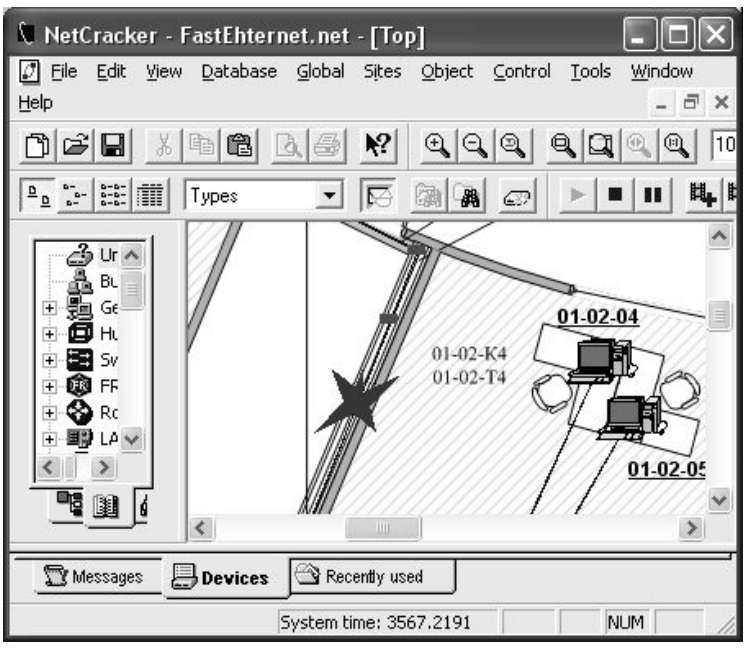


Рис. 3.3.3. Розрив зв'язку в комп'ютерній мережі

4. Для поновлення роботи обладнання, яке вийшло з ладу, або для відновлення зв'язку на ділянці мережі, необхідно повторно натиснути у точці появи червоного спалаху вказівником миші в режимі *Break/Restore.*

Візуалізація значень характеристик роботи мережевого обладнання

Для візуалізації характеристик необхідно:

1. Запустити моделювання роботи мережі, натиснувши кнопку *Start*.
2. Призупинити моделювання, натиснувши кнопку *Pause*.
3. На обладнанні, для якого необхідно візуалізувати значення характеристик, натиснути правою кнопкою миші. У контекстному меню, яке з'явилося, вибрати пункт *Statistics*.
4. У діалоговому вікні *Statistical Items* (рис. 3.3.4), яке з'явилося, вибрати необхідні характеристики роботи мережевого обладнання (наприклад, *Current Utilization*);
5. Біля індикатора, який з'явився біля мережевого обладнання, повинно з'явитися значення установленої характеристики. Для кращого відображення значення індикатора необхідно збільшити розмір шрифту та змінити його колір на більш яскравий (рис. 3.3.5). Для цього необхідно правою кнопкою миші натиснути на індикатор та вибрати з контекстного меню пункт *Properties;*
6. Відновити моделювання роботи комп'ютерної мережі, натиснувши на кнопку *Pause*.

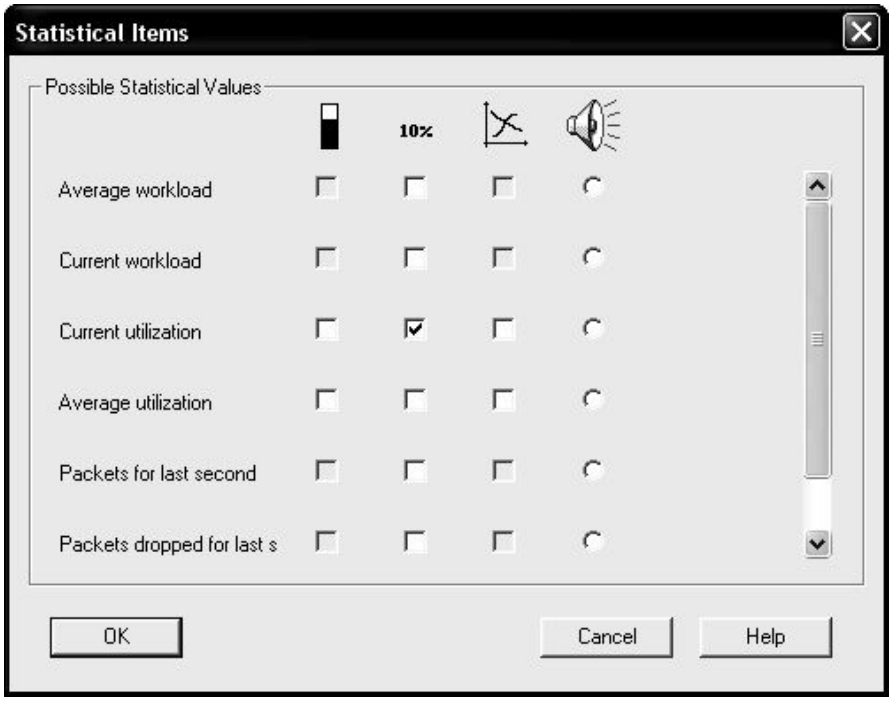


Рис. 3.3.4. Діалогове вікно Statistical Items

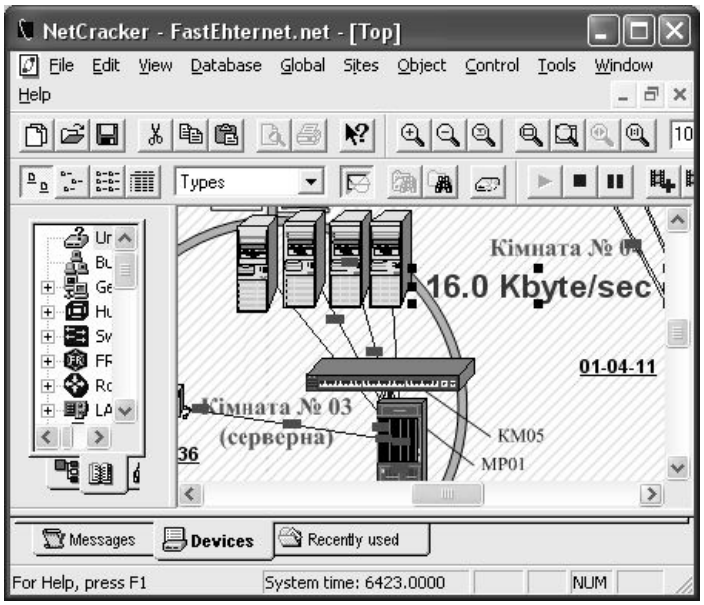


Рис. 3.3.5. Візуалізація значення індикатора

Завдання до роботи

Необхідно провести імітаційне моделювання роботи комп'ютерних мереж Fast Ethernet, Token Ring, FDDI, які були спроектовані в лабораторній роботі № 2. Під час імітаційного моделювання необхідно візуально визначити працездатність комп'ютерної мережі. У випадку нормальної роботи мережі джерела будуть направляти пакети приймачам без візуальних перекручувань. У протилежному випадку проблеми передачі пакетів по мережі будуть відображатися візуально у вигляді червоного спалаху (рис. 3.3.6).

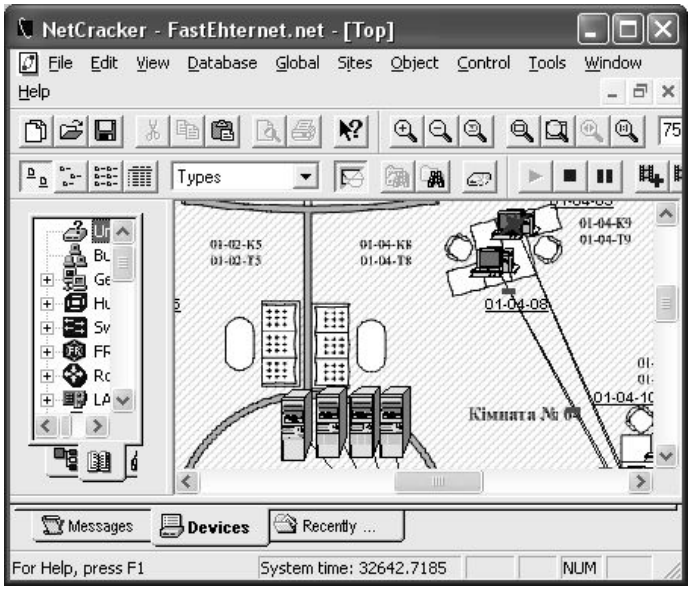


Рис. 3.3.6. Візуальне відображення несправності при передачі пакетів

Для більш точної оцінки працездатності комп'ютерної мережі необхідно виміряти наступні характеристики роботи мережевого обладнання (табл. 3.3.1).

Таблиця 3.3.1

Характеристики роботи мережевого обладнання

Назва характеристики	Назва характеристики в NetCracker Professional
Поточне використання мережевого обладнання	Current utilization
Середнє використання мережевого обладнання	Average utilization
Середня затримка	Average delay
Середнє робоче навантаження	Average workload
Поточне робоче навантаження	Current workload
Пакети, передані за останню секунду	Packets for last seconds
Пакети, втрачені за останню секунду	Packets dropped for last seconds

Значення характеристик, представлених у табл. 3.3.1, необхідно відобразити у вікні проекту для всього мережевого обладнання та занести їх в окрему таблицю.

Також необхідно змоделювати ситуацію розриву зв'язку в комп'ютерній мережі й поломки мережевого обладнання. Після цього виміряти характеристики, представлені в табл. 3.3.1, і також занести в окрему таблицю.

Порівняти характеристики при нормальній роботі мережі та при її несправній роботі.

План виконання роботи

Для кожної із трьох комп'ютерних мереж (Fast Ethernet, Token Ring і FDDI) необхідно зробити наступні дії (рис. 3.3.7 – 3.3.9):

1. Призначити тип трафіка *Small office* від однієї робочої станції до всіх інших робочих станцій.
2. Запустити процедуру імітаційного моделювання роботи комп'ютерної мережі.
3. Призупинити імітаційне моделювання роботи комп'ютерної мережі, натиснувши на кнопку *Pause*.
4. Установити індикатор характеристики *Average utilization* для обраного мережевого обладнання (окрім робочих станцій) і візуалізувати його значення в головному вікні проекту. Запустити імітаційне моделювання роботи мережі. Призупинити імітаційне моделювання роботи комп'ютерної мережі й занести значення індикатора в таблицю.

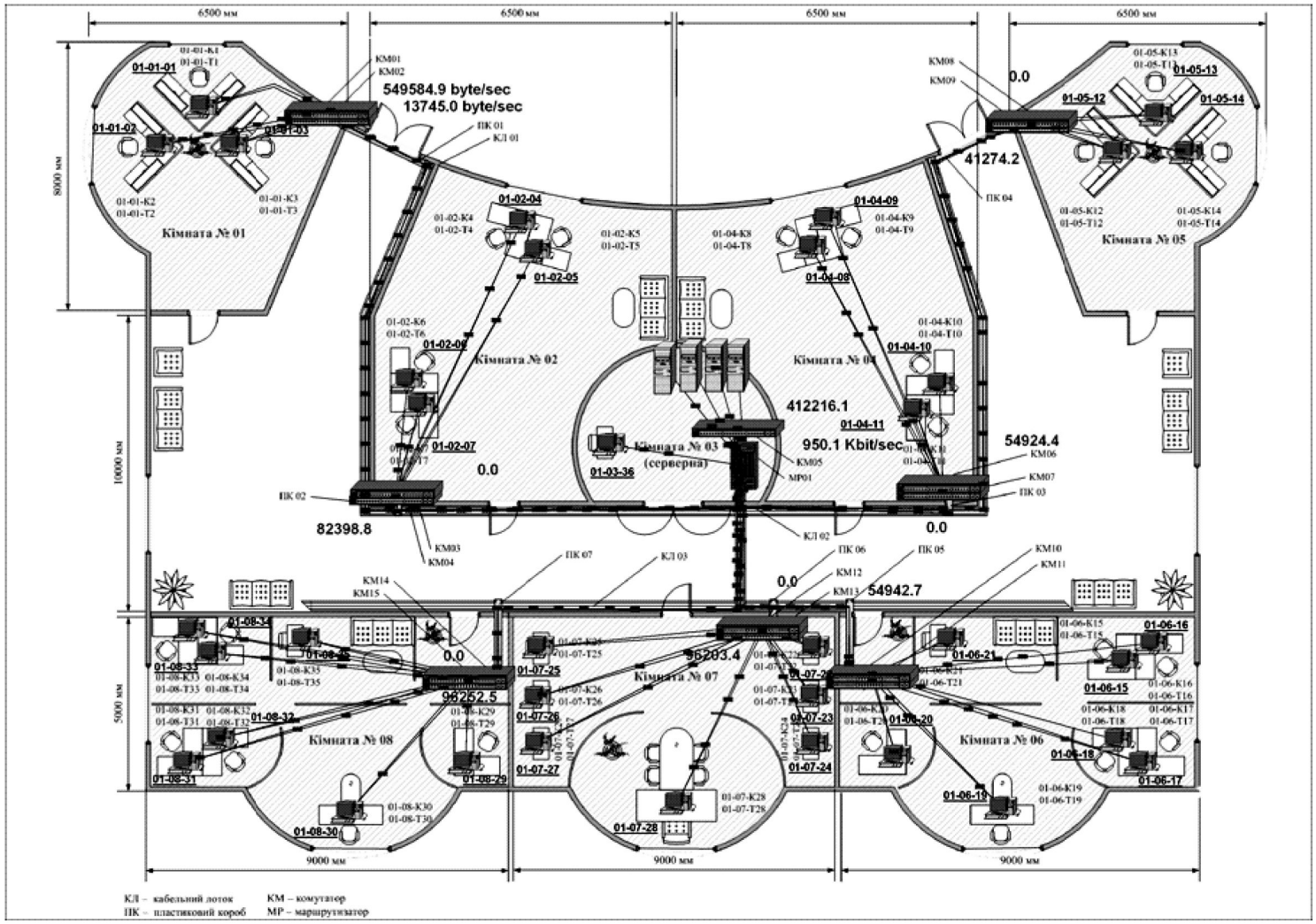


Рис. 3.3.7. Приклад імітаційного моделювання роботи комп'ютерної мережі Fast Ethernet

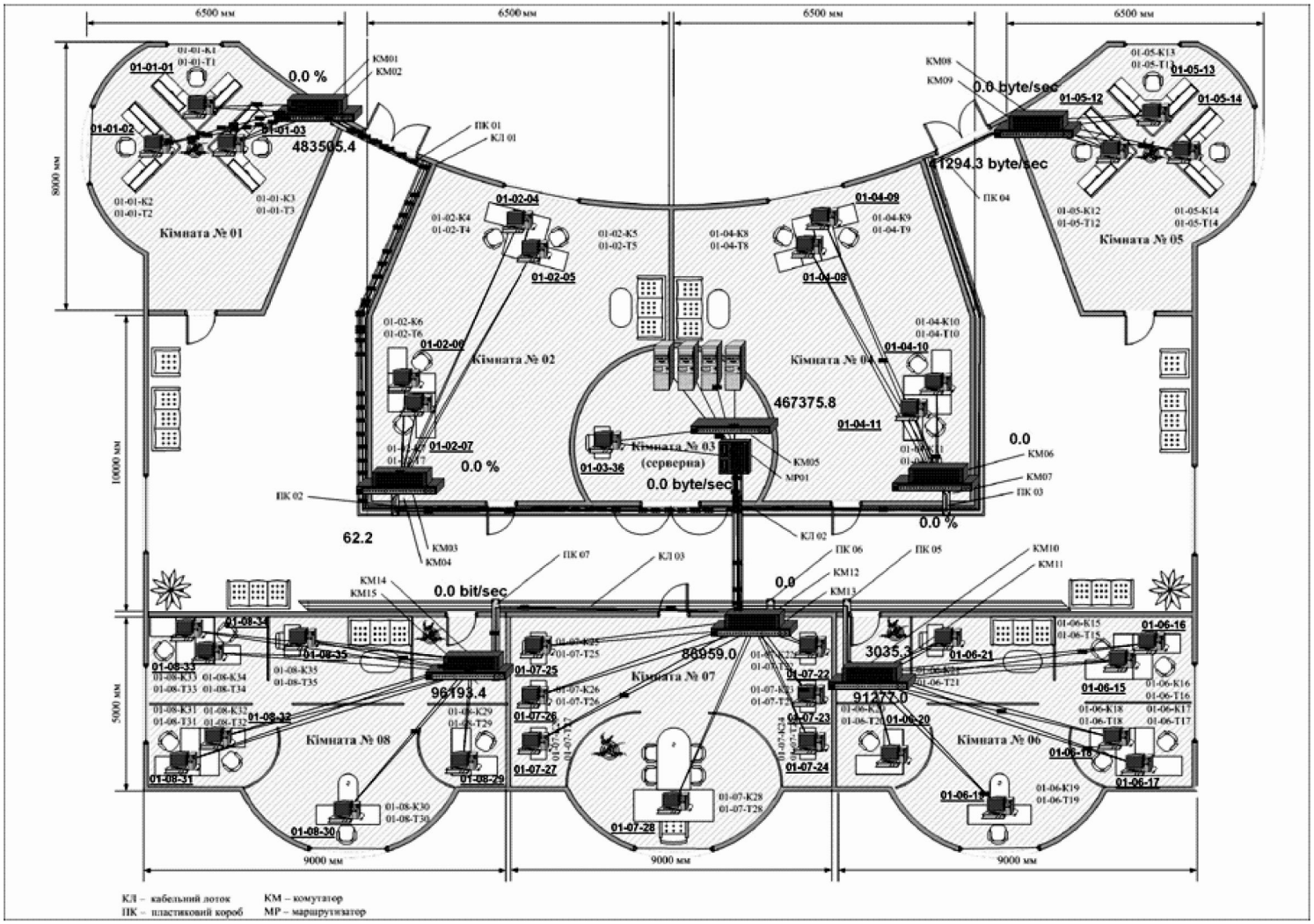


Рис. 3.3.8. Приклад імітаційного моделювання роботи комп'ютерної мережі Token Ring

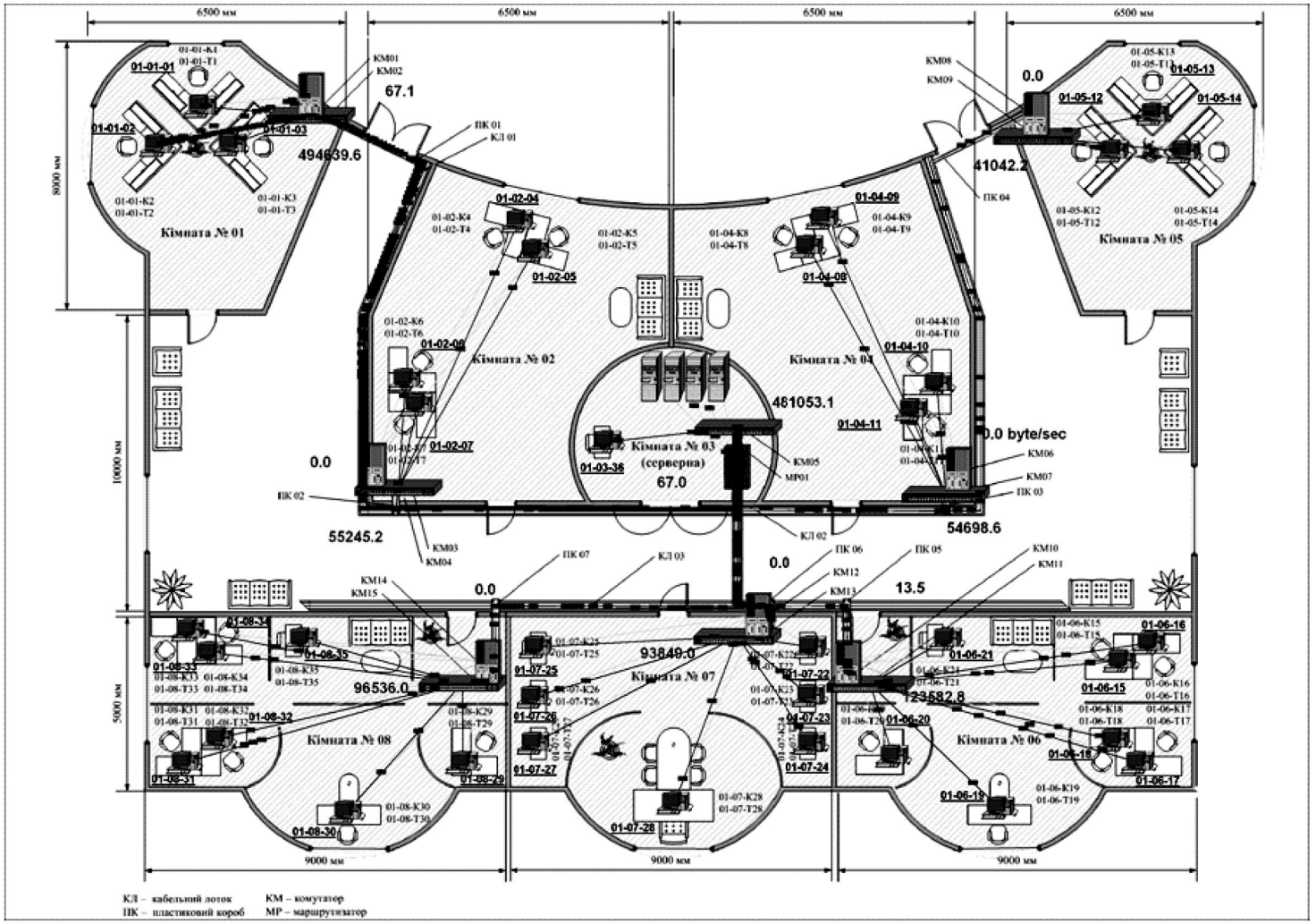


Рис. 3.3.9. Приклад імітаційного моделювання роботи комп'ютерної мережі FDDI

5. Приховати індикатор *Average utilization* для обраного мережевого обладнання. Установити індикатор характеристики *Average delay* для обраного мережевого обладнання (окрім робочих станцій) і візуалізувати його значення в головному вікні проекту. Запустити імітаційне моделювання роботи мережі. Призупинити імітаційне моделювання роботи комп'ютерної мережі й занести значення індикатора в таблицю.
6. Приховати індикатор *Average delay* для обраного мережевого обладнання. Установити індикатор характеристики *Average workload* для обраного мережевого обладнання (окрім робочих станцій) і візуалізувати його значення в головному вікні проекту. Запустити імітаційне моделювання роботи мережі. Призупинити імітаційне моделювання роботи комп'ютерної мережі й занести значення індикатора у таблицю.
7. Приховати індикатор *Average workload* для обраного мережевого обладнання. Установити індикатор характеристики *Current workload* для обраного мережевого обладнання (окрім робочих станцій) і візуалізувати його значення в головному вікні проекту. Запустити імітаційне моделювання роботи мережі. Призупинити імітаційне моделювання роботи комп'ютерної мережі й занести значення індикатора в таблицю.
8. Приховати індикатор *Current workload* для обраного мережевого обладнання. Установити індикатор характеристики *Packets for last seconds* для обраного мережевого обладнання (окрім робочих станцій) і візуалізувати його значення в головному вікні проекту. Запустити імітаційне моделювання роботи мережі. Призупинити імітаційне моделювання роботи комп'ютерної мережі й занести значення індикатора в таблицю.
9. Приховати індикатор *Packets for last seconds* для обраного мережевого обладнання. Установити індикатор характеристики *Packets dropped for last seconds* для обраного мережевого обладнання (окрім робочих станцій) і візуалізувати його значення в головному вікні проекту. Запустити імітаційне моделювання роботи мережі. Призупинити імітаційне моделювання роботи комп'ютерної мережі. Занести значення індикатора у таблицю.
10. Повторити дії 4-9 для всього мережевого обладнання (окрім робочих станцій).
11. Змоделювати ситуацію обриву зв'язку в комп'ютерній мережі. Для цього на будь-якому відрізку кабелю, який з'єднує робочу станцію та комутатор, необхідно засобами NetCracker Professional розірвати зв'язок. Значення всіх характеристик для комутатора занести в таблицю.

12. Змоделювати ситуацію виходу з ладу мережевого обладнання. Для цього необхідно засобами NetCracker Professional перевести в непрацездатний стан комутатор, який з'єднує робочі станції. Значення всіх характеристик для кожної з робочих станцій, підключених до непрацездатного комутатора, занести в таблицю;
13. Використовуючи значення характеристик роботи мережевого обладнання (у випадку працездатності комп'ютерної мережі й у випадку обриву зв'язку або виходу з ладу обладнання), зробити висновок про те, яким чином змінюються значення характеристик при виході з ладу обладнання або при обриві зв'язку.

Питання для захисту роботи

1. Що таке імітаційне моделювання? З якою метою воно проводиться?
2. Які дії необхідно здійснити, щоб провести процедуру імітаційного моделювання в NetCracker Professional?
3. Моделювання яких типів мережевого трафіка можна реалізувати в NetCracker Professional?
4. Значення яких характеристик комп'ютерної мережі можна виміряти засобами NetCracker Professional?
5. Яким чином засобами NetCracker Professional можна розірвати зв'язок у комп'ютерній мережі й перевести мережеве обладнання в непрацездатний стан?
6. Як впливає розрив зв'язку та вихід з ладу мережевого обладнання на значення характеристик комп'ютерної мережі?
7. Яким чином засобами NetCracker Professional можна змінити швидкість мережевих пакетів, їхню інтенсивність і розмір?

ЛІТЕРАТУРА: [5, 14, 19, 24].

Лабораторна робота № 4
Тема "ПРОЕКТУВАННЯ Й ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ РОБОТИ МІСЬКОЇ МЕРЕЖІ ВІДДІЛЕНЬ КОМЕРЦІЙНОГО БАНКУ"

Мета роботи: одержати навички проектування й імітаційного моделювання міської мережі відділень комерційного банку.

Методичні вказівки

Дана лабораторна робота може бути виконана в інструментальному середовищі NetCracker Professional, яке підтримує проектування й імітаційне моделювання роботи ієрархічної міської комп'ютерної мережі або в іншому подібному інструментальному середовищі.

Стисла характеристика технології WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) – це технологія надання бездротового широкосмугового доступу в Інтернет. WiMAX базується на стандарті IEEE 802.16. Забезпечує мультисервісність, гнучкий розподіл частот, завдання пріоритетів різним видам трафіка, можливість забезпечення різного рівня якості (QoS), підтримку інтерфейсів IP, TDM E1/T1. Ця технологія дозволяє паралельно передавати голос, мультимедійну інформацію та цифрові дані по одному каналу зв'язку. Важливою перевагою є можливість швидко нарощувати ємність і розширювати територію зв'язку. Базові станції не вимагають наявності високих щогл, досить розмістити антени на високих будинках або існуючих щоглах, висотою приблизно 50 м. Є проекти розміщення базової станції на аеростаті з фіксованим положенням. У цьому випадку можливе покриття території діаметром 500-600 км.

Одна типова станція в мережі стандарту 802.16 може обслуговувати велику кількість користувачів і надавати їм послуги різного рівня: наприклад, для 60 бізнесів-користувачів – послуги по каналу E1 (зі швидкістю 2.048 Мбіт/с) і одночасно для сотень домашніх користувачів з меншими смугами необхідних частот.

Стандарт 802.16 забезпечує високий рівень конфіденційності та безпеки повідомлень, шифрування трафіка в межах всієї бездротової мережі. Забезпечується транспорт голосових даних по IP – VoIP. За допомогою WiMAX можна поєднувати локальні мережі віддалених офісів.

Мережа WiMAX за своєю архітектурою подібна стільниковій мережі. У місті встановлюється мережа базових станцій (BS). Кожна базова станція за схемою "точка до багатьох точок" (point-multipoint) може обслуговувати за допомогою всеспрямованих антен свою групу будинків у радіусі 6-8 км, утворюючи подобу чарунок бджолиних сот.

При необхідності зв'язку між вилученими комірками базові станції можуть мати спрямовані антени й виконувати роль ретрансляторів за схемою "точка-точка" по радіоканалу на відстанях до 50 км. За допомогою ретрансляторів можна створювати регіональні мережі, які складаються немов би з острівців локальних мереж. Доступ до глобальних мереж забезпечується тим, що або кожна базова станція, або одна з них, до якої через ретранслятори або спрямовані антени мають доступ усі інші базові станції, підключається дротовим з'єднанням або оптоволокном до магістральної мережі. Таку базову станцію називають *точкою доступу до магістралі Backhaul*. Схема такої архітектури показана на рис. 3.4.1.

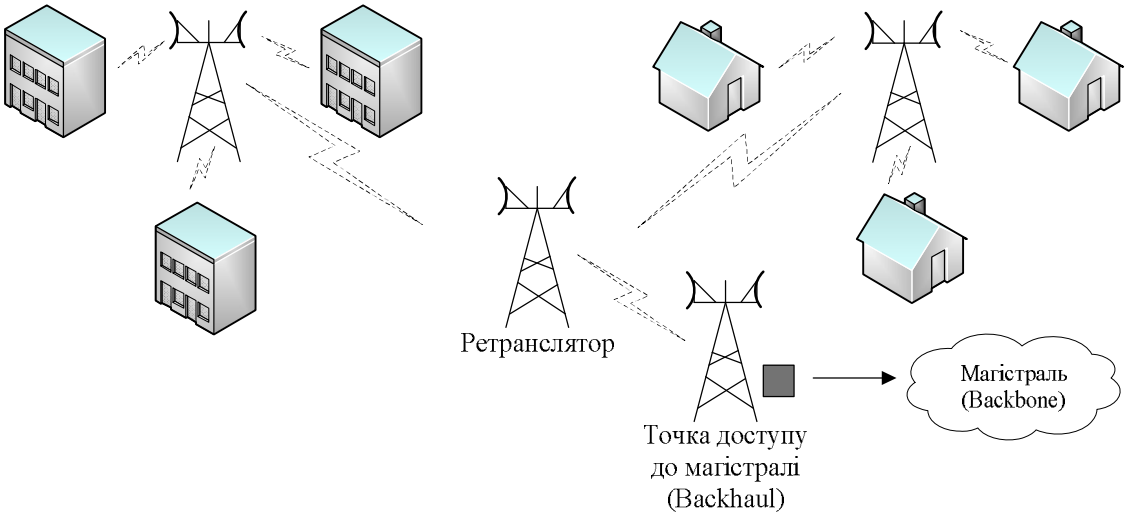


Рис. 3.4.1. Архітектура мережі WiMAX

Антени базових станцій можуть бути встановлені не тільки на щоглах, але й на дахах високих будинків.

Для забезпечення роботи комп'ютерної мережі на будівлях, що обслуговуються, установлюються фіксовані зовнішні антени, підключені до блоку трансівера – станції клієнтів (SS), яка знаходиться усередині будинку. У блоці трансівера є стандартні дротові Ethernet-інтерфейси для підключення обладнання клієнтів. Ноутбуки, що знаходяться усередині будинку і підтримують бездротовий стандарт 802.11 (WiFi), мають у будинку загальну точку доступу. Для організації виходу в зовнішню мережу трафік користувачів від різного обладнання поєднуються за допомогою мультиплексора, вихід якого підключається до блоку трансівера клієнтів і далі передається мережею WiMAX (рис. 3.4.2).

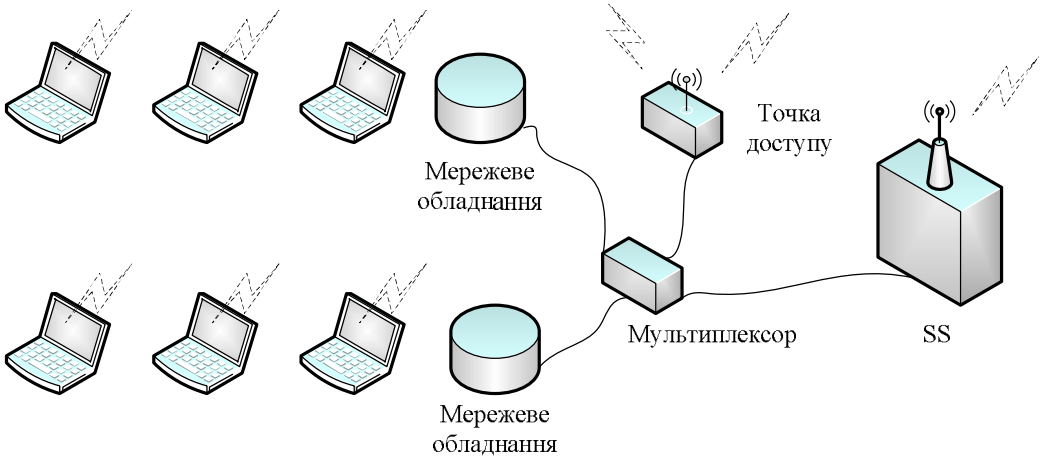


Рис. 3.4.2. Схема підключення офісного обладнання через точку доступу до мережі WiMAX

Стисла характеристика технології FDDI

Мережа FDDI (стандарт IEEE 802.8) (Fiber Distributed Data Interface – оптоволоконний розподілений інтерфейс даних) – технологія для мережевої архітектури високошвидкісної передачі даних по оптоволоконних лініях. Стандарт FDDI, запропонований Американським національним інститутом стандартів ANSI (специфікація ANSI X3T9.5), орієнтувався на швидкість передачі (100 Мбіт/с) і на застосування перспективного оптоволоконного кабелю.

Вибір оптоволокна як середовища передачі визначив такі переваги нової мережі, як висока перешкодозахищеність, максимальна таємність передачі інформації та прекрасна гальванічна розв'язка абонентів. Висока швидкість передачі, яка у випадку використання оптоволоконного кабелю досягається набагато простіше, дозволяє вирішувати багато задач, недоступних менш швидкісним мережам, наприклад, передачу зображень у реальному масштабі часу. Крім того, оптоволоконний кабель легко вирішує проблему передачі даних на відстань декількох кілометрів без ретрансляції, що дозволяє будувати набагато більші за розмірами мережі, які охоплюють навіть цілі міста та мають при цьому всі переваги локальних мереж (зокрема, низький рівень помилок).

За основу стандарту FDDI був узятий метод маркерного доступу, передбачений міжнародним стандартом IEEE 802.5 – Token Ring. Невеликі відмінності від цього стандарту визначаються необхідністю забезпечити високу швидкість передачі інформації на більші відстані. Топологія мережі FDDI – це кільце, причому застосовується два різноспрямованих оптоволоконних кабелі, що дозволяє в принципі використати повнодуплексну передачу інформації з подвоєною ефективною швидкістю в 200 Мбіт/с (при цьому кожний із двох каналів працює на швидкості 100 Мбіт/с). Застосовується й зірково-кільцева топологія з концентраторами, включеними в кільце.

Основні технічні характеристики мережі FDDI наступні:

- максимальна кількість абонентів мережі – 1000;
- максимальна довжина кільця мережі – 20 км;
- максимальна відстань між абонентами мережі – 2 км;
- середовище передачі – оптоволоконний кабель (можливе застосування витої пари);
- метод доступу – маркерний;
- швидкість передачі інформації – 100 Мбіт/с (200 Мбіт/с для повнодуплексного режиму передачі).

Слід зазначити, що обмеження на загальну довжину мережі в 20 км пов'язане не із загасанням сигналів у кабелі, а з необхідністю обмеження часу повного проходження сигналу по кільцю для забезпе-

чення гранично припустимого часу доступу. А максимальна відстань між абонентами (2 км при багатомодовому кабелі) визначається саме загасанням сигналів у кабелі. Передбачена також можливість застосування одномодового кабелю, і в цьому випадку відстань між абонентами може досягати 45 км, а повна довжина кільця – 100 км.

Також існує реалізація FDDI на витій парі (CDDI – Copper Distributed Data Interface або TPDDI – Twisted Pair Distributed Data Interface). При цьому використовується кабель категорії 5 з роз'ємами RJ-45. Максимальна відстань між абонентами в цьому випадку повинна бути не більше 100 м. Вартість обладнання мережі на основі електричного кабелю в кілька разів менше.

Стандарт FDDI для досягнення високої гнучкості мережі передбачає включення в кільце абонентів двох типів:

- абоненти (станції) класу А (абоненти подвійного підключення, DAS – Dual-Attachment Stations). Вони підключаються до обох (внутрішнього і зовнішнього) кілець мережі. При цьому реалізується можливість обміну зі швидкістю до 200 Мбіт/с або ж можливість резервування кабелю мережі (при ушкодженні основного кабелю використовується резервний кабель). Апаратура цього класу використовується в найбільш критичних частинах мережі;
- абоненти (станції) класу В (абоненти одинарного підключення, SAS – Single-Attachment Stations) підключаються тільки до одного (зовнішнього) кільця мережі. Вони більш прості й дешеві, ніж адаптери класу А, і не мають їхніх можливостей. У мережу вони можуть включатися тільки через концентратор або обхідний комутатор, який відключає їх у випадку аварії.

Крім абонентів (комп'ютерів, терміналів) у мережі використовуються зв'язні концентратори (Wiring Concentrators), включення яких дозволяє зібрати в одне місце всі точки підключення з метою контролю за роботою мережі, діагностики несправностей і спрощення реконфігурації. При застосуванні кабелів різних типів (наприклад, оптоволоконного кабелю й витої пари) концентратор виконує також функцію перетворення електричних сигналів в оптичні та навпаки. Концентратори бувають подвійного підключення (DAC – Dual-Attachment Concentrator) і одинарного підключення (SAC – Single-Attachment Concentrator). Приклад найпростішої конфігурації мережі FDDI представлений на рис. 3.4.3.

FDDI визначає чотири типи портів абонентів (станцій):

- порт А визначений тільки для пристроїв подвійного підключення, його вхід підключається до первинного кільця, а вихід – до вторинного;

- порт B визначений тільки для пристроїв подвійного підключення, його вхід підключається до вторинного кільця, а вихід – до первинного;
- порт M (Master) визначений для концентраторів і з'єднує два концентратори між собою або концентратор з абонентом;
- порт S (Slave) визначений тільки для пристроїв одинарного підключення та використовується для з'єднання двох абонентів або абонента та концентратора.

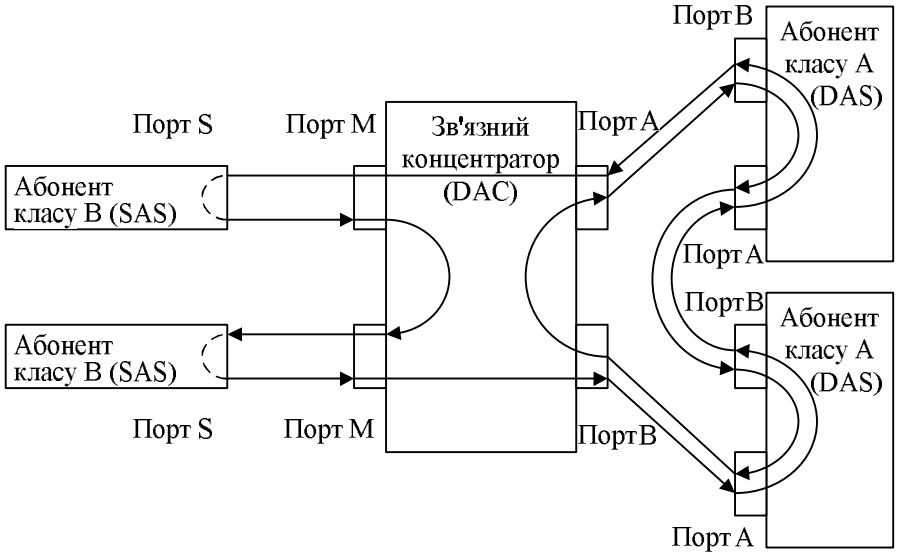


Рис. 3.4.3. Приклад конфігурації FDDI

Стандарт FDDI передбачає також можливість реконфігурації мережі з метою збереження її працездатності у випадку ушкодження кабелю. На рис. 3.4.4 проілюстровано, як ушкоджена ділянка кабелю виключається з кільця, але цілісність мережі при цьому не порушується внаслідок переходу на одне кільце замість двох.

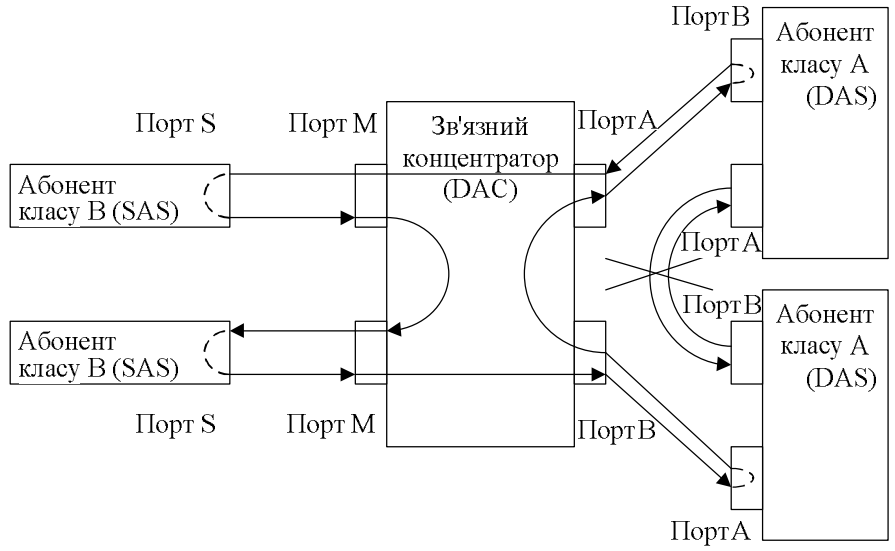


Рис. 3.4.4. Реконфігурація мережі FDDI при ушкодженні кабелю

Процедура створення ієрархічного проекту комп'ютерної мережі в інструментальному середовищі NetCracker Professional

Ієрархічні проекти комп'ютерних мереж створюють, коли необхідно сформувати проект мережі в рамках будинку, міста або декількох міст.

Для створення ієрархічного проекту комп'ютерної мережі в рамках міста необхідно виконати наступні дії:

1. У головному вікні проекту необхідно розмістити об'єкт *City* (Місто). Даний об'єкт перебуває в категорії *Buildings, campuses and LAN workgroups.*
2. Необхідно відкрити робочу область об'єкта *City*. Для цього треба для нього викликати контекстне меню й вибрати пункт *Expand.*
3. У робочій області міста розмістити необхідну кількість об'єктів *Building* (Будинок). Даний об'єкт знаходиться в категорії *Buildings, campuses and LAN workgroups*.
4. Для кожного об'єкта *Building* необхідно відкрити робочу область (див. п. 2) і розмістити в ній необхідну кількість об'єктів *Floor* (Поверх).
5. Для кожного об'єкта *Floor* необхідно відкрити робочу область і розмістити в ній необхідне мережеве обладнання для локальної мережі поверху.
6. Усі елементи ієрархічного проекту комп'ютерної мережі необхідно об'єднати в єдину мережу. Інакше кажучи, необхідно з'єднати між собою поверхи в рамках будинків, а також всі будинки в рамках міста.

Завдання до роботи

Необхідно спроектувати міську комп'ютерну мережу відділень комерційного банку. Кожне відділення розташовується в окремому триповерховому будинку. Зв'язок відділень між собою забезпечується за технологією FDDI або WiMAX. Усередині будинку комп'ютерні мережі поверхів спроектовані за технологією Fast Ethernet. План кожного поверху відділень, а також структура комп'ютерних мереж ідентичні між собою та відповідають плану та структурі мереж, спроектованих у попередніх лабораторних роботах.

Наступним етапом виконання лабораторної роботи є моделювання роботи спроектованої міської комп'ютерної мережі відділень комерційного банку.

План виконання роботи

Для виконання даної лабораторної роботи необхідно виконати наступні дії:

1. Визначити ієрархію об'єктів міської комп'ютерної мережі відділень комерційного банку (рис. 3.4.5).

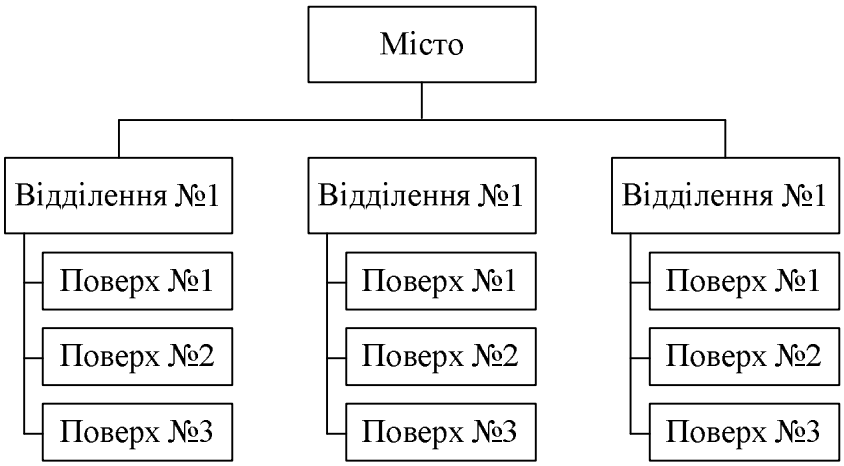


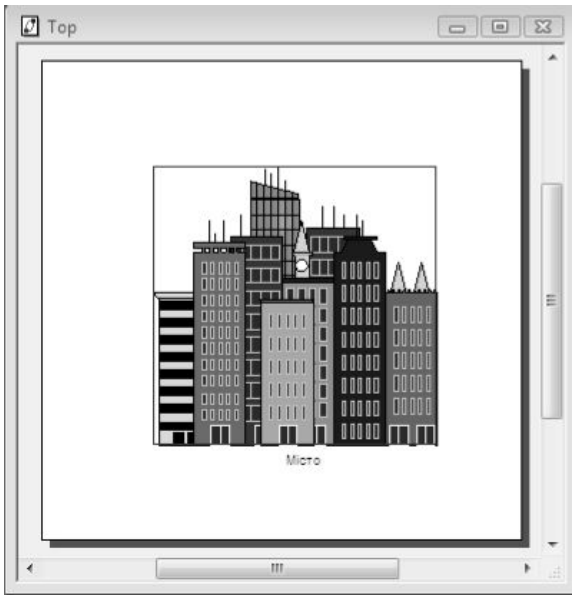
Рис. 3.4.5. Ієрархія об'єктів комп'ютерної мережі

2. Зробити декомпозицію об'єктів міської комп'ютерної мережі до поверхів відділень комерційного банку (рис. 3.4.6).
3. Для кожного поверху необхідно використати план приміщень, сформований у попередніх лабораторних роботах (рис. 3.4.6, г).
4. Установити зв'язки між відділеннями й поверхами відділень. У підсумку повинна вийти єдина міська мережа, яка буде спроектована за технологіями Fast Ethernet (на рівні поверхів) і FDDI або WiMAX (між відділеннями) (рис. 3.4.6).
5. Провести імітаційне моделювання міської комп'ютерної мережі відділень комерційного банку (рис. 3.4.6).

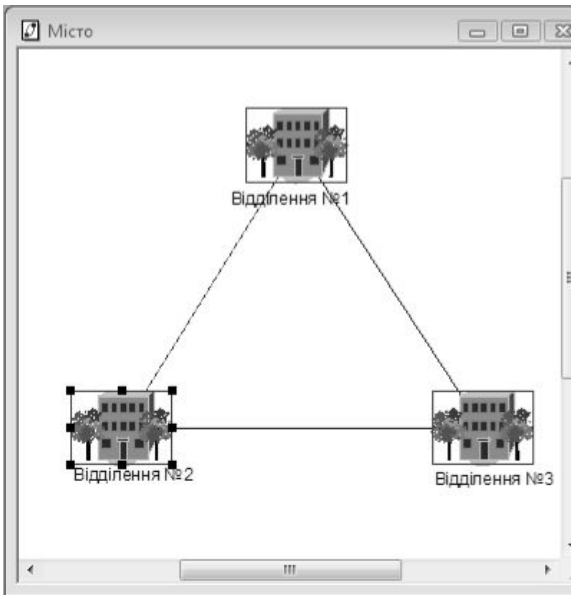
Питання для захисту роботи

1. Дайте характеристику класу комп'ютерних мереж "міська мережа". Які відмінні ознаки має даний клас у порівнянні із класами "локальні" та "глобальні мережі"?
2. Які характеристики технології WiMAX Вам відомі?
3. Які характеристики технології FDDI Вам відомі?
4. Які типи абонентів застосовуються в мережах FDDI?
5. Які типи концентраторів застосовуються в мережах FDDI?
6. Яким чином забезпечується надійна робота мережі, спроектованої за технологією FDDI, при одиночному ушкодженні мережевого кабелю?
7. Перерахуйте основні етапи створення ієрархічного проекту в інструментальному середовищі NetCracker Professional?

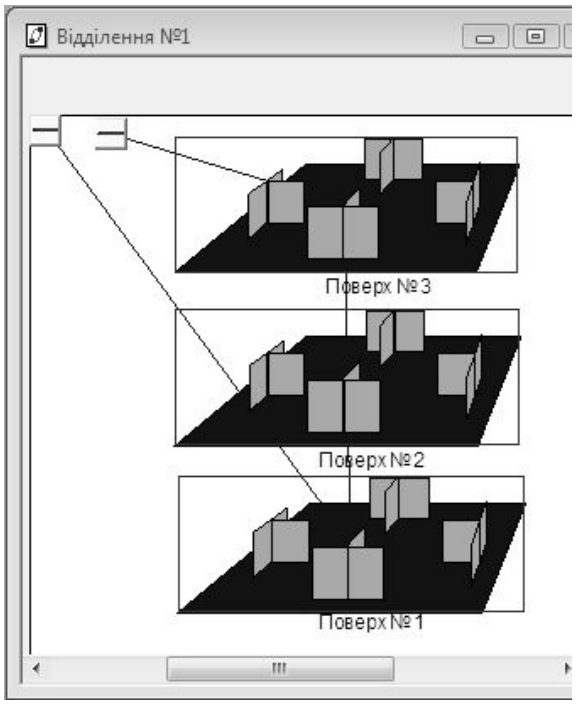
ЛІТЕРАТУРА: [5, 11, 31, 32].



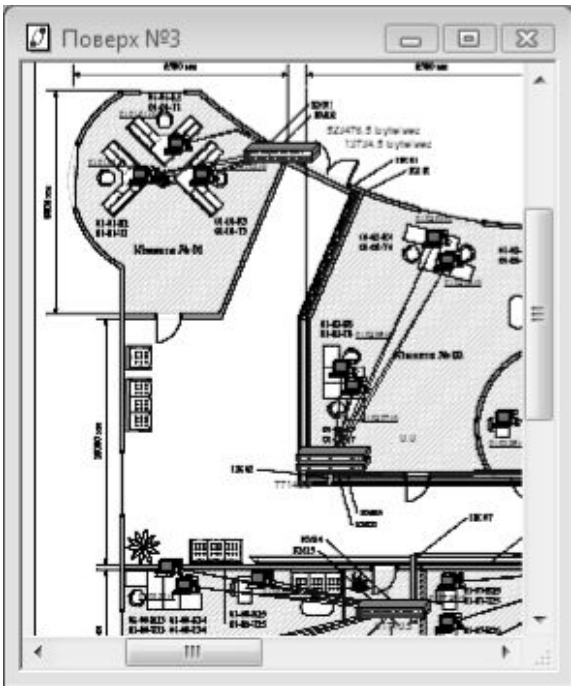
а) об’єкт City



б) об’єкти відділень банку



в) об’єкти поверхів відділення комерційного банку



г) об’єкт поверху відділення банку (план приміщень)

Рис. 3.4.6. Структура комп’ютерної міської мережі відділень комерційного банку в інструментальному середовищі NetCracker Professional

Лабораторна робота № 5
Тема “IP-АДРЕСАЦІЯ МІСЬКОЇ КОМП’ЮТЕРНОЇ МЕРЕЖІ ВІДДІЛЕНЬ КОМЕРЦІЙНОГО БАНКУ”

Мета роботи: одержати навички призначення IP-адрес і розподілу міської мережі на підмережі.

Методичні вказівки

Мережеві IP-адреси

Для того, щоб об’єднати мережі TCP/IP, необхідна глобальна система адресації, яка *не залежить від способів адресації вузлів в окремих мережах.* Ця система адресації повинна універсальним і однозначним способом ідентифікувати будь-який інтерфейс складеної мережі. Очевидним рішенням є унікальна нумерація всіх мереж складеної мережі, а потім нумерація всіх вузлів у межах кожної із цих мереж. Пара, що складається з номера мережі та номера вузла, відповідає поставленим умовам і може служити як мережева адреса.

Номером вузла може бути або локальна адреса (MAC-адреса) цього вузла (така схема прийнята у стеці IPX/SPX), або деяке число, ніяк не пов’язане з локальною технологією, та яке однозначно ідентифікує вузол у межах даної підмережі. У першому випадку мережева адреса стає залежною від локальних технологій, що обмежує її застосування. Наприклад, мережеві адреси IPX/SPX розраховані на роботу в складених мережах, що поєднують мережі, у яких використовуються тільки MAC-адреси або адреси аналогічного формату. Другий підхід більш універсальний, він характерний для стека TCP/IP.

У термінах стека протоколів TCP/IP мережеву адресу називають *IP-адресою*.

Кожного разу, коли пакет направляється адресатові через складену мережу, у його заголовку вказується IP-адреса вузла призначення. По номеру мережі призначення кожний наступний маршрутизатор знаходить IP-адресу наступного маршрутизатора.

Перед тим, як відправити пакет у наступну мережу, маршрутизатор повинен визначити на підставі знайденої IP-адреси наступного маршрутизатора його локальну адресу. Для цього протокол IP, як показано на рис. 3.5.1, звертається до протоколу дозволу адрес (ARP).

Формат IP-адреси

У заголовку IP-пакета для зберігання IP-адрес відправника й одержувача виділяються два поля, кожне має фіксовану довжину 4 байти (32 біти). IP-адреса складається із двох логічних частин – номера мережі та номера вузла в мережі.

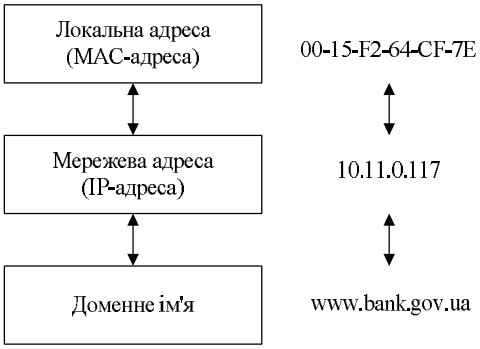


Рис. 3.5.1. Перетворення адрес

Найпоширенішою формою представлення IP-адреси є запис у вигляді чотирьох чисел, які представляють значення кожного байта в десятковій формі та розділені крапками, наприклад:

- IP-адреса у десятковому форматі: 128.10.2.30;
- IP-адреса у двійковому форматі: 10000000 00001010 00000010 00011110;
- IP-адреса у шістнадцятковому форматі: 80.0A.02.1D.

Слід зазначити, що запис адреси не передбачає *спеціального розмежувального знаку* між номером мережі та номером вузла. Разом з тим, при передачі пакета по мережі часто виникає необхідність розділити адресу на ці дві частини. Наприклад, маршрутизація, як правило, здійснюється на підставі номера мережі, тому кожний маршрутизатор, одержуючи пакет, повинен прочитати з відповідного поля заголовка адресу призначення та виділити з неї номер мережі. Для встановлення межі між номером мережі та номером вузла існує два основні підходи.

Перший, найпоширеніший донедавна, *підхід* до розподілу IP-адрес полягає у використанні класів адрес. Межа між номером мережі та номером вузла в IP-адресі може бути розташованою в різних позиціях. На початковому етапі розвитку комп'ютерних мереж припустимими позиціями межі були межі байтів IP-адреси. Відповідно до конкретного місця розподілу вводилися п'ять класів адрес: A, B, C, D, E. Три з них – A, B та C – використовувалися для адресації мереж, а два – D і E – мали спеціальне призначення.

Сьогодні, як правило, застосовується інший підхід для призначення IP-адрес, заснований на застосуванні маски, а саме *безкласова адресація (Classless Inter Domain Routing – CIDR)*. Використання цього підходу дозволяє більш гнучко керувати простором IP-адрес, не використовуючи жорстких рамок класової адресації. Безкласова адресація грунтується на використанні *мережевих масок змінної довжини (Variable Length Mask Length – VLSM)*, які не обов'язково мають зада-

вати розподіл між номером мережі та номером вузла на межі байту, тоді як в класовій адресації довжина масок строго фіксована. Цей підхід дозволяє економно використовувати IP-адреси.

Класи IP-адрес

Ознакою, на підставі якої IP-адреса належить до того або іншого класу, є значення кількох перших бітів адреси. У табл. 3.5.1 проілюстровано структуру IP-адрес різних класів.

Таблиця 3.5.1

Класи IP-адрес

Клас	Перші біти	Найменший номер мережі	Найбільший номер мережі	Максимальне число вузлів у мережі
A	0	1.0.0.0	126.0.0.0	2^{24} (поле 3 байти)
B	10	128.0. 0.0	191. 255.0.0	2^{16} (поле 2 байти)
C	110	192.0. 0.0	223. 255.255.0	2^{8} (поле 1 байт)
D	1110	224.0. 0.0	239. 255.255.255	Групові адреси
E	11110	240.0. 0.0	247. 255.255.255	Зарезервований

До класу A належить адреса, у якій старший біт має значення 0. В адресах класу A під ідентифікатор мережі приділяється 1 байт, а інші 3 байти інтерпретуються як номер вузла в мережі. Мережі, усі IP-адреси яких мають значення першого байта в діапазоні від 1 (00000001) до 126 (01111110), називаються мережами класу A. Значення 0 (00000000) першого байта не використовується, а значення 127 (01111111) зарезервовано для спеціальних цілей. Мереж класу A порівняно небагато, але кількість вузлів у них може досягати 2^{24}, тобто 16 777 216 вузлів.

До класу B належать всі адреси, старші два біти яких мають значення 10. В адресах класу B під номер мережі та під номер вузла приділяється по два байти. Мережі, значення перших двох байтів адрес яких перебувають у діапазоні від 128.0. (10000000 00000000) до 191.255(10111111 11111111), називаються мережами класу B. Очевидно, що мереж класу B більше, ніж мереж класу A, а розміри їх менше. Максимальна кількість вузлів у мережах класу B становить 2^{16} (65 536).

До класу C належать всі адреси, старші три біти яких мають значення 110. В адресах класу C під номер мережі приділяється 3 байти, а під номер вузла – 1 байт. Мережі, старші три байти яких перебувають у діапазоні від 192.0.0 (11000000 00000000 00000000) до 223.255 (11011111 11111111 11111111), називаються мережами класу C. Ме-

режі класу С найпоширеніші та мають найменше максимальне число вузлів – 2^8 (256).

Якщо адреса починається з послідовності 1110, то вона є адресою класу D і позначає особливу, групову адресу (multicast address). У той час, як адреси класів A, B і C використовуються для ідентифікації окремих мережевих інтерфейсів, тобто є індивідуальними адресами (unicast address), групова адреса ідентифікує групу мережевих інтерфейсів, які в загальному випадку можуть належати різним мережам. Інтерфейс, що входить у групу, одержує поряд зі звичайною індивідуальною IP-адресою ще одну групову адресу. Якщо при відправленні пакета як адреса призначення зазначена адреса класу D, то такий пакет повинен бути доставлений всім вузлам, які входять у групу.

Якщо адреса починається з послідовності 11110, то це значить, що дана адреса належить до класу E. Адреси цього класу зарезервовані для майбутніх застосувань.

Щоб одержати з IP-адреси номер мережі та номер вузла, потрібно не тільки розділити адресу на дві відповідні частини, але й доповнити кожну з них нулями до повних 4 байтів. Візьмемо, наприклад, адресу класу B – 129.64.134.5. Перші два байти ідентифікують мережу, а наступні два – вузол. Таким чином, номером мережі є адреса 129.64.0.0, а номером вузла – адреса 0.0.134.5.

Використання масок при IP-адресації

Супроводжуючи кожну IP-адресу маскою, можна відмовитися від понять класів адрес і зробити більш гнучкою систему адресації.

Нехай, наприклад, для IP-адреси 129.64.I34.5 зазначена маска 255.255.128.0, тобто у двійковому виді IP-адреса 129.64.134.5/17 – це:

10000001.01000000.10000110.00000101,

а маска 255.255.128.0 – це:

11111111.11111111.1000000000000000.

Якщо ігнорувати маску й інтерпретувати адресу 129.64.134.5 на основі класів, то номером мережі є 129.64.0.0, а номером вузла – 0.0.134.5 (оскільки адреса належить до класу B).

Якщо ж використати маску, то 17 послідовних двійкових одиниць у масці 255.255.128.0, “накладені” на IP-адресу 129.64.134.5, ділять її на дві частини:

- номер мережі: 10000001.01000000.1;
- номер вузла: 0000110.00000101.

У десятковій формі запису номери мережі та вузла, доповнені нулями до 32 біт, виглядають, відповідно, як 129.64.128.0 і 0.0.6.5.

Накладення маски можна інтерпретувати як виконання логічної операції “І” (AND). Так, у попередньому прикладі номер мережі з адреси 129.64.134.5 є результатом виконання логічної операції AND з маскою 255.255.128.0:

10000001 01000000 10000110 00000101

AND

11111111.11111111.10000000.00000000

Для стандартних класів мереж маски мають наступні значення:

- клас А – 11111111. 00000000. 00000000. 00000000 (255.0.0.0);
- клас В – 11111111. 11111111.00000000.00000000(255.255.0.0);
- клас ІЗ – 11111111. 11111111. 11111111.00000000(255.255.255.0).

Механізм використання масок змінної довжини широко розповсюджений в IP-маршрутизації, причому маски можуть використовуватися для різних цілей. За їхньою допомогою адміністратор може розбивати одну, виділену йому постачальником послуг мережу певного класу, на декілька інших, не вимагаючи додаткових номерів мереж – ця операція називається *поділом на підмережі (subnetting)*. На основі цього ж механізму постачальники послуг можуть поєднувати адресні простори декількох мереж шляхом введення так званих “префіксів” для зменшення обсягу таблиць маршрутизації та підвищення за рахунок цього продуктивності маршрутизаторів – така операція називається *об’єднанням підмереж (supernetting)*.

Варто відзначити, що для передачі інформації всім абонентам підмережі застосовується широкомовна адреса.

Широкомовна адреса – це адреса, яка забезпечує передачу пакетів всім абонентам підмережі.

Порядок призначення IP-адрес

За визначенням схема IP-адресації повинна забезпечувати унікальність нумерації мереж, а також унікальність нумерації вузлів у межах кожної з мереж. Отже, процедури призначення номерів як мережам, так і вузлам мереж, повинні бути *централізованими.*

Призначення адрес автономної (приватної) мережі

Коли справа стосується мережі, яка є частиною Інтернету, унікальність нумерації може бути забезпечена тільки зусиллями спеціально створених для цього центральних органів. У невеликій же автономній IP-мережі умова унікальності номерів мереж і вузлів може бути виконана силами мережевого адміністратора.

У цьому випадку в розпорядженні адміністратора є весь адресний простір, тому що збіг IP-адрес у незв'язаних між собою мережах не викличе ніяких негативних наслідків. Адміністратор може вибирати адреси довільно, дотримуючись лише синтаксичних правил, ураховуючи обмеження на особливі адреси.

Однак при такому підході виключена можливість у майбутньому приєднати дану мережу до Інтернету. Дійсно, довільно обрані адреси даної мережі можуть збігтися із централізовано призначеними адресами Інтернету. Для того, щоб уникнути колізій, пов'язаних з такого роду збігами, у стандартах Інтернету визначено декілька так званих приватних адрес, які рекомендують для автономного використання:

- у класі A – мережа 10.0.0.0;
- у класі B – діапазон з 16 мереж – 172.16.0.0-172.31.0.0;
- у класі C – діапазон з 255 мереж – 192.168.0.0-192.168.255.0.

Ці адреси виключені з адрес, які розподіляються централізовано, і становлять величезний адресний простір, достатній для нумерації вузлів автономних мереж практично будь-яких розмірів. Варто також відзначити, що приватні адреси, як і при довільному виборі адрес, у різних автономних мережах можуть збігатися. У той же час використання приватних адрес для адресації автономних мереж робить можливим коректне підключення їх до Інтернету.

Централізований розподіл адрес

У великих мережах, подібних до Інтернету, унікальність мережевих адрес гарантується централізованою, ієрархічно організованою системою їхнього розподілу. Номер мережі може бути призначений тільки за рекомендацією спеціального підрозділу Інтернету. Головним органом реєстрації глобальних адрес в Інтернеті з 1998 року є неурядова некомерційна організація *ICANN (Internet Corporation for Assigned Names and Numbers)*. Ця організація координує роботу регіональних відділів, діяльність яких охоплює великі географічні площі: ARIN (Америка), RIPE (Європа), APNIC (Азія й Тихоокеанський регіон). Регіональні відділи виділяють блоки адрес мереж великим постачальникам послуг, а ті, у свою чергу, розподіляють їх між своїми клієнтами, серед яких можуть бути й більш дрібні постачальники.

Проблемою централізованого розподілу адрес є їхній дефіцит. Вже порівняно давно дуже важко одержати адресу класу B та практично неможливо стати власником адреси класу A. При цьому треба відзначити, що дефіцит обумовлений не тільки зростанням кількості мереж, але й тим, що наявний адресний простір використовується нераціонально. Дуже часто власники мереж класу C витрачають лише

невелику частину з наявних у них 254 адрес. Розглянемо приклад, коли дві мережі необхідно з'єднати глобальним зв'язком. У таких випадках як лінію зв'язку використовують два маршрутизатори, з'єднаних за схемою "точка-точка" (рис. 3.5.2). Для такої мережі, яка утворена лінією зв'язку, що зв'язує порти двох суміжних маршрутизаторів, доводиться виділяти окремий номер мережі, хоча в цій мережі є всього два вузли.

Рис. 3.5.2. Приклад нераціонального використання простору IP-адрес

Для вирішення проблеми дефіциту IP-адрес розробники стека TCP/IP пропонують різні підходи. Принциповим рішенням є перехід на нову версію протоколу IP – протокол IPv6, у якому різко розширюється адресний простір за рахунок використання виділення на адресу 16 байтів (128 біт) замість 4 байтів (32 біти), як у протоколі IPv4.

Приклад IP-адресації

Необхідно призначити IP-адреси для всіх інтерфейсів в мережі, починаючи з адреси 172.16.20.0/25. Розрахувати кількість вузлів даної мережі.

На рис. 3.5.3 представлений приклад IP-адресації.

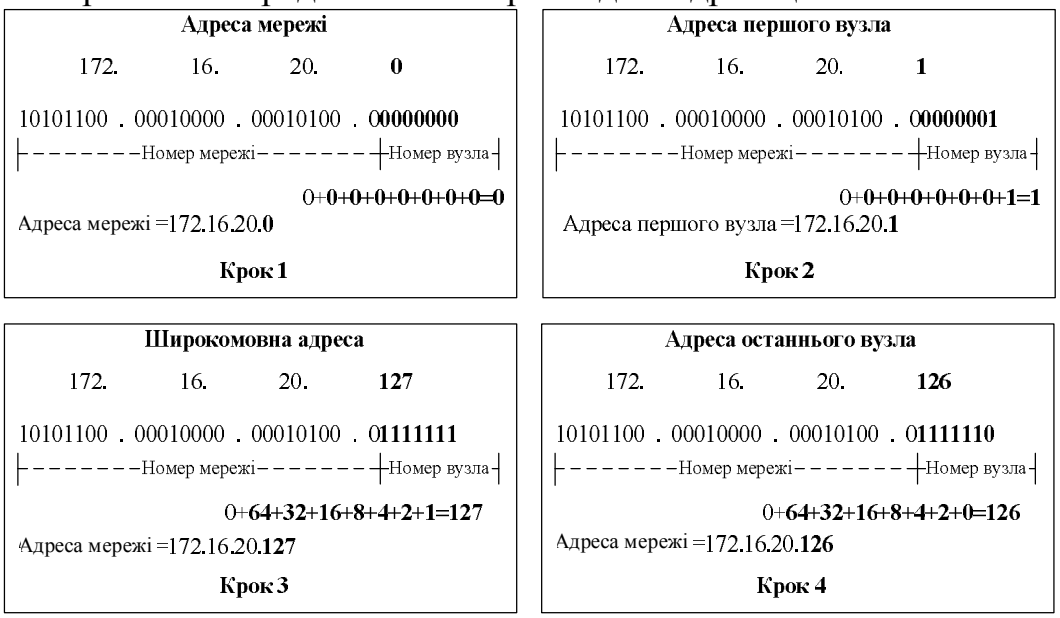


Рис. 3.5.3. Приклад IP-адресації

На першому кроці призначається адреса мережі. Маска мережі в цьому випадку включає 25 біт, а 7 останніх біт – це біти адрес робочих станцій. В адресі мережі останні 7 біт повинні приймати значення 0. У результаті була отримана адреса мережі 172.16.20.0 з маскою 255.255.255.128.

На другому кроці призначається адреса першого вузла в мережі. Адреса першого вузла в мережі є наступною адресою після адреси мережі. Для призначення першої, найнижчої адреси вузла в мережі останній сьомий біт повинен прийняти значення 1. У результаті ми маємо адресу 172.16.20.1 з маскою 255.255.255.128.

На третьому кроці визначається широкомовна адреса. У широкомовній адресі необхідно, щоб розряди вузла були встановлені в 1, тобто в даному прикладі сім останніх бітів повинні бути встановлені в 1. У такий спосіб в останньому октеті ми одержимо значення 127, що дає нам широкомовну адресу 172.16.20.127.

На четвертому кроці призначається адреса останнього вузла в мережі. Адреса останнього вузла в мережі завжди менше широкомовної адреси. Це означає, що в адресі останнього вузла мережі останній біт повинен бути встановлений в 0, а при широкомовному запиті в 1. У такий спосіб адреса останнього вузла в мережі буде 172.16.20.126.

Кількість вузлів даної мережі дорівнює 2^n-2, де n – кількість бітів, виділених для адресації вузлів. Одна адреса віднімається, оскільки вона призначається широкомовному запитові, а одна – оскільки вона призначається адресі мережі. Тобто у нашому випадку кількість вузлів буде 2^7-2, що дорівнює 126.

Завдання до роботи

Необхідно розробити схему IP-адресації для міської комп'ютерної мережі відділень комерційного банку, що була спроектована в ході виконання лабораторної роботи № 4.

Для цього необхідно призначити IP-адресу для кожного інтерфейсу маршрутизатора або комутатора третього рівня. Ґрунтуючись на структурі комп'ютерної мережі, необхідно визначити кількість підмереж, пам'ятаючи, що підмережі розділяються маршрутизаторами або комутаторами третього рівня. Далі для кожної підмережі слід призначити: IP-адресу, маску підмережі та адресу широкомовного запиту. Після цього необхідно в рамках визначених підмереж визначити початкову й кінцеву адреси для робочих станцій. Також необхідно розрахувати кількість вузлів кожної підмережі.

План виконання роботи

Для виконання лабораторної роботи необхідно виконати наступні дії:

- визначити кількість підмереж, пам'ятаючи, що підмережі розділяються маршрутизаторами або комутаторами третього рівня;

- для кожної підмережі призначити: IP-адресу, маску піжмережі, адресу широкомовного запиту;
- призначити IP-адресу для кожного інтерфейсу маршрутизатора або комутатора третього рівня;
- у рамках підмережі для робочих станцій призначити початкову та кінцеву IP-адреси;
- розрахувати кількість вузлів кожної підмережі.

Питання для захисту роботи

1. Які апаратні пристрої дозволяють розділити мережу на підмережі? На якому рівні моделі OSI вони працюють?
2. Що таке IP-адреса? Для чого вона необхідна?
3. Які класи мереж Вам відомі? За якою ознакою розділені ці мережі?
4. Що таке маска підмережі? Яку функцію вона виконує?
5. Опишіть процедуру призначення IP-адрес.

ЛІТЕРАТУРА: [1, 2, 5, 17, 25].

Лабораторна робота № 6
Тема “ВИВЧЕННЯ МЕТОДИКИ ОБТИСКУ МІДНОГО КАБЕЛЮ UTP”

Мета роботи: одержати практичні навички обтиску мідного кабелю UTP.

Методичні вказівки

Процедуру обтиску мідного кабелю UTP застосовують, коли необхідно підключити мережевий пристрій або робочу станцію до мережевої розетки або до іншого мережевого пристрою за технологією Fast Ethernet. Дана процедура полягає у встановленні на кінцях кабелю UTP роз’ємів RJ-45.

Перед початком обтиску необхідно визначити, для з’єднання яких типів пристроїв буде використаний сегмент UTP. Від цього залежить тип обтиску кабелю.

Існує два типи обтиску кабелю:

- обтиск прямого кабелю (Ethernet straight-through). Застосовується для з’єднання пристроїв різного типу, таких як робоча станція та комутатор, робоча станція та концентратор;
- обтиск зворотного кабелю (Ethernet crossover). Застосовується для з’єднання пристроїв одного типу, таких як робоча станція та робоча станція, концентратор та концентратор, маршрутизатор та маршрутизатор. Виключенням є з’єднання зворотним кабелем пристроїв різного типу, а саме робочої станції та маршрутизатора.

Після визначення типу обтиску кабелю UTP потрібно відміряти необхідну довжину та відрізати сегмент кабелю UTP. Варто переконатися, що кінці кабелю чисті та обрізані під прямим кутом (рис. 3.6.1).

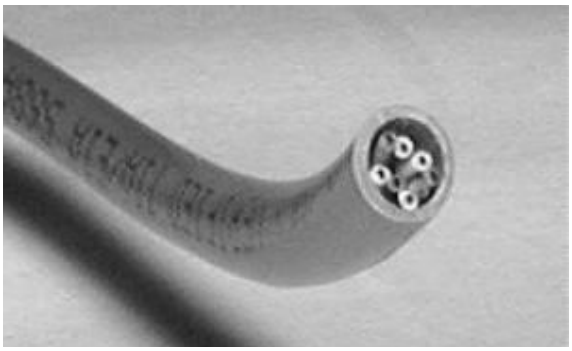
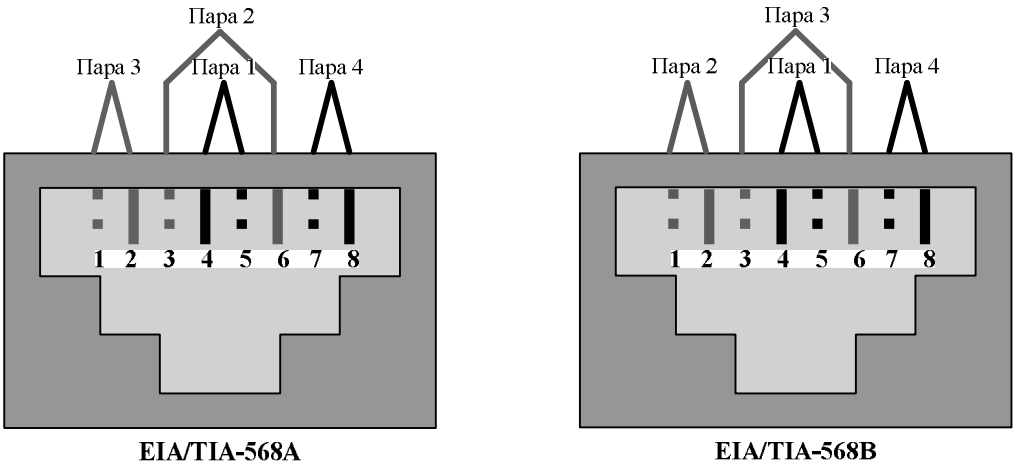


Рис. 3.6.1. Закінчення кабелю UTP

Далі варто розплести жили кабелю. Зверніть увагу, що усередині кабелю знаходяться 4 пари кольорових жил. Вони повинні бути відсортовані відповідно до типу обтиску кабелю. Послідовності кольорових жил для різних типів обтиску представлені на рис. 3.6.2.



EIA/TIA-568A

1 – зелено-білий
2 – зелений
3 – помаранчево-білий
4 – синій
5 – синьо-білий
6 – помаранчевий
7 – коричнево-білий
8 – коричневий

EIA/TIA-568B

1 – помаранчево-білий
2 – помаранчевий
3 – зелено-білий
4 – синій
5 – синьо-білий
6 – зелений
7 – коричнево-білий
8 – коричневий

Рис. 3.6.2. Послідовність кольорових жил відповідно до типів обтиску

При обтиску зворотного кабелю необхідно з однієї сторони розташувати кольорові жили у відповідності зі стандартом EIA/TIA-568A, а з іншої сторони – у відповідності зі стандартом EIA/TIA-568B. При обтиску прямого кабелю необхідно з обох сторін розташувати кольорові жили у відповідності зі стандартом EIA/TIA-568A або у відповідності зі стандартом EIA/TIA-568B.

Далі необхідно вирівняти жили в одну лінію, а потім відрізати міліметр або декілька міліметрів, щоб жили були однієї довжини й видавалися із зовнішньої ізоляції приблизно на сантиметр-півтора (рис. 3.6.3).

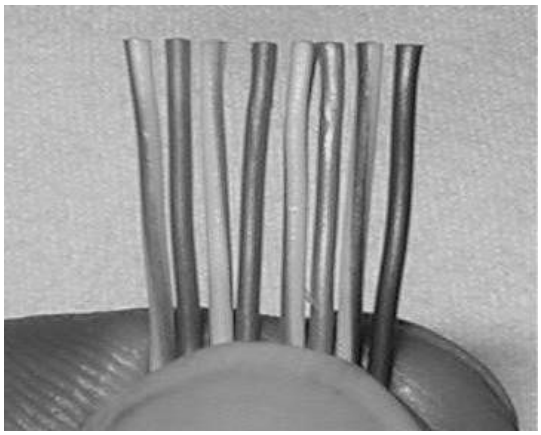


Рис. 3.6.3. Вирівнювання кольорових жил

Наступним кроком є з'єднання кабелю з конектором RJ-45. Для цього необхідно взяти конектор RJ-45 так, щоб пластиковий фіксатор дивився убік від Вас і вниз. Потім акуратно вставити відсортовані та вирівняні жили в конектор RJ-45. Усередині RJ-45 є направляючі, по одній на кожну жилу, які допомагають направити жили в потрібному напрямку та вставити їх до упору (рис. 3.6.4).

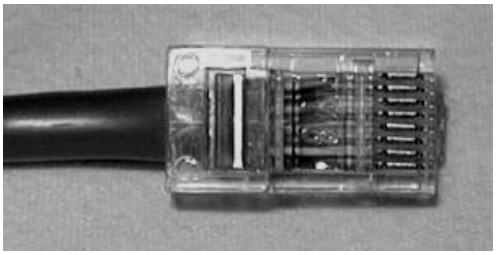


Рис. 3.6.4. Правильне з'єднання кабелю UTP з конектором RJ-45

На рис. 3.6.5 зображені неправильні варіанти з'єднання кабелю UTP з конектором RJ-45, а саме ліворуч жили занадто довгі й ізоляція не доходить до тримача, а праворуч жили занадто короткі та не доходять до контактної площадки.

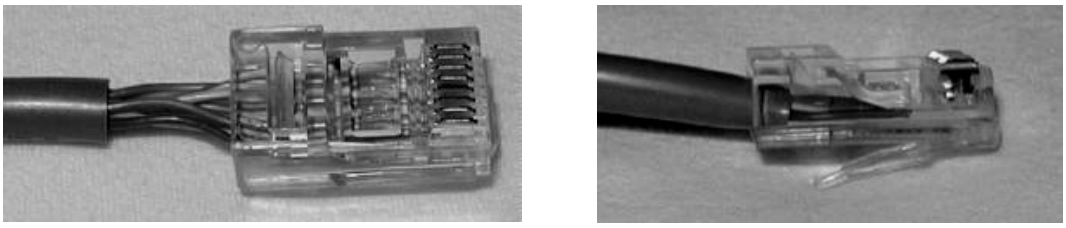


Рис. 3.6.5. Неправильне з'єднання кабелю UTP з конектором RJ-45

На останньому етапі необхідно вставити конектор RJ-45 у відповідне гніздо обтискного інструмента й плавно зімкнути ручки інструмента (рис. 3.6.6).

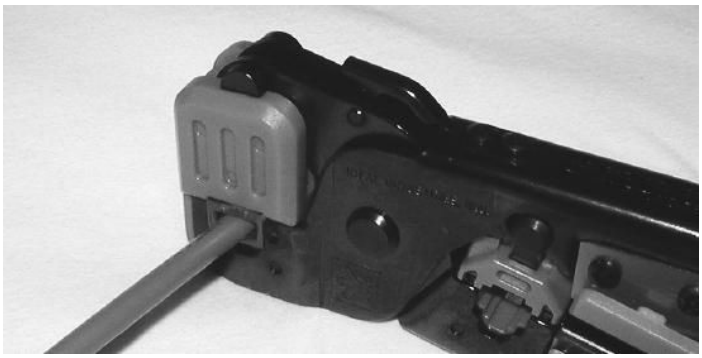


Рис. 3.6.6. Використання обтискного інструмента

Далі необхідно обжати інший кінець кабелю з урахуванням того, який тип кабелю Вам потрібен.

Після обтискання кабель необхідно протестувати, використовуючи спеціальний тестер (рис. 3. 6.7).

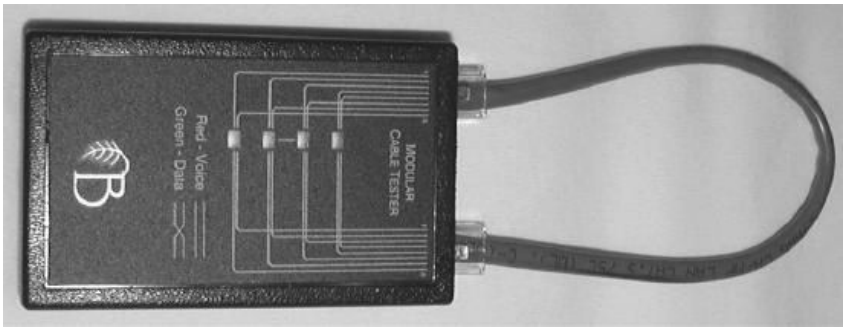


Рис. 3.6.7. Тестування обтиснутого кабелю

Завдання до роботи

Необхідно обтиснути прямий та зворотний кабелі UTP та протестувати їх працездатність.

План виконання роботи

1. Необхідно ознайомитися з методичними вказівками, описаними вище.

2. Слід переконатися, що всі необхідні елементи, які застосовуються при обтиску кабелю, у Вас є в наявності, а саме: кабель UTP, чотири конектори RJ-45 та інструмент для обтискання.
3. Обтиснути прямий кабель UTP.
4. Протестувати обтиснутий прямий кабель UTP.
5. Обтиснути зворотний кабель UTP.
6. Протестувати обтиснутий зворотний кабель UTP.

Питання для захисту роботи

1. Укажіть послідовність кольорових жил кабелю UTP при прямому обтиску.
2. Укажіть послідовність кольорових жил кабелю UTP при зворотному обтиску.
3. Для підключення яких типів пристроїв застосовується прямий кабель UTP?
4. Для підключення яких типів пристроїв застосовується зворотний кабель UTP?
5. Яким чином можна протестувати прямий кабель UTP за відсутності спеціального тестера?
6. Які дії необхідно виконати, якщо довжина кольорових жил кабелю UTP при обтиску вийшла короткою та жили не доходять до контактної площадки?
7. Які дії необхідно виконати, якщо довжина кольорових жил кабелю UTP при обтиску вийшла довгою та ізоляція не доходить до тримача конектора RJ-45?

ЛІТЕРАТУРА: [22, 28, 29].

Лабораторна робота № 7
Тема “КОНФІГУРУВАННЯ МЕРЕЖЕВОГО IP-ЕКРАНУ З ВИКОРИСТАННЯМ ПОЛІТИК ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS XP”

Мета роботи: дослідження властивостей мережевих екранів, набуття навичок конфігурування політик IP-безпеки Windows XP.

Методичні вказівки

Для виконання даної роботи рекомендується використовувати програмне забезпечення для створення і налаштування віртуальних комп’ютерів Microsoft Virtual PC 2007 та віртуальні комп’ютери із встановленими операційними системами Windows XP.

Мережеві екрани відіграють надзвичайно важливу роль у забезпеченні захисту інформації в мережах. Мережеві екрани встановлюються на

межі між довіреними і недовіреними мережами, причому всі з'єднання повинні проходити через мережевий екран, оскільки лише в такому випадку буде здійснюватись фільтрація вхідного і вихідного трафіку. У випадку, коли передача даних може бути здійснена в обхід мережевого екрану, весь сенс використання мережевого екрану втрачається. *Довірена мережа* – це мережа, при роботі в якій комп'ютер не піддається атакам і спробам несанкціонованого доступу до даних. Якщо мережа довірена – буде дозволена будь-яка мережева активність у рамках цієї мережі.

Доступ до політик налаштування вбудованого мережевого екрану здійснюється за допомогою меню "*Панель управления \ Администрирование \ Локальная политика безопасности*" (рис. 3.7.1).

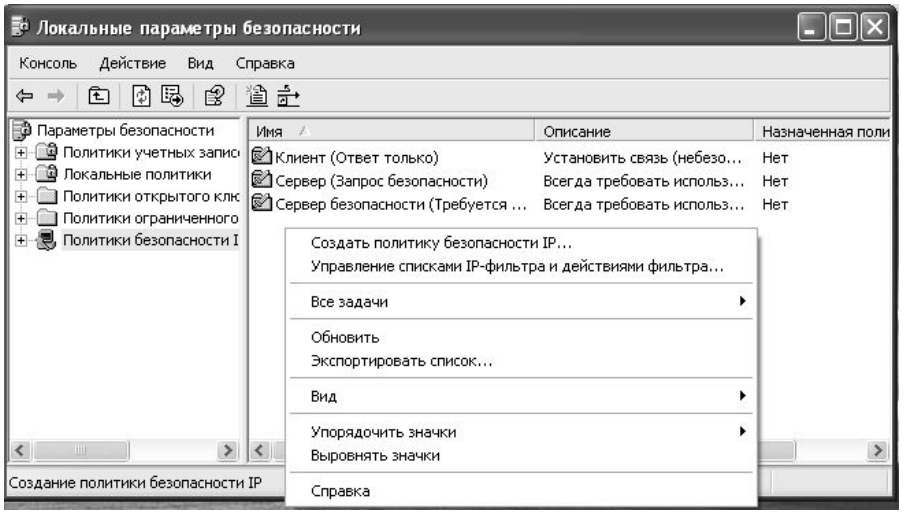


Рис. 3.7.1. Діалог створення нової політики безпеки

При виборі меню створення нової політики безпеки буде запущено майстер створення політик (рис. 3.7.2).

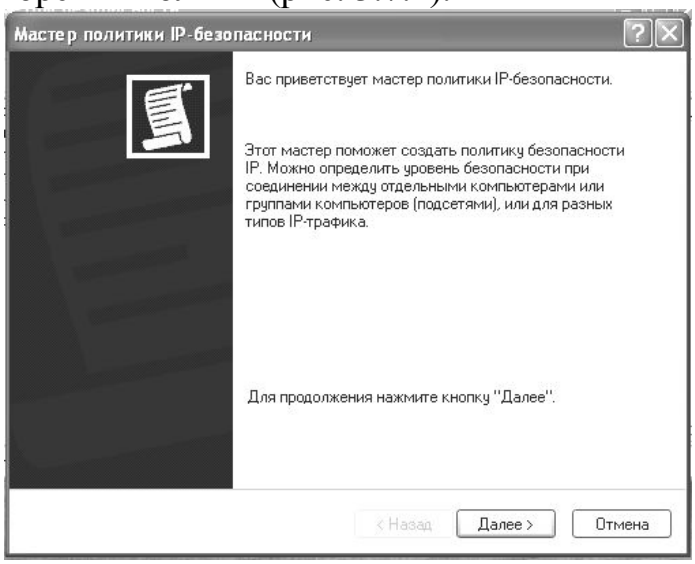


Рис. 3.7.2. Вікно майстра створення політики

За допомогою майстра користувач може вибрати назву політики, її опис, вибрати метод перевірки автентичності для правила безпеки. На початковому етапі створення політики рекомендується залишити все за замовчуванням. Після проходження кроків майстра створення політики безпеки користувачу буде запропоновано змінити властивості новоствореної політики (рис. 3.7.3).

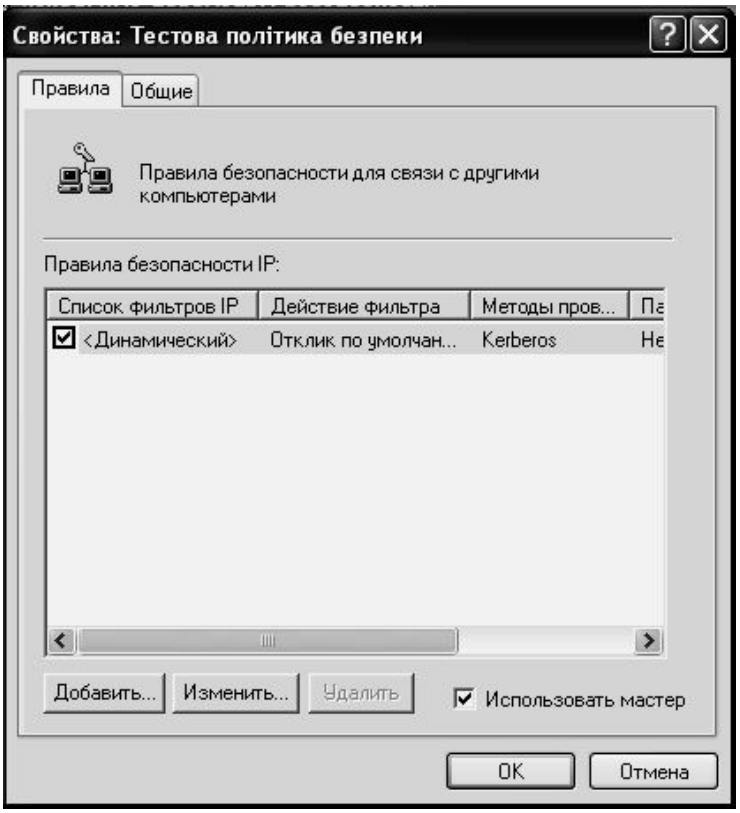


Рис. 3.7.3. Вікно властивостей політики безпеки

Надалі потрібно створити правила для фільтрації. При додаванні нового правила можна скористатись майстром IP-безпеки, що буде доцільно на початкових етапах налаштування політик, для цього необхідно залишити вибраною опцію *“Использовать мастер”*. Правила безпеки містять у собі набір дій щодо забезпечення безпеки, які виконуються, коли підключення підпадає під певний критерій у списку фільтрів. При додаванні нового правила (рис. 3.7.4) відкриється вікно з налаштуваннями функцій даного правила.

У випадку використання майстра наведене вікно відкриється по завершенню його роботи. При створенні правил політики безпеки рекомендується скористатися правилом: “Заборонено все, що не дозволено”, тобто потрібно заборонити всі підключення, а потім створити правила з дозволу певного виду трафіка. Оскільки правила дозволу мають більш високий пріоритет перед правилами заборони, то правило забо-

рони буде впливати лише на той вид трафіка, який не має прямого дозволу. На вкладці "*Список фильтров IP"* створюються фільтри, а на вкладці "*Действие фильтра"* потрібно вибрати дію, яку буде виконувати створений фільтр, у випадку блокування всього трафіка, який явно не дозволений, потрібно вибрати дію "*Блокировать"* (рис. 3.7.5).

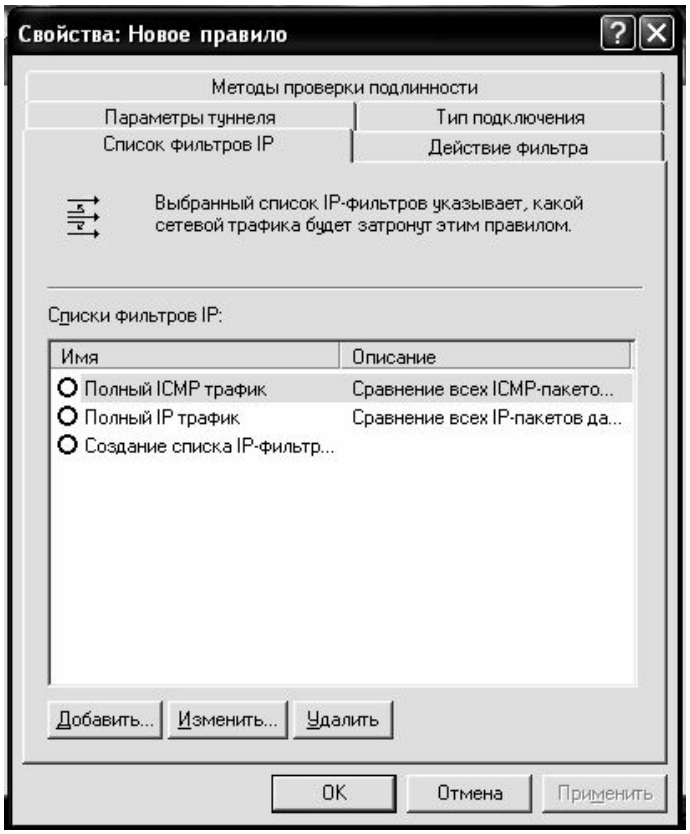


Рис. 3.7.4. Опції налаштування нового правила безпеки

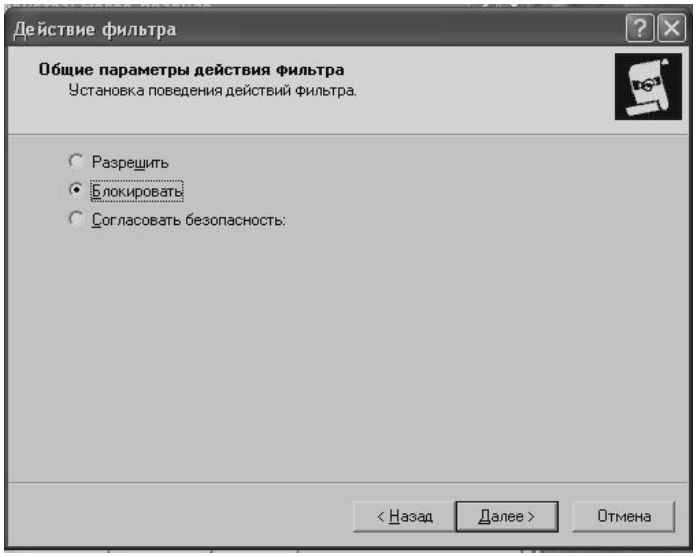


Рис. 3.7.5. Вибір дії фільтру

Відповідно, при створенні правил дозволу, потрібно вибирати дію "*Разрешить".* Після вибору дії фільтра в новоствореній політиці з'явилося правило, що забороняє проходження будь-якого трафіка. Для того щоб політика запрацювала, потрібно її призначити (клацнути правою кнопкою миші по назві політики і вибрати *"Назначить")*.

Після того, як було створено правило заборони, потрібно зробити відповідні дозволи для потрібних протоколів і адрес комп'ютерів в мережі. Для цього у новостворену політику слід додати нове правило дозволу проходження пакетів, наприклад, для протоколу ICMP (рис. 3.7.6).

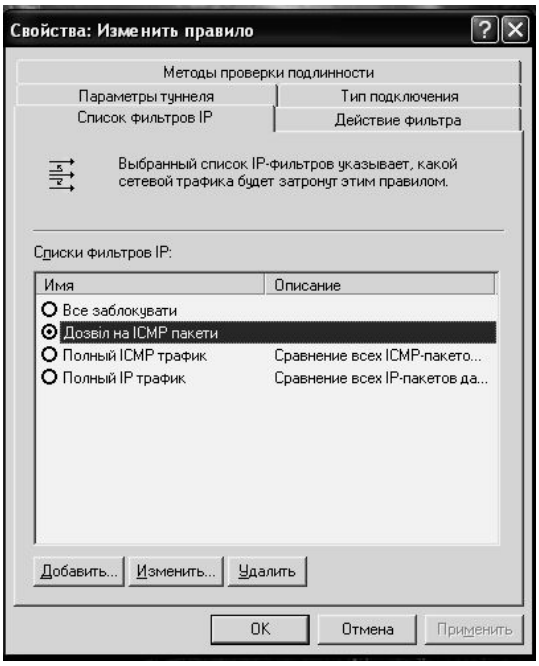


Рис. 3.7.6. Створення фільтра на дозвіл проходження ICMP-пакетів

Для того, щоб дозвіл на проходження пакетів за протоколом ICMP стосувався лише окремих IP-адрес, потрібно визначити ці адреси на вкладці адресації у властивостях фільтра (рис. 3.7.7).

Після створення фільтра необхідно вибрати для нього дію із тих, що вже створені, або ж створити нову (рис. 3.7.8).

Для перевірки роботи налаштувань мережевого екрану рекомендується скористуватися командою "*ping+адреса"*.

Завдання до роботи

Об'єктом дослідження виступає комп'ютер із встановленою операційною системою Windows XP. За допомогою вбудованих політик IP-безпеки потрібно налаштувати доступ до окремих протоколів передачі даних.

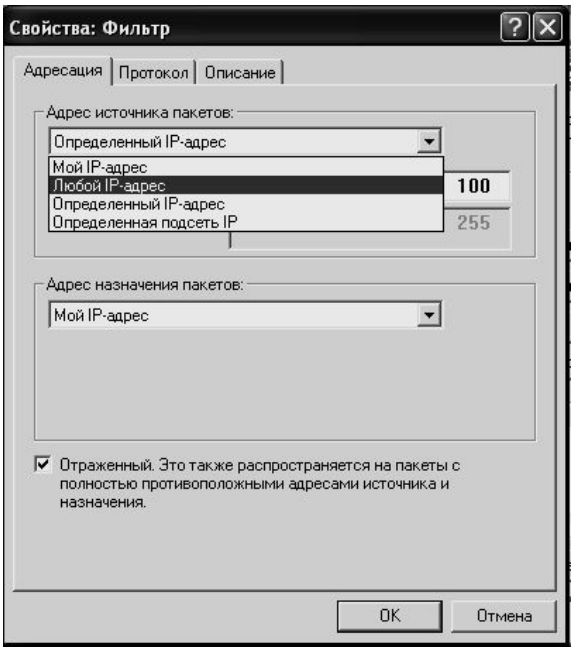


Рис. 3.7.7. Вибір адресації для фільтра

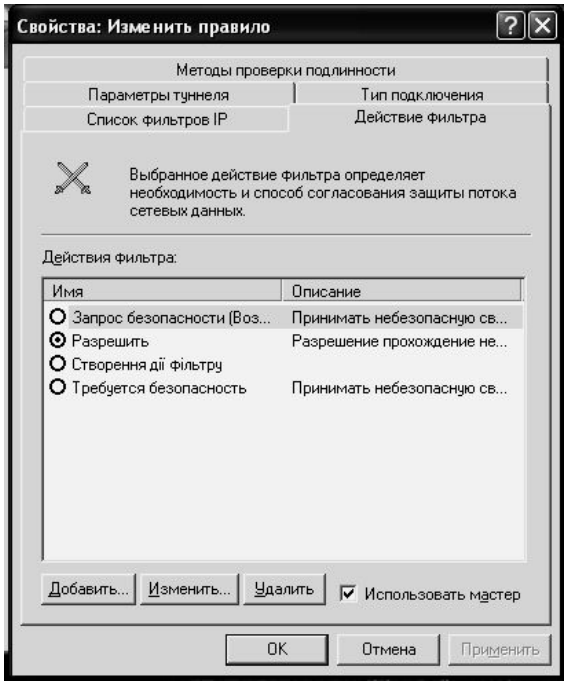


Рис. 3.7.8. Вибір дії для фільтра

Оскільки заборона дозволу для різних протоколів відбувається однотипним чином, то пропонується для лабораторної роботи, використовувати протокол ICMP. Відповідно до виданого варіанта, необхідно із табл. 3.7.1 вибирати діапазон IP-адрес для дозволу проходження пакетів протоколом ICMP, проходження пакетів із інших адрес повинно бути заборонено. Також у кожного діапазону є додат-

кова IP-адреса. Якщо вказана адреса входить до первинного діапазону, то потрібно додатково заборонити надходження запитів із вказаної адреси, якщо адреса не входить до вказаного діапазону, то, навпаки, дозволити доступ із додаткової IP-адреси.

Таблиця 3.7.1

Варіанти завдань до лабораторної роботи

№ варіанта	Діапазон для дозволу доступу	Додаткова адреса
1	192.168.1.0-192.168.1.63	192.168.1.150
2	192.168.1.64-192.168.1.127	192.168.1.151
3	192.168.1.128-192.168.1.191	192.168.1.152
4	192.168.1.192-192.168.1.255	192.168.1.153
5	192.168.1.0-192.168.1.63	192.168.1.154
6	192.168.1.64-192.168.1.127	192.168.1.155
7	192.168.1.128-192.168.1.191	192.168.1.156
8	192.168.1.192-192.168.1.255	192.168.1.157
9	192.168.1.0-192.168.1.63	192.168.1.158
10	192.168.1.64-192.168.1.127	192.168.1.159
11	192.168.1.128-192.168.1.191	192.168.1.160
12	192.168.1.192-192.168.1.255	192.168.1.161
13	192.168.1.0-192.168.1.63	192.168.1.162
14	192.168.1.64-192.168.1.127	192.168.1.163
15	192.168.1.128-192.168.1.191	192.168.1.164

План виконання роботи

1. Відповідно до виданого викладачем варіанта вибрати завдання.
2. Налаштувати мережевий адаптер віртуального комп'ютера таким чином, щоб він входив до мережі 192.168.1.0/24.
3. Створити налаштування для мережевого екрану відповідно до обраного варіанта та приведених у роботі рекомендацій. Особливо акцентувати увагу на тому, що після створення нової політики безпеки її потрібно буде задіяти, оскільки за замовчуванням вона буде неактивною.
4. Перевірити дію мережевого екрану. Для перевірки дії створеної політики безпеки потрібно скористатися додатковим віртуальним комп'ютером із встановленою операційною системою Windows XP. Сама перевірка повинна здійснюватися з використанням ко-

манди "*ping"*. На додатковому комп'ютері почергово встановлюються IP-адреси, що входять до діапазону адрес, із якими дозволений зв'язок, потім, що не входять до даного діапазону, і, на завершення, перевіряється додаткова IP-адреса.

Питання до захисту роботи

1. Які існують типи мережевих екранів, чим вони відрізняються?
2. Яке призначення мережевого екрану, де він повинен бути встановлений?
3. Яке призначення протоколу ICMP?
4. Функціонування мережевого екрану із пакетною фільтрацією.
5. Основні принципи роботи мережевого екрану прикладного рівня.
6. Які наявні рішення мережевих екранів і яких компаній Ви можете назвати?
7. Яким чином здійснюється доступ до налаштувань IP-політик в операційній системі Windows XP?

ЛІТЕРАТУРА: [21, 27].

Лабораторна робота № 8
Тема "КОНФІГУРУВАННЯ ПЕРСОНАЛЬНОГО МЕРЕЖЕВОГО ЕКРАНУ З ПАКЕТНОЮ ФІЛЬТРАЦІЄЮ"

Мета роботи: дослідити властивості мережевих екранів, набути навички з конфігурування персонального мережевого екрану.

Методичні вказівки

Для виконання даної роботи рекомендується використовувати програмне забезпечення для створення і налаштування віртуальних комп'ютерів Microsoft Virtual PC 2007 та віртуальних комп'ютерів з операційною системою Windows XP.

Хоча використання вбудованих політик операційної системи Windows XP може видатися ефективним методом заборони певного виду трафіка, однак недружній інтерфейс даного засобу не дозволяє повною мірою задовольнити потреби користувачів. Налаштування дозволу і заборони доступу до операційної системи за обраними протоколами і IP-адресами відбувається не прозоро, тому використання даного механізму є недостатньо зручним.

Як правило, мережеві екрани, які пропонуються сторонніми розробниками, мають зручний інтерфейс, їх легко налаштувати, крім того, вони можуть мати додаткові функції, наприклад, вбудований антивірус тощо. Також, серед мережевих екранів, які присутні на ринку, існують безкоштовні варіанти та умовно-безкоштовні варіанти, на-

приклад: Comodo Free Firewall, Kaspersky Anti-Hacker, ZoneAlarm, Kaspersky Internet Security, Kerio Personal Firewall та інші.

Налаштувати персональний мережевий екран досить просто. Окрім зручного інтерфейсу (рис. 3.8.1), деякі з них мають спеціальні режими "навчання", де за допомогою підказок користувач може налаштувати режим функціонування мережевого екрану.

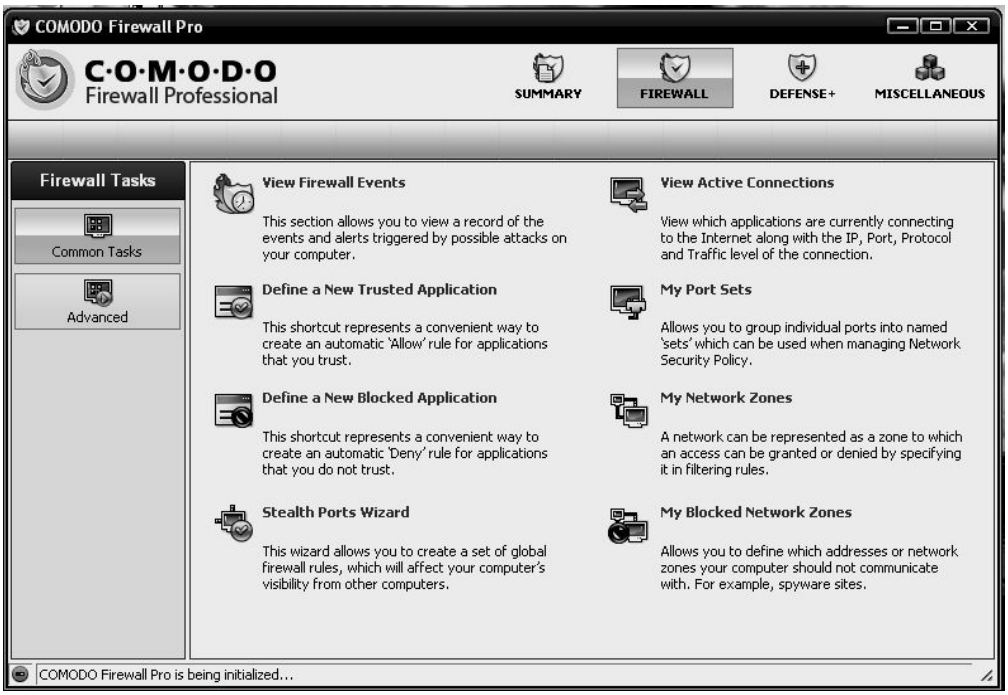


Рис. 3.8.1. Вікно безкоштовного мережевого екрану COMODO Firewall Pro

Крім того, при використанні стороннього мережевого екрану досить просто встановлювати розподіл для дозволу чи заборони доступу до даного комп'ютера. Наприклад, при використанні персонального мережевого екрану "COMODO Firewall Professional" для створення діапазону IP-мереж, із яких дозволений доступ до даного комп'ютера, достатньо вибрати опцію "My Network Zones" (рис. 3.8.2) та додати нову зону, призначивши їй ім'я та зробивши відповідні налаштування (рис. 3.8.3).

Розподіл за зонами інтуїтивно зрозумілий і не потребує додаткових розрахунків маски мережі від користувача. Таким чином, можна надавати доступ чи, навпаки, забороняти його до даного комп'ютера окремим IP-адресам, фізичним (MAC) адресам, за ім'ям комп'ютера тощо.

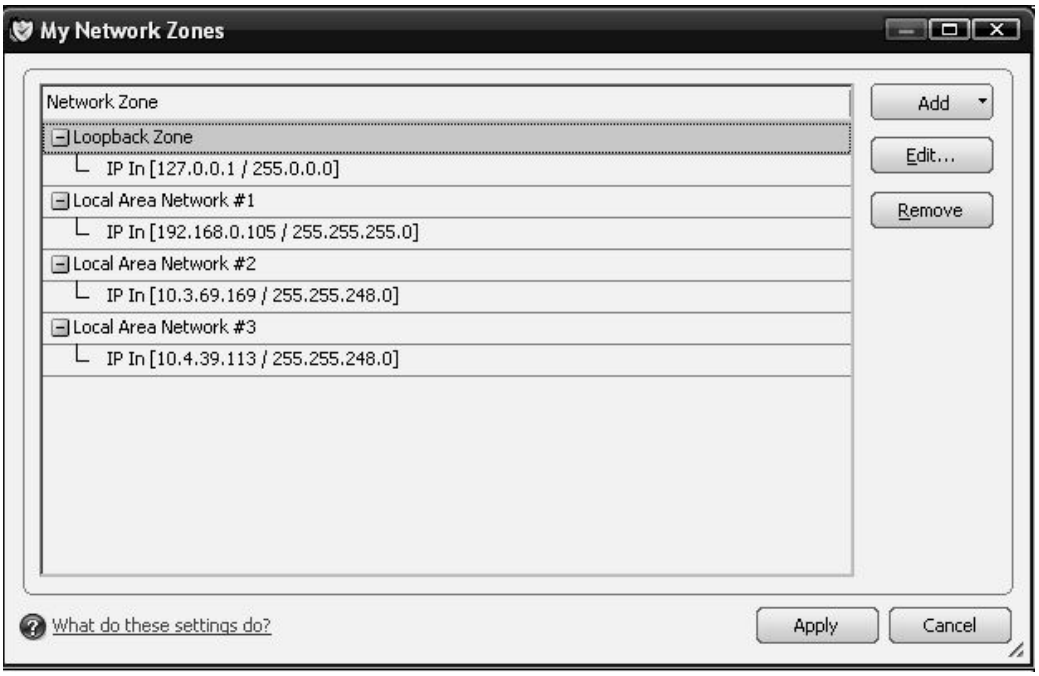


Рис. 3.8.2. Діалогове вікно налаштування мережевих зон мережевого екрану COMODO Firewall Pro

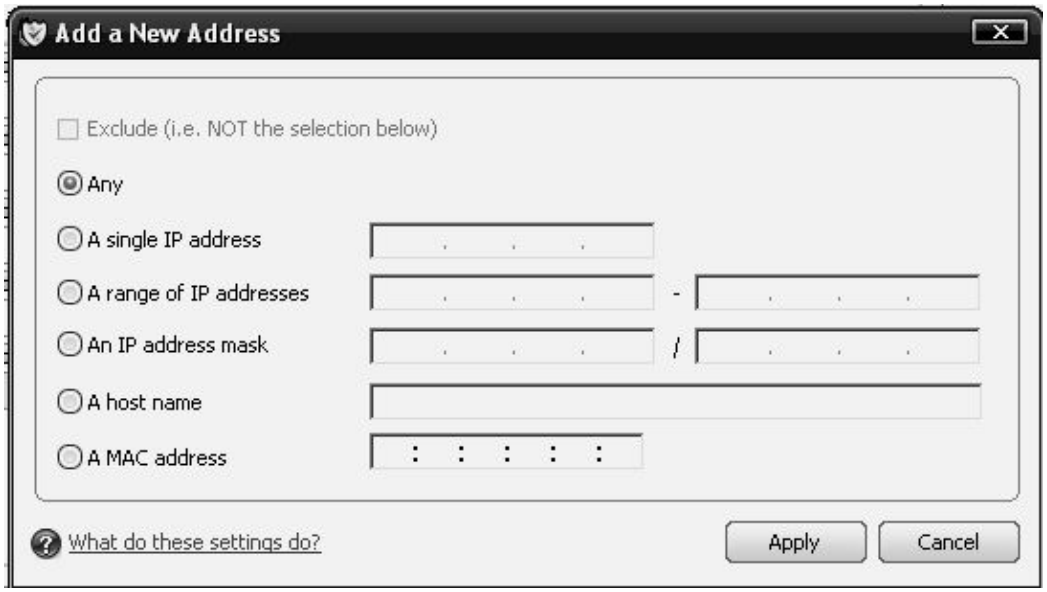


Рис. 3.8.3. Діалогове вікно додавання нових адрес до створеної зони в мережевому екрані COMODO Firewall Pro

Завдання до роботи

Об’єктом дослідження виступає комп’ютер із встановленою операційною системою Windows XP. Пропонується скористатися одним із запропонованих мережевих екранів сторонніх розробників для виконання завдання. При виконанні завдання вбудований мережевий екран потрібно відключити.

Оскільки заборона дозволу для різних протоколів відбувається однотипним чином, то пропонується для лабораторної роботи використовувати протокол ICMP. Відповідно до виданого варіанта необхідно із табл. 3.8.1 вибирати діапазон IP-адрес для дозволу проходження пакетів протоколом ICMP, проходження пакетів із інших адрес повинно бути заборонено. Також у кожного діапазону є додаткова IP-адреса. Якщо вказана адреса входить до первинного діапазону, то потрібно додатково заборонити надходження запитів із вказаної адреси, якщо адреса не входить до вказаного діапазону, то, навпаки, дозволити доступ із додаткової IP-адреси.

Таблиця 3.8.1

Варіанти завдань до лабораторної роботи

№ варіанта	Діапазон для дозволу доступу	Додаткова адреса
1	192.168.1.0-192.168.1.33	192.168.1.150
2	192.168.1.34-192.168.1.63	192.168.1.151
3	192.168.1.64-192.168.1.97	192.168.1.152
4	192.168.1.98-192.168.1.127	192.168.1.153
5	192.168.1.128-192.168.1.163	192.168.1.154
6	192.168.1.164-192.168.1.197	192.168.1.155
7	192.168.1.198-192.168.1.221	192.168.1.156
8	192.168.1.222-192.168.1.255	192.168.1.157
9	192.168.1.0-192.168.1.63	192.168.1.158
10	192.168.1.64-192.168.1.127	192.168.1.159
11	192.168.1.128-192.168.1.191	192.168.1.160
12	192.168.1.192-192.168.1.255	192.168.1.161
13	192.168.1.0-192.168.1.63	192.168.1.162
14	192.168.1.64-192.168.1.127	192.168.1.163
15	192.168.1.128-192.168.1.191	192.168.1.164

План виконання роботи

1. Відповідно до виданого викладачем варіанта вибрати завдання.
2. Налаштувати мережевий адаптер віртуального комп'ютера таким чином, щоб він входив до мережі 192.168.1.0/24.
3. Вивчити інтерфейс та основні можливості обраного мережевого екрану із пакетною фільтрацією.
4. Відповідно до варіанта роботи здійснити налаштування мережевого екрану.
5. Перевірити роботу створених налаштувань мережевого екрану. Для здійснення даної перевірки потрібно скористатися додатковим віртуальним комп'ютером із встановленою операційною сис-

темою Windows XP. Перевірка повинна здійснюватись із використанням команди *“ping”*. На додатковому комп’ютері почергово встановлюються IP-адреси, що входять до діапазону адрес, із якими дозволений зв’язок, потім, що не входять до даного діапазону, і, на завершення, перевіряється додаткова IP-адреса.

Питання до захисту роботи

1. Які переваги персональних мережевих екранів перед вбудованими IP-політиками Ви можете назвати?
2. Які додаткові функціональні можливості мережеві фільтри можуть запропонувати користувачеві?
3. Які персональні мережеві екрани Ви можете назвати?
4. Яким чином можна здійснити розподіл мережі на підмережі за допомогою маски?
5. У якому випадку використання мережевого екрану буде неефективним?

ЛІТЕРАТУРА: [21, 27].

4. ПИТАННЯ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ ТА ДИСКУСІЙ

Тема 1. Класи та топології комп'ютерних мереж

1. Загальні принципи побудови мереж.
2. Розвиток, топологія та архітектура глобальної мережі Інтернет.
3. Приклади мережевих топологій.
4. Характеристики комп'ютерних мереж.

Література: [21, 31].

Тема 2. Модель OSI та інкапсуляція даних

1. Порівняння моделей TCP та OSI.
2. Модель ATM.
3. Переваги використання багаторівневих моделей для опису функціонування комп'ютерної мережі.

Література: [1, 2, 4, 31].

Тема 3. Середовище передачі даних та обладнання комп'ютерних мереж

1. Супутниковий зв'язок та мобільні телефонні системи.
2. Огляд номенклатури та характеристик активного мережевого обладнання на прикладі обладнання компанії Cisco Systems.
3. Огляд номенклатури та характеристик обладнання для тестування роботи комп'ютерних мереж на прикладі обладнання компанії Fluke.

Література: [8, 33, 41].

Тема 4. Технології побудови локальних комп'ютерних мереж

1. Архітектура протоколів Fibre Channel.
2. Методи забезпечення якості обслуговування (QoS).
3. Віртуальні локальні мережі (VLAN).
4. Технологія Bluetooth.

Література: [2, 22, 29, 31].

Тема 5. Технології побудови розподілених комп'ютерних мереж

1. Проектування розподіленої мережі.
2. Технологія Metro Ethernet.

3. Технологія WiMAX.
4. Використання протоколу PPP для розподілених мереж.

Література: [2, 31].

Тема 6. Стеки протоколів комп'ютерних мереж

1. Історія та перспективи розвитку стека протоколів TCP/IP.
2. Специфікація протоколів прикладного рівня стека TCP/IP.
3. Специфікація протоколів транспортного рівня стека TCP/IP.

Література: [1, 39, 53, 54].

Тема 7. Адресація в комп'ютерних мережах

1. Алгоритм роботи протоколу динамічної конфігурації вузлів в мережі DHCP.
2. Формат пакета у протоколі IPv4.
3. Опис роботи протоколу IPv6.
4. Приклади адресації у комп'ютерних мережах.

Література: [1, 13, 29[.

Тема 8. Маршрутизація в комп'ютерних мережах

1. Метод безкласової адресації CIDR.
2. Метод призначення масок змінної довжини – VLSM.
3. Протокол маршрутизації RIPv2.
4. Протокол маршрутизації OSPF.

Література: [22, 29, 42, 49, 52].

Тема 9. Методика проектування мережі та СКС

1. Волоконно-оптичні компоненти СКС.
2. Вимоги міжнародного стандарту ISO/IEC 11801:2002 до волоконно-оптичної частини СКС.
3. Огляд номенклатури та характеристики пасивного мережевого обладнання на прикладі обладнання компанії Reichle & De-Massari AG.
4. Тестування оптоволоконних ліній та каналів СКС.
5. Приклад проектування СКС.

Література: [26, 27, 50].

Тема 10. Безпека комп'ютерних мереж

1. Цифрові підписи.
2. Управління відкритими ключами.
3. Захист з'єднань.
4. Протоколи аутентифікації.

Література: [19, 25, 31].

5. ЗАВДАННЯ ДЛЯ САМОКОНТРОЛЮ ТА ПЕРЕВІРКИ ЗНАНЬ

Тест 1. Класи та топології комп'ютерних мереж

1. Виникнення чого вплинуло на появу перших локальних мереж?
   а) маршрутизаторів;
   б) великих інтегральних схем;
   в) мейнфреймів;
   г) багатотермінальних систем.

2. Оберіть існуючі мережеві топології:
   а) шина;
   б) кільце;
   в) топологічна;
   г) пряма;
   д) зірка.

3. З якою метою використовують комірчасту (mesh) топологію?
   а) для спрощення топології;
   б) для збільшення надійності мережі;
   в) для передачі електричного сигналу високого рівня;
   г) для поєднання декількох мереж.

4. Який з описів терміна "топологія" є найкращим?
   а) з'єднання комп'ютерів, принтерів та інших пристроїв з метою організації обміну даними між ними;
   б) фізичне розташування вузлів мережі і мережевого середовища передачі даних усередині мережевої структури підприємства;
   в) тип мережі, який не допускає виникнення конфліктів пакетів даних;
   г) метод фільтрації мережевого трафіка з метою зменшення ймовірності виникнення вузьких місць і уповільнення передачі даних.

5. Як у мережах з шинною топологією проводиться повторна передача з затримкою?
   а) це робить найближчий до місця конфлікту міст;
   б) це робить термінатор;
   в) це робиться мережевим адаптером кожного пристрою в тому сегменті, де виникла колізія;
   г) це робить найближчий до місця конфлікту маршрутизатор.

6. Яку перевагу дає використання топології "зірка"?
   а) висока надійність;
   б) природна надмірність;

в) низька вартість;
г) витрачається мінімальний обсяг кабелю.

7. За територіальною поширеністю мережі поділяються на:
а) локальні;
б) мережі користувачів;
в) кампусні;
г) інтернет;
д) міські;
е) глобальні.

8. Що можна віднести до недоліків топології кільце?
а) вихід з ладу хоча б одного з комп'ютерів або пристрою порушує роботу всієї мережі;
б) обрив або коротке замикання в будь-якому з кабелів кільця робить роботу всієї мережі неможливою;
в) щоб запобігти зупинці мережі при відмові комп'ютера або обриві кабелю, як правило, прокладають два кільця, що суттєво здорожує мережу;
г) на кінцях кабелю потрібно встановлювати термінатори;
д) комп'ютери, об'єднані за топологією "кільце", не ретранслюють сигнали, тому для цього необхідно використовувати повторювачі.

9. Для чого використовувались перфокарти?
а) для введення команд та даних;
б) для підключення робочої станції до мережі;
в) для запису результатів обробки даних;
г) для пошуку інформації.

10. Що таке робоча станція?
а) персональний комп'ютер з мережевим адаптером;
б) принтер;
в) частина мережі, яка містить у собі персональні комп'ютери та мережеве обладнання;
г) мережеве обладнання, що виконує функцію посилення електричного сигналу.

11. Недоліком якого способу доступу до середовища є те, що при великій кількості комп'ютерів і високому навантаженні на мережу кількість зіткнень зростає, а пропускна спроможність падає?
а) множинний доступ з контролем несучої і виявленням зіткнень;
б) множинний доступ з контролем несучої та запобіганням зіткненням;
в) передача маркера.

Тест 2. Модель OSI та інкапсуляція даних

1. Який з цих пристроїв працює на фізичному рівні моделі OSI? Канальному рівні? Мережевому рівні?
   а) маршрутизатор;
   б) комутатор;
   в) міст;
   г) повторювач;
   д) мережевий адаптер;
   е) концентратор.

2. Які з нижченаведених тверджень Ви вважаєте помилковими?
   а) протокол – це програмний модуль, що вирішує задачу взаємодії систем;
   б) протокол – це формалізований опис правил взаємодії, що містять у собі послідовність обміну повідомленнями та їх формати;
   в) терміни “інтерфейс” та “протокол”, по суті, є синонімами.

3. Який рівень еталонної моделі OSI вирішує питання щодо сповіщення про несправності, враховує топологію мережі і управляє потоком даних?
   а) фізичний;
   б) канальний;
   в) транспортний;
   г) мережевий.

4. Який рівень еталонної моделі OSI встановлює, обслуговує і керує сеансами взаємодії прикладних програм?
   а) транспортний;
   б) сеансовий;
   в) рівень представлення;
   г) прикладний.

5. Що з нижченаведеного найкраще описує функцію рівня представлення?
   а) він забезпечує форматування коду і подання даних;
   б) він обробляє повідомлення про помилки, враховує топологію мережі і управляє потоком даних;
   в) він надає мережеві послуги для користувача прикладним програмам;
   г) він забезпечує електричні, механічні, процедурні і функціональні засоби для активізації та підтримки каналу зв’язку між системами.

6. Який номер має канальний рівень у еталонній моделі OSI?
   а) 1;
   б) 2;
   в) 3;
   г) 4.

7. Який з наведених нижче описів канального рівня еталонної моделі OSI є найкращим?
   а) передає дані іншим рівням;
   б) забезпечує послуги прикладним процесам;
   в) приймає слабкий сигнал, очищує його, підсилює і відправляє далі в мережу;
   г) забезпечує надійну передачу даних з фізичного каналу.

8. Який опис п’яти етапів перетворення даних у процесі інкапсуляції при відправленні поштового повідомлення одним комп’ютером іншому є правильним?
   а) дані, сегменти, пакети, кадри, біти;
   б) біти, кадри, пакети, сегменти, дані;
   в) пакети, сегменти, дані, біти, кадри;
   г) сегменти, пакети, кадри, біти, дані.

9. Під час відправлення поштового повідомлення з комп’ютера А на комп’ютер Б дані необхідно інкапсулювати. Який з описів першого етапу інкапсуляції є правильним?
   а) алфавітно-цифрові символи конвертуються в дані;
   б) повідомлення сегментується в блоки, що легко транспортуються;
   в) до повідомлення додається мережевий заголовок (адреси джерела й одержувача);
   г) повідомлення перетворюється у двійковий формат.

10. Під час відправлення поштового повідомлення з комп’ютера А на комп’ютер Б по локальній мережі дані необхідно інкапсулювати. Що відбувається після створення пакета?
   а) пакет передається по середовищу;
   б) пакет розміщується в кадр;
   в) пакет сегментується на кадри;
   г) пакет перетворюється у двійковий формат.

11. Під час відправлення поштового повідомлення з комп’ютера А на комп’ютер Б дані необхідно інкапсулювати. Що відбувається після перетворення алфавітно-цифрових символів у дані?
   а) дані перетворюються у двійковий формат;
   б) до даних додається мережевий заголовок;

в) дані сегментуються на менші блоки;
г) дані розміщуються в кадр.

12. Що з нижченаведеного найкраще описує дейтаграму?
а) повідомлення, яке передається джерелу з підтвердженням отримання непошкоджених даних;
б) двійкове подання інформації про маршрутизацію;
в) пакет даних розміром менше 100 байт;
г) пакет мережевого рівня.

Тест 3. Середовище передачі даних та обладнання комп'ютерних мереж

1. Як називається середовище, що забезпечує проходження сигналу в мережі?
а) середовище прикладних програм;
б) мережеве середовище;
в) середовище передачі даних;
г) системне середовище.

2. Яку перевагу має використання в мережах оптоволоконного кабелю?
а) дешевизна;
б) простота монтажу;
в) це – промисловий стандарт, і він є у продажу в будь-якому магазині, що продає електронні пристрої;
г) швидкість передачі даних по оптоволоконному кабелю вище, ніж по витій парі або коаксіальному кабелю.

3. Яке з наведених нижче визначень найкраще описує поняття "середовище передачі даних"?
а) кабелі й дроти, по яких переміщуються дані;
б) різні фізичні середовища, придатні для передачі сигналу;
в) комп'ютерні системи та дроти, які утворюють мережу;
г) будь-які мережеві апаратні і програмні засоби.

4. У якому вигляді інформація зберігається у комп'ютері?
а) у вигляді десяткових чисел;
б) у вигляді двійкових чисел;
в) у вигляді електронів;
г) у вигляді слів і малюнків.

5. На якому рівні еталонної моделі OSI працює мережевий адаптер?
а) на канальному;
б) на фізичному;
в) на транспортному;
г) на рівні представлення.

6. Як по-іншому називається MAC-адреса?
   а) двійкова адреса;
   б) вісімкова адреса;
   в) фізична адреса;
   г) адреса TCP/IP;
   д) локальна адреса.

7. Для чого служить мережевий адаптер?
   а) встановлює, управляє і припиняє сеанси між додатками та здійснює управління обміном даних між об'єктами рівня представлення;
   б) надає комп'ютерним системам можливість здійснювати двонаправлений обмін даними по мережі;
   в) надає послуги прикладним процесам;
   г) надає можливості для встановлення, підтримки і закриття віртуальних каналів, виявлення помилок передачі, відновлення і керування потоком інформації.

8. Яким чином відправник вказує даним місцезнаходження одержувача в мережі?
   а) мережевий адаптер одержувача ідентифікує свою MAC-адресу в пакеті даних;
   б) пакет даних зупиняється в пункті призначення;
   в) мережевий адаптер одержувача посилає свою MAC-адресу джерелу;
   г) джерело посилає унікальний пакет даних за кожною MAC-адресою в мережі.

9. Для чого використовуються міжмережеві пристрої?
   а) вони дозволяють збільшувати число вузлів, протяжність мережі і об'єднувати окремі мережі;
   б) вони підвищують швидкість передачі даних і зменшують рівень електромагнітних перешкод у будівлях;
   в) вони забезпечують для сигналу резервні шляхи доставки, тим самим запобігаючи його втрату і пошкодження;
   г) дозволяють поєднувати пристрої в усьому будинку.

10. Який з описів вузла є найкращим на Ваш погляд?
   а) пристрій, що визначає оптимальний маршрут руху трафіка по мережі;
   б) пристрій, який встановлює, підтримує і завершує сеанси між додатками і управляє обміном даними між об'єктами рівня представлення;

в) пристрій, який синхронізує взаємодіючі програми та узгоджує процедури відновлення після помилок та перевірки цілісності даних;
г) кінцева точка мережевого з'єднання або загальний стик двох або більше ліній, що служить як контрольна точка.

11. Яка з проблем може бути легко усунена за допомогою повторювача?
а) занадто багато типів несумісного обладнання в мережі;
б) занадто великий трафік в мережі;
в) занадто низька швидкість передачі даних;
г) занадто багато вузлів і/або недостатньо кабелю.

12. Який недолік має використання концентратора?
а) він не може збільшити робочі відстані в мережі;
б) він не може фільтрувати мережевий трафік;
в) він не може посилати ослаблений сигнал через мережу;
г) він не може посилювати ослаблені сигнали.

13. Який з описів колізії в мережі є найкращим?
а) це результат передачі даних у мережу двома вузлами незалежно один від одного;
б) це результат одночасної передачі даних у мережу двома вузлами;
в) це результат повторної передачі даних у мережу двома вузлами;
г) це результат невиконання передачі даних у мережу двома вузлами.

14. Який опис терміна "домен колізій" є найкращим?
а) область мережі, у якій поширюються конфліктуючі пакети даних;
б) область мережі, яка обмежується мостами, маршрутизаторами або комутаторами;
в) область мережі, у якій встановлені маршрутизатори та концентратори;
г) область мережі, у якій не використовується фільтрація трафіка.

15. У чому полягає відмінність між мостами й комутаторами?
а) мости пересилають широкомовний трафік, а концентратори – ні;
б) міст у кожний момент часу може передавати тільки один кадр, обслуговуючи передачу від одного комп'ютера до іншого, а комутатор вміє будувати велику кількість віртуальних каналів зв'язку між портами;
в) мости не можуть підтримувати таблицю відповідності своїх портів і використаних у мережі MAC-адрес, а комутатори можуть;

г) мости працюють на фізичному рівні моделі OSI, а комутатори ще й на канальному, – точніше, на підрівні керування доступом до середовища (MAC).

16. Який мережевий пристрій здатний вирішити проблему надмірного широкомовного трафіка?
   а) міст;
   б) маршрутизатор;
   в) концентратор;
   г) шлюз.

Тест 4. Технології побудови локальних комп'ютерних мереж

1. Яка швидкість забезпечується у мережі, спроектованій за технологією Fast Ethernet?
   а) 10 Мбіт/с;
   б) 56 Кбіт/с;
   в) 100 Мбіт/с;
   г) 1000 Мбіт/с.

2. Який метод доступу до середовища використовується у мережах, спроектованих за технологією Token Ring?
   а) CSMA/CA;
   б) CSMA/CD;
   в) маркерний.

3. Яка з зазначених технологій проектування локальних мереж має підвищену відмовостійкість?
   а) Gigabit Ethernet;
   б) Fast Ethernet;
   в) Ethernet;
   г) WIMAX;
   д) Token Ring;
   е) FDDI;
   ж) WLAN.

4. Які з зазначених мережевих технологій мають топологію кільце?
   а) Gigabit Ethernet;
   б) Fast Ethernet;
   в) Ethernet;
   г) WIMAX;
   д) Token Ring;
   е) FDDI;
   ж) WLAN.

5. Які технології можна віднести до бездротових технологій побудови локальних мереж?
   а) Gigabit Ethernet;
   б) Fast Ethernet;
   в) Ethernet;
   г) WIMAX;
   д) Token Ring;
   е) FDDI;
   ж) WLAN.

6. Яке з цих тверджень справедливе по відношенню до мереж CSMA/CD?
   а) дані від вузла-джерела проходять через усю мережу. У міру руху дані приймаються й аналізуються кожним вузлом;
   б) сигнали посилаються безпосередньо одержувачу, якщо його MAC- і IP-адреси відомі відправникові;
   в) дані від вузла-джерела надходять до найближчого маршрутизатора, який направляє їх безпосередньо адресатові;
   г) сигнали завжди посилаються в режимі широкомовлення.

7. Що з нижчеперерахованого належить до переваг технологій Ethernet?
   а) простота реалізації;
   б) використання методу CSMA/CD;
   в) підвищена відмовостійкість;
   г) висока сумісність різних варіантів Ethernet;
   д) використання будь-яких видів кабелю.

8. Який з перелічених стандартів належить до стандартів бездротових мереж?
   а) IEEE 802.3;
   б) IEEE 802.11;
   в) IEEE 803.5;
   г) IEEE 802.4.

9. Які види кабелю визначаються як фізичне середовище передачі даних для технології Gigabit Ethernet?
   а) оптоволоконний кабель;
   б) тонкий коаксіальний кабель;
   в) товстий коаксіальний кабель;
   г) екранована вита пара;
   д) неекранована вита пара.

10. Які види кабелю визначаються як фізичне середовище передачі даних для технології Ethernet?
   а) оптоволоконний кабель;
   б) тонкий коаксіальний кабель;
   в) товстий коаксіальний кабель;
   г) екранована вита пара;
   д) неекранована вита пара.

Тест 5. Технології побудови розподілених комп'ютерних мереж

1. Які технології належать до технологій проектування глобальних мереж?
   а) Fast Ethernet;
   б) Frame Relay;
   в) FDDI;
   г) X.25;
   д) ATM;
   е) ISDN.

2. Які бувають типи віртуальних каналів?
   а) мережеві;
   б) комутовані;
   в) постійні;
   г) високошвидкісні;
   д) розподілені.

3. Який з описів глобальних мереж є найкращим?
   а) використовуються для об'єднання локальних мереж, розділених значними географічними відстанями;
   б) об'єднують робочі станції, термінали та інші пристрої, розташовані в межах міста;
   в) об'єднують локальні мережі, розташовані в межах великого будинку;
   г) об'єднують автоматизовані робочі місця, термінали та інші пристрої, розташовані в межах будівлі.

4. На якому рівні еталонної моделі OSI знаходиться обладнання DCE і DTE?
   а) на мережевому рівні;
   б) на канальному рівні;
   в) на фізичному рівні;
   г) на транспортному рівні.

5. На якому типі обладнання зазвичай використовуються CSU/CDU?
   а) маршрутизатор;
   б) DTE;
   в) комутатор;
   г) DCE.

6. На яких рівнях еталонної моделі OSI працюють глобальні мережі?
   а) фізичний рівень та рівень додатків;
   б) фізичний і канальний рівні;
   в) канальний і мережевий рівні;
   г) канальний рівень і рівень представлення.

7. Чим глобальні мережі відрізняються від локальних?
   а) зазвичай існують у певних географічних областях;
   б) забезпечують високошвидкісні сервіси з множинним доступом;
   в) використовують маркери для регулювання мережевого трафіка;
   г) використовують служби операторів зв'язку.

8. Який з описів ISDN є найкращим?
   а) це цифровий сервіс для передачі голосу і даних по існуючих телефонних лініях;
   б) забезпечує з'єднання "маршрутизатор-маршрутизатор" і "хост-мережа" як по синхронним, так і по асинхронним лініям зв'язку;
   в) використовує високоякісне цифрове обладнання і є найшвидшим протоколом глобальних мереж;
   г) підтримує багатоточечні та двоточечні з'єднання, а також використовує символи кадру і контрольні суми.

9. Що таке демаркація?
   а) процедура налаштування обладнання між користувачем та провайдером;
   б) точка, у якій закінчується CPE і починається локальне відгалуження служби провайдера;
   в) механізм, який ліквідує колізії у глобальних мережах;
   г) цей термін не має відношення до глобальних мереж.

10. Що таке остання миля?
   а) це відстань між маршрутизатором та комутатором;
   б) це відстань між робочою станцією та мережевим активним обладнанням;
   в) кабель (зазвичай мідний дріт), що веде від пункту демаркації до телефонної станції провайдера;
   г) це відстань між двома робочими станціями користувачів.

11. Як називається обладнання, яке розташоване в приміщеннях користувача та приєднане до центрального офісу провайдера служби?
   а) DTE;
   б) DCE;
   в) CPE;
   г) CSU/DSU.

12. У мережах з комутацією пакетів встановлені при включенні комутаторів маршрути називаються:
   а) постійними віртуальними каналами (Permanent virtual circuits – PVCs);
   б) комутованими віртуальними каналами (Switched virtual circuits – SVCs);
   в) постійною віртуальною службою (Permanent virtual service – PVS);
   г) комутованою віртуальною службою (Switched virtual service – SVS).

13. Прикладами технологій, що використовують з'єднання з комутацією пакетів або гнізд є:
   а) X.25;
   б) загальнодоступна телефонна мережа, що комутується (Public Switched Telephone Network – PSTN);
   в) Frame Relay;
   г) ATM;
   д) інтерфейс базової швидкості ISDN (Basic Rate Interface – BRI);
   е) інтерфейс первинної швидкості ISDN (Primary Rate Interface – PRI).

Тест 6. Безпека комп'ютерних мереж

1. Як називається спосіб перетворення відкритої інформації в закриту, і навпаки?
   а) декодування;
   б) формування;
   в) шифрування;
   г) біометрія.

2. Програмне або апаратне рішення, яке націлене на виявлення фактів неавторизованого доступу в інформаційну систему чи мережу та несанкціонованого керування ними, як правило, через Інтернет, це:
   а) мережевий екран;
   б) система виявлення вторгнень;
   в) система попередження вторгнень;

г) антивірус;
д) сканер вразливостей.

3. Який метод шифрування недопустимий при передачі зашифрованого повідомлення електронною поштою?
а) асиметричний;
б) симетричний;
в) гібридний;
г) вузловий.

4. Програмне або апаратне рішення, яке здійснює контроль і фільтрацію мережевих пакетів, що проходять через нього на різних рівнях моделі OSI у відповідності до заданих правил, це:
а) мережевий екран;
б) система виявлення вторгнень;
в) система попередження вторгнень;
г) антивірус;
д) сканер вразливостей.

5. Який тип мережевого екрану найкраще підійде для захисту корпоративної мережі від зовнішніх загроз?
а) з пакетною фільтрацією;
б) прикладного рівня;
в) персональний;
г) немає вірної відповіді.

6. Різновид комп'ютерних програм, що мають здатність до саморозмноження, називають:
а) троянськими програмами;
б) комп'ютерними вірусами;
в) шпигунськими програмами;
г) шкідливими програмами.

7. Що таке проксі-сервер?
а) це виділений комп'ютер, на якому встановлено серверну операційну систему;
б) це інша назва мережевого екрану прикладного рівня;
в) це інша назва мережевого екрану з пакетною фільтрацією;
г) це сервер, на якому розміщено веб-сайт компанії.

8. Microsoft Baseline Security Analyzer, Security Administrator's Integrated Network Tool, QualysGuard, X-scan – це все різні типи:
а) мережевих екранів;
б) антивірусного програмного забезпечення;
в) систем виявлення і попередження вторгнень;

г) сканерів вразливостей;
д) рішень попередження витоку інформації.

9. Якщо в інформаційній системі компанії було встановлено рішення попередження витоку інформації і не було проіндексовано документи, що не підлягають розголосу, то дана система при передачі конфіденційної інформації:
а) не зможе виявити необхідні документи, оскільки індексація секретних документів відсутня;
б) зможе виявити необхідні документи за допомогою аналізу самого контенту;
в) система попередження витоку інформації призначена для блокування небажаного контенту зовні.

10. Виберіть функції, які не належать до завдань системи попередження витоку інформації:
а) архівування повідомлень, що пересилаються. Архіви можуть знадобитися для подальшого розслідування можливих справ;
б) попередження передачі зовні не лише конфіденційної інформації, але й іншої, що є небажаною для компанії;
в) оптимізація загрузки каналів передачі інформації;
г) виявлення небажаного програмного забезпечення;
д) попередження витоку інформації не лише зовні, а й з зовнішнього середовища до інформаційної системи;
е) попередження використання співробітниками службових інформаційних ресурсів в особистих цілях;
ж) сканування вразливих місць інформаційної системи;
з) контроль присутності співробітників на робочому місці.

ТЕРМІНОЛОГІЧНО-ТЛУМАЧНИЙ СЛОВНИК

Ethernet – пакетна технологія комп'ютерних мереж, переважно локальних. Стандарти Ethernet визначають з'єднання дротів і електричні сигнали на фізичному рівні, формат кадрів і протоколи управління доступом до середовища на канальному рівні моделі OSI. Ethernet в основному описується стандартами IEEE групи 802.3.

FDDI (Fiber Distributed Data Interface) – технологія передачі даних у локальній мережі, простягнутій на відстані до 200 кілометрів. Технологія заснована на стандарті Token Ring. Окрім великої території, мережа FDDI здатна підтримувати декілька тисяч користувачів.

IP-адреса (IP-address) – 32-розрядна адреса, яка призначається хосту в протоколі TCP/IP і за допомогою якої комп'ютер однозначно ідентифікується в IP-мережі. Кожна адреса складається з номера мережі, необов'язкового номера підмережі і номера комп'ютера. Номери мережі і підмережі використовуються для маршрутизації, а номер комп'ютера – для адресації унікального хоста в мережі або підмережі.

MAC-адреса (MAC-address) – це унікальний ідентифікатор довжиною 48-біт, який призначаєтсья кожному мережевому пристрою (мережевій карті тощо) Ethernet для його ідентифкації в мережі. MAC-адреса мережевих пристроїв призначається виробником.

Token Ring – "маркерне кільце", архітектура кільцевої мережі з маркерним (естафетним) доступом в мережу. Описується стандартом IEEE 802.5.

А

Абонент мережі – комп'ютер або інший пристрій, підключений до мережі.

Антивірусна програма (або просто антивірус) – це програма, яка призначена для знаходження небажаного програмного забезпечення (комп'ютерні віруси, троянські програми, програми-шпигуни тощо), для лікування заражених файлів, а також попередження зараження інформаційної системи.

Асиметричне шифрування (у системах з відкритими ключами – public-key systems) – метод шифрування, при використанні якого кожен користувач має пару ключів – відкритий для шифрування та закритий (секретний) для дешифрування.

Б

Безкласова адресація (Classless InterDomain Routing – CIDR) – метод IP-адресації, який дозволяє гнучко керувати простором IP-адрес, не використовуючи жорсткі рамки класової адресації. Використання цього методу дозволяє економно використовувати обмежений ресурс IP-адрес, оскільки можливе застосування різних масок підмереж до різних підмереж.

Блок канального інтерфейсу/блок цифрової служби (channel service unit/digital service unit – CSU/DSU) – пристрій цифрового зв'язку, який з'єднує обладнання з кінцевим користувачем та відгалуження локальної телефонної станції.

В

Виділена лінія або канал типу "точка-точка" (Leased line або point-to-point link) – канал, який забезпечує окремий, заздалегідь встановлений шлях комунікації від стаціонарного обладнання споживача до віддаленої мережі через мережу провайдера, таку, наприклад, як мережа телефонної компанії.

Виділений (dedicated) сервер – комп'ютер в мережі, який працює виключно як сервер мережі і не здатний виконувати інші (не мережеві) задачі.

Вита пара – середовище передачі інформації з двох перекручених між собою електричних дротів, яке характеризується найбільшою простотою монтажу і низькою вартістю.

Віртуальний канал (virtual circuit) – канал типу "точка-точка", який являє собою не фізичний, а логічний ланцюг і створюється для забезпечення надійного зв'язку між двома мережевими пристроями.

Вірус – це різновид комп'ютерних програм, особливістю яких є здатність до розмноження (самореплікація).

Вузол – комп'ютер або інший пристрій, підключений до мережі, те саме, що й абонент.

Г

Глобальна мережа (Wide Area Network – WAN) – сукупність мереж, що поєднують територіально розосереджені комп'ютери, які перебувають у різних містах і країнах. Ще її називають розподіленою мережею.

Група – логічне об'єднання комп'ютерів мережі, які вирішують спільні задачі та мають однакові права доступу.

Д

Датаграма, дейтаграмма – спосіб передачі пакетів у довільному порядку без підтвердження отримання; правильний порядок відновлюється абонентом-одержувачем.

Демаркація (або демарк) (Demarcation або demarc) – точка, у якій закінчується CPE і починається локальне відгалуження служби провайдера. Часто ця точка знаходиться в точці присутності будівлі.

Домен – область ієрархічного простору доменних імен мережі Інтернет, яка позначається унікальним доменним ім'ям.

Домен конфлікту (область колізій) – декілька абонентів (вузлів) мережі Ethernet, які здійснюють доступ до мережі за методом CSMA/CD. Частина мережі, на яку поширюється ситуація конфлікту. Може включати в себе всю мережу.

Доменне ім'я – символьне ім'я домену. Повинно бути унікальним в рамках одного домена. Повне ім'я домена складається з імен всіх доменів, у які він входить, розділених крапками.

З

Зірка (star) – вид топології локальної мережі, у якому до одного центрального абонента (концентратора) підключаються кілька периферійних абонентів, при цьому все управління мережею і (або) передачу всієї інформації в ній здійснює центральний абонент.

І

Інтернет-провайдер – це організація, яка надає послуги доступу до Інтернету та інші пов'язані з Інтернетом послуги.

Інтерфейс базової швидкості (Basic Rate Interface – BRI) – ISDN-інтерфейс, що складається з двох B-каналів і одного D-каналу для канально-комутованої передачі голосу, відео й інших даних.

Інтерфейс первинної швидкості (Primary Rate Interface – PRI) – ISDN-інтерфейс для основного доступу. Складається з одного D-каналу (64 Кбіт/с) і двадцяти трьох (для T1) або 30 (для E1) B-каналів для голосу або даних.

К

Кабельна система – це набір комутаційних елементів (кабелів, роз'ємів, з'єднувачів, спеціальних шаф, кронштейнів, кабель-

каналів тощо), спільне використання яких закріплено певною методикою.

Кадр (frame) – фрагмент даних на канальному рівні моделі OSI.

Кампусна мережа – мережа, що охоплює територію університету або студентського містечка.

Кільце (ring) – вид топології локальної мережі, у якому всі абоненти послідовно передають інформацію один одному по ланцюжку, замкнутому в кільце.

Кінцеве обладнання даних (data circuit-terminating equipment – DCE) – пристрій, який використовуються для перетворення даних користувача з формату DTE у формат, який використовується обладнанням служби розподіленої мережі.

Класова адресація – метод IP-адресації. IP-адреса кожного інтерфейсу належить до одного з п'яти класів (A, B, C, D або E). Використання цього методу не дозволяє економно використовувати обмежений ресурс IP-адрес, оскільки неможливе застосування різних масок підмереж до різних підмереж.

Клієнт – абонент, який не віддає свої ресурси в мережу, але який має доступ до ресурсів мережі. Іноді клієнтами називаються також робочі станції на противагу серверові.

Ключ – секретна інформація, яка використовується криптографічним алгоритмом шифрування.

Коаксіальний кабель (coaxial cable) – середовище передачі інформації, електричний кабель, який складається з центрального провідника і металевої сітки, розділених діелектриком.

Колізія – ситуація, при якій у мережу передаються кілька пакетів одночасно, що викликає видозмінення інформації. Називається також конфліктом або зіткненням.

Комп'ютерна мережа (або *мережа передачі даних*) – це деяка сукупність вузлів (комп'ютерів, робочих станцій чи іншого обладнання), з'єднаних комунікаційними каналами, а також набір обладнання, який забезпечує з'єднання станцій і передачу між ними інформації.

Концентратор або хаб (hub) – пристрій, який служить для об'єднання декількох сегментів єдиної мережі і не перетворює інформацію, яка передається.

Комутатор або світч (switch) – пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента. На відміну від концентратора, який розповсюджує трафік від одного підключеного пристрою до всіх інших, комутатор передає дані лише безпосередньо отримувачу, виняток становить широкомовний трафік усіх вузлів мережі.

Комутатор розподіленої мережі – це мережевий пристрій з декількома портами, який зазвичай комутує потоки даних таких протоколів, як Frame Relay, X.25 тощо.

Комутатор телефонної станції (CO switch) – комутуючий пристрій, який являє собою найближчу точку присутності для служби провайдера розподіленої мережі.

Комутатор 3-го рівня – це комутатор, який містить у собі також функції маршрутизації пакетів.

Комутовані віртуальні канали (switched virtual circuit – SVC) – це канали, які створюються динамічно за запитом і припиняють своє існування після закінчення передачі.

Л

Локальна мережа або локальна обчислювальна мережа (Local Area Network – LAN) – це мережа, яка містить у собі комп'ютери, що розташовані у межах одного приміщення, будинку або невеликої території, і дозволяє обмін даними та спільне використання різних пристроїв (принтерів, сканерів тощо).

Локальне відгалуження (або "остання миля") – кабель (зазвичай мідний дріт), що веде від пункту демаркації до телефонної станції провайдера.

М

Маска підмережі – це 32-розрядне число, яке складається з одиниць, що йдуть спочатку, та з нулів, що йдуть наприкінці, наприклад (в десятковому поданні), 255.255.255.0 або 255.255.240.0.

Маршрутизатор (router) – пристрій, який служить для визначення маршруту, по якому найбільш доцільно пересилати пакет, та для з'єднання мереж, які використовують різні архітектури та протоколи.

Мережа на основі сервера – мережа, у якій є чіткий поділ абонентів на клієнтів і серверів і в якій є хоча б один виділений сервер.

Мережева архітектура – це сукупність мережевих апаратних і програмних рішень, методів доступу та протоколів обміну інформацією.

Мережева операційна система – програмне забезпечення, яке керує роботою мережі і яке дозволяє підтримувати зв'язок і спільно використовувати ресурси.

Мережева технологія – це узгоджений набір стандартних протоколів та програмно-апаратних засобів, що їх реалізують, достатній для побудови локальної обчислювальної мережі.

Мережевий адаптер або мережева карта – електронна плата (карта) для сполучення комп'ютера з середовищем передачі інформації в мережі.

Мережевий екран – це програмне або апаратне рішення, яке здійснює контроль і фільтрацію мережевих пакетів, що проходять через нього, на різних рівнях моделі OSI у відповідності до заданих правил.

Мережевий трафік – інформаційні потоки, які передаються мережею.

Метод доступу до середовища передачі – це набір правил, які визначають, як саме комп'ютери повинні надсилати та приймати дані по мережі.

Міжмережевий протокол (Internet Protocol – IP) – протокол, який забезпечує передачу даних у мережах. До його основних функцій належать адресація та фрагментація пакетів.

Міжмережевий протокол четвертої версії (Internet Protocol version 4 – IPv4) – маршрутний мережевий протокол, протокол мережевого рівня стека TCP/IP. У протоколі IP цієї версії кожному вузлу мережі ставиться у відповідність IP-адреса довжиною 4 октети (4 байти).

Міжмережевий протокол шостої версії (Internet Protocol version 6 – IPv6) – нова версія протоколу IP, покликана вирішити проблеми, з якими зіткнулася попередня версія (IPv4) при її використанні в Інтернеті, за рахунок використання довжини адреси 128 біт замість 32 бітів.

Міст (bridge) – пристрій, який служить для об'єднання в єдину мережу декількох мереж різних типів, а також для зниження навантаження в мережі.

Міська мережа (Metropolitan Area Network – MAN) – це мережа, яка поєднує комп'ютери на території міського району або всього міста в цілому.

Модем (модулятор-демодулятор) – пристрій, який перетворює цифрові дані від комп'ютера в аналогові сигнали перед їх передачею по послідовній лінії та який робить зворотне перетворення після передачі. Це дозволяє передавати цифрові дані звичайними телефонними лініями.

Мультиплексування з поділом часу (time-division multiplexing – TDM) – сигнал комутації каналу, що використовується для визначення маршруту виклику, який є виділеним шляхом від відправника до одержувача.

Н

Невиділений сервер – сервер, який може виконувати не тільки функції з обслуговування мережі, а ще й інші задачі.

О

Обладнання терміналу даних (data terminal equipment – DTE) – пристрій, розташований на користувальницькому кінці інтерфейсу "користувач-мережа", який може виступати як джерело даних, одержувач даних або в якості обох. DTE з'єднується з мережею даних за допомогою пристрою DCE (наприклад, модему) і зазвичай використовує часові сигнали, які генеруються DCE. Обладнання терміналу включає в себе такі пристрої, як комп'ютери, транслятори протоколів та мультиплексори.

Однорангова мережа (peer-to-peer network) – мережа, у якій немає виділених серверів й ієрархії серед комп'ютерів. Усі комп'ютери можуть бути серверами та клієнтами.

Оптоволоконний кабель (fiber optic cable*)* – середовище передачі інформації. Являє собою скляне або пластикове волокно в оболонці, через яке поширюється світловий сигнал.

П

Пакет (packet) – фрагмент даних на мережевому рівні моделі OSI.

Петля – замкнутий контур передачі інформації в топології мережі.

Платна частина мережі (toll network) – комутатори та інші пристрої колективного користування в середовищі провайдера.

Повторювач, репітер (repeater) – пристрій, який функціонує на фізичному рівні еталонної моделі OSI і призначений для відновлення та

посилення сигналів у мережі, збільшуючи таким чином довжину мережі.

Постійний віртуальний канал (permanent virtual circuit – PVC) – це канал, який має тільки один режим роботи (передачу даних) і використовується в тих випадках, коли обмін даними між пристроями носить постійний характер.

Приватна адреса – це IP-адреса, яка призначається для вузлів локальної мережі, що не підключені до Інтернету.

Пристрій CSU/DSU – це пристрій з цифровим інтерфейсом (іноді два окремі цифрові пристрої), який адаптує фізичний інтерфейс на пристрої DTE (такому, наприклад, як термінал) до інтерфейсу на DCE-пристрої (такому, як комутатор) у мережі з комутованим носієм.

Протокол – набір правил, алгоритм обміну інформацією між абонентами мережі.

Протокол X.25 – стандарт ITU-T, який визначає спосіб підтримки з'єднань між DTE і DCE для віддаленого термінального доступу і комп'ютерних комунікацій в загальнодоступних мережах передачі даних. Протокол Frame Relay певною мірою витіснив X.25.

Протокол віртуального терміналу (TELecommunication NETwork – Telnet) – протокол в наборі протоколів Internet, який дозволяє користувачам одного хосту підключатися до іншого віддаленого хосту і працювати з ним як через звичайний термінал.

Протокол динамічної конфігурації вузла (Dynamic Host Configuration Protocol – DHCP) – це мережевий протокол, який дозволяє комп'ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі TCP/IP.

Протокол зворотного перетворення адрес (Reverse Address Resolution Protocol – RARP) – протокол сімейства TCP/IP, являє собою метод визначення IP-адрес за MAC-адресами.

Протокол керування передачею (Transmission Control Protocol – TCP) – протокол, який працює з встановленням логічного з'єднання між віддаленими прикладними процесами, а також використовує принцип автоматичної повторної передачі пакетів, що містять помилки.

Протокол користувальницьких дейтаграм (User Datagram Protocol – UDP) – протокол, який є спрощеним варіантом TCP і працює без

встановлення логічного з'єднання, відповідно, не забезпечує перевірку на наявність помилок і підтвердження доставки пакета.

Протокол маршрутизації кінцевих систем (End System to Intermediate System routing exchange protocol – ES-IS) – протокол, за допомогою якого кінцеві системи (робочі станції) сповіщають про себе проміжні системи (наприклад, концентратори).

Протокол маршрутизації проміжних станцій (Intermediate System to Intermediate System routing exchange protocol – IS-IS) – протокол, за допомогою якого проміжні системи обмінюються інформацією про діючі маршрути в мережі.

Протокол міжмережевих керуючих повідомлень (Internet Control Message Protocol – ICMP) – протокол, призначений для організації зворотного зв'язку з окремими вузлами мережі при обміні інформацією про помилки, наприклад, про неможливість доставки пакета, про перевищення часу життя або тривалості складання пакета із фрагментів, про ненормальні значення параметрів.

Протокол передачі гіпертексту (HyperText Transfer Protocol – HTTP) – протокол, основою якого є технологія "клієнт-сервер", тобто клієнти ініціюють з'єднання і посилають запит, а сервери очікують з'єднання для отримання запиту, роблять необхідні дії і повертають назад повідомлення з результатом.

Протокол передачі файлів (File Transfer Protocol – FTP) – протокол, який використовує як транспортний протокол із встановленням з'єднань TCP, що підвищує надійність передачі файлів. Протокол призначений для забезпечення передачі та прийому файлів між серверами та клієнтами.

Протокол передачі файлів (Trivial File Transfer Protocol – TFTP) – протокол, який використовується головним чином для первинного завантаження бездискових робочих станцій. TFTP, на відміну від FTP, не містить можливостей аутентифікації (хоча можлива фільтрація по IP-адресі) і заснований на транспортному протоколі UDP.

Протокол перетворення адрес (Address Resolution Protocol – ARP) – Internet-протокол сімейства TCP/IP, який використовується для перетворення IP-адреси в MAC-адресу.

Протокол ретрансляції фреймів або *протокол Frame Relay (Frame Relay)* – стандартний промисловий комутований протокол канального рівня, який обслуговує велику кількість віртуальних ла-

нцюгів, використовуючи HDLC-інкапсуляцію між сполученими пристроями. Frame Relay є більш ефективним, ніж протокол X.25, і розглядається як його заміна.

Протокол управління групами Інтернету (Internet Group Management Protocol – IGMP) – протокол, що використовується IP-вузлами і маршрутизаторами, для того щоб підтримувати групову розсилку повідомлень.

Протокол шифрування безпечного з'єднання (Secure SHell – SSH) – протокол, який дозволяє проводити віддалене управління операційною системою. Схожий за функціональністю з протоколом Telnet, але, на відміну від нього, шифрує весь трафік, враховуючи і передані паролі. SSH допускає вибір різних алгоритмів шифрування. SSH-клієнти і SSH-сервери є для більшості мережевих операційних систем.

Публічна адреса – це IP-адреса, яка була призначена мережевим реєстром IANA (Internet Assigned Numbers Authority). Адреси, які призначає IANA, можуть використовувати трафік від вузлів Інтернету.

Р

Розмір мережі – це кількість об'єднаних у мережу комп'ютерів та відстань між ними.

Робоча станція – інша назва абонента мережі, клієнта мережі (на противагу серверові) або спеціального комп'ютера, орієнтованого на роботу в мережі.

Ретрансляція – прийом і передача інформації без її зміни, але з відновленням рівнів сигналів та їх форми.

Режим асинхронної передачі (Asynchronous Transfer Mode – ATM) – міжнародний стандарт для передачі гнізд, у яких застосовуються різні типи даних (такі, наприклад, як аудіо- і відеодані). Дані передаються в гніздах фіксованої довжини (53 байти). Використання гнізд фіксованої довжини дозволяє обробляти їх на стаціонарному обладнанні, скорочуючи тим самим транзитні затримки. ATM дозволяє скористатися високошвидкісними середовищами передачі, такими як E3, SONET і T3.

Рішення попередження витоку інформації (Data Leak Prevention або DLP) – це технології, які попереджують втечу конфіденційної інформації із інформаційної системи, а також технічні засоби для попередження такого витоку.

Розподілена мережа або глобальна мережа (wide-area network – WAN) – мережа передачі даних, яка обслуговує користувачів, розташованих на великому географічному просторі; такі мережі часто використовують пристрої передачі, які надаються загальними провайдерами. Прикладами технологій розподілених мереж можуть бути Frame Relay, X.25.

С

Сеанс – логічне з'єднання між абонентами мережі для обміну інформацією. Включає в себе передачу декількох пакетів.

Сегмент (segment) – частина мережі, обмежена мережевими пристроями (репітерами, концентраторами, мостами, маршрутизаторами, шлюзами), іноді використовується як синонім поняття мережі. Також сегментом називають фрагмент даних на транспортному рівні моделі OSI.

Сервер – абонент мережі, який віддає в мережу свої ресурси і який має або не має доступу до ресурсів мережі. Також сервером називають спеціалізований комп'ютер, призначений для роботи в мережі (має швидкодіючі диски великого обсягу, швидкий процесор, велику пам'ять).

Середовище передачі даних – фізичне середовище, придатне для проходження сигналу.

Симетричне шифрування – шифрування, при якому один і той самий ключ використовується як для шифрування, так і для дешифрування (розшифрування) даних.

Система виявлення вторгнень (Intrusion Detection System – IDS) – це програмне або апаратне рішення, яке націлене на виявлення фактів неавторизованого доступу до інформаційної системи чи мережі та несанкціонованого керування ними, як правило, через Інтернет.

Система доменних імен (Domain Name System – DNS) – система забезпечення перетворення символічних імен і псевдонімів локальних мереж і вузлів у мережі Інтернет в IP-адреси, і навпаки.

Система попередження вторгнень (Intrusion Prevention system – IPS) – це система виявлення вторгнень, яка не лише веде збір інформації щодо дій в системі, але й здійснює активні дії, направлені на попередження можливих вторгнень до інформаційної системи.

Сканери вразливостей – це програмні або апаратні рішення, які призначені для діагностики і моніторингу мережевих комп'ютерних систем.

Стандарт СКС – це узгоджений набір правил, які визначають структуру СКС, робочі параметри конструктивних елементів, принципи проектування, правила монтажу, методику вимірювання, правила адміністрування, вимоги телекомунікаційного заземлення.

Стаціонарне обладнання користувача (Customer's premises equipment – CPE) – це пристрої, фізично розташовані в приміщеннях користувача. Вони включають в себе як пристрої, які належать споживачеві, так і пристрої, орендовані у провайдера.

Стек протоколів – це ієрархічно впорядкована сукупність протоколів, достатніх для реалізації взаємодії вузлів у комп'ютерній мережі.

Стек протоколів IPX/SPX (Internetwork Packet eXchange/Sequenced Packet eXchange) – стек протоколів, який використовується в мережах Novell NetWare. Протокол IPX забезпечує мережевий рівень (доставку пакетів, аналог IP), SPX – транспортний і сеансовий рівень (аналог TCP).

Стек протоколів NetBIOS/SMB (Network Basic Input/Output System/Server Message Block) – спільний проект компаній Microsoft та IBM. Стек працює з усіма найбільш розповсюдженими протоколами нижнього рівня. На верхніх рівнях працюють протоколи NetBEUI та SMB.

Стек протоколів TCP/IP (Transmission Control Protocol/Internet Protocol) – набір мережевих протоколів різних рівнів моделі мережевої взаємодії DOD, що використовуються в мережах. Протоколи працюють один з одним у стеку – це означає, що протокол, який розташовується на рівні вище, працює "поверх" нижнього, використовуючи механізми інкапсуляції. Наприклад, протокол TCP працює поверх протоколу IP.

Структура мережі – це спосіб поділу мережі на частини (сегменти), а також спосіб об'єднання цих сегментів між собою.

Структурована кабельна система (СКС) – це сукупність кабелів, роз'ємів, панелей і розподільчих пристроїв, яка поєднує будинок або групу будинків в єдиний інформаційний простір. Така система включає в себе комп'ютерні, телефонні, телевізійні мережі, а також кабелі охоронної та пожежної сигналізації, систем контролю доступу та інших систем безпеки.

Т

Телефонна мережа загального користування (Public Switched Telephone Network – PSTN) – це мережа, для доступу до якої ви-

користовуються звичайні телефонні апарати, міні-АТС та обладнання передачі даних.

Телефонна станція (Central Office – CO) – офіс місцевої телефонної компанії, до якого приєднані всі місцеві лінії та в якому відбувається комутація каналів абонентських ліній.

Термінальний адаптер ISDN – це пристрій, який використовується для з'єднання інтерфейсу базової швидкості передачі з іншими інтерфейсами.

Топологія мережі – спосіб опису конфігурації мережі, схема розташування та з'єднання мережевих пристроїв. Існує три базові топології, на основі яких будується переважна більшість мереж: шина, кільце, зірка. Інші способи є комбінаціями базових.

Точка присутності (point of presence – POP) – точка з'єднання комунікаційних пристроїв, які надаються телефонною компанією, з головним розподільчим центром будівлі.

Троянська програма – небажана програма, яка проникає до системи під виглядом корисної (кодеку, різного роду корисного програмного забезпечення тощо).

Ф

Фільтрація трафіка – процес, у ході якого в мережевому трафіку контролюються певні характеристики, наприклад, адреса джерела, адреса одержувача або протокол, і на підставі встановлених критеріїв ухвалюється рішення – пропускати трафік далі або ігнорувати його.

Х

Хост (host) – це будь-яка одиниця комп'ютерної техніки, яка підключена до комп'ютерної мережі. Хостом може бути сервер, комп'ютер тощо. Щоб позначити ім'я хосту, використовується його мережеве ім'я – це для локальної мережі, або IP-адреса або доменне ім'я, якщо говорити про Інтернет.

Ц

Цифрова абонентська лінія (Digital Subscriber Line – xDSL) – сімейство технологій, які дозволяють значно розширити пропускну здатність абонентської лінії місцевої телефонної мережі шляхом використання ефективних лінійних кодів і адаптивних методів корекції помилок лінії на основі сучасних досягнень мікроелектроніки і методів цифрової обробки сигналу.

Цифрова мережа інтегрованих служб (Integrated Services Digital Network – ISDN) – комунікаційний протокол, запропонований телефонними компаніями, який дозволяє передавати інформацію по телефонних мережах, у тому числі голосові дані, а також дані, отримані з інших джерел.

Ш

Шина (bus) – вид топології локальної мережі, у якій використовується один кабель, що називається магістраллю або сегментом, уздовж якого підключені всі комп'ютери мережі. Дані у вигляді електричних сигналів передаються всім комп'ютерам мережі, але інформацію приймає тільки той, адреса якого відповідає адресі одержувача, причому в кожен момент часу тільки один комп'ютер може вести передачу.

Широкомовна область (broadcast domain) – частина мережі (або вся мережа), у якій поширюються широкомовні пакети (повідомлення).

Широкомовне повідомлення – повідомлення, призначене для всіх користувачів мережі і прийняте всіма абонентами.

Шифрування – це спосіб перетворення відкритої інформації в закриту і навпаки.

Шлюз (gateway) – пристрій, який служить для об'єднання мереж з абсолютно різними протоколами обміну.

Шпигунське програмне забезпечення – програмне забезпечення, яке інсталюється в інформаційну систему для повного або часткового контролю над нею без відповідної згоди на це користувача даної системи.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Амато Вито. Основы организации сетей Cisco [Текст] : в 2 т. Т. 1. : пер. с англ. / Вито Амато. – М. : Вильямс, 2002. – 512 с. – ISBN 5-8459-0258-4.
2. Амато Вито. Основы организации сетей Cisco [Текст] : в 2 т. Т. 2. : пер. с англ. / Вито Амато. – М. : Вильямс, 2002. – 464 с. – ISBN 5-8459-0283-5.
3. Борисенко Л. А. Локальная сеть. Просто как дважды два [Текст] / – Л. А. Борисенко. – М. : Эксмо, 2007. – 160 с. ISBN 978-5-699-14119-7.
4. Буассо М. Введение в технологию АТМ [Текст] / М. Буассо, М. Деманж, Ж.-М. Мюнье. – М. : Радио и связь, 2007. – 128 с. – ISBN 5-256-01359-9.
5. Гаршина В. В. Проектирование компьютерных сетей в среде Netcracker : учебно-методическое пособие [Текст] / В. В. Гаршина, А. С. Коваль. – Воронеж : ИПЦ ВГУ, 2007. – 38 с.
6. Гудыно Л. П. Вычислительные системы, сети и телекоммуникации [Текст] / Л. П. Гудыно, А. А. Кириченко, А. П. Пятибратов. – М. : Финансы и статистика Инфра-М, 2008. – 736 с. – ISBN 978-5-279-03285-3.
7. Гук Михаил. Аппаратные средства локальных сетей. Энциклопедия [Текст] / Михаил Гук. – СПб. : Питер, 2000. – 576 с. – ISBN 5-8046-0113-X.
8. Дансмор Брэдли. Справочник по телекоммуникационным технологиям [Текст] / Брэдли Дансмор. – М. : Диалектика-Вильямс, 2003. – 640 с. – ISBN: 5-8459-0562-1.
9. Дилип Найк. Стандарты и протоколы Интернета [Текст] / Найк Дилип. – Channel Trading Ltd, 1999. – 362 с. – ISBN 5-7502-0102-3.
10. Жуков А. И. Основы сетевых технологий [Текст] : учебное пособие / А. И. Жуков, М. М. Ластовченко. – М. : МК-Пресс Додэка, 2007. – 432 с. – ISBN 978-966-8806-30-8.
11. Колбин Р. В. Глобальные и локальные сети: создание, настройка и использование [Текст] / Р.В. Колбин. – М. : Бином. Лаборатория знаний, 2008. – 55 с. – ISBN 978-5-94774-565-8.
12. Кульгин Максим. Компьютерные сети, практика построения [Текст] / Максим Кульгин. – СПб. : Питер, 2003. – 464 с. – ISBN 5-94723-563-3.
13. Кульгин Максим. Практика построения компьютерных сетей. Для профессионалов [Текст] / Максим Кульгин. – СПб. : Питер, 2001. – 320 с. – ISBN 5-272-00351-9.

14. Куроуз Дж. Компьютерные сети [Текст] / Дж. Куроуз, К. Росс. – 2-е издание. – СПб. : Питер, 2004. – 765 с. – ISBN 5-8046-0093-1.
15. Леинванд Аллан. Конфигурирование маршрутизаторов Cisco [Текст] / Аллан Леинванд, Брюс Пински. – 2-е издание. – М. : Вильямс, 2001. – 558 с. – ISBN 5-8459-0219-3.
16. Лемке Джуди. Office Visio 2007 [Текст] / Джуди Лемке. – М. : ЭКОМ Паблишерз, 2008. – 368 с. – ISBN 978-5-9790-0065-7.
17. Майкрософт. Основы компьютерных сетей [Текст] / Майкрософт.– Бином, 2007. – 160 с. – ISBN: 978-5-94774-752-2.
18. Максимов Н. В. Компьютерные сети [Текст] : учебное пособие / Н. В. Максимов, И. И. Попов. – М. : ФОРУМ, 2008. – 448 с. – ISBN 978-5-91134-235-7.
19. Новиков, Ю. В. Локальные сети: архитектура, алгоритмы, проектирование [Текст] / Ю.В. Новиков, С.В. Кондратенко. – М: ЭКОМ, 2000. – 312с. – ISBN 7163-0061-8.
20. Новиков Ю. В. Основы локальных сетей. Курс лекций [Текст] / Ю. В. Новиков, С. В. Кондратенко. – М. : Интуит, 2005. – 360 с. – ISBN 5-9556-0032-9.
21. Норберг Стефан. Безопасность серверов Windows NT/2000 в Интернете [Текст] / Стефан Норберг. – СПб. : Символ-Плюс, 2001. – 224 с. – ISBN 5-93286-022-7.
22. Обжим сетевого кабеля [Електронний ресурс] / Краснодарський філіал ЗАО “ЮТК”. – Режим доступу : http://www.kuban.ru/forum_new/forum1/modpage/FAQ/faq/lan/index.htm. – Назва з сторінки Інтернету.
23. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] / В.Г. Олифер, К.А. Олифер. – СПб. : Питер, 2001. – 672 с. – ISBN 5-8046-0133-4.
24. Олифер В.Г. Сетевые операционные системы [Текст] / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2002. – 544 с. – ISBN 5-272-00120-6.
25. Основы компьютерных сетей [Текст] : учебное пособие / Б. Д. Виснадул, С. А. Лупин, С. В. Сидоров, П. Ю. Чумаченко. – М. : ФОРУМ:ИНФРА-М, 2007. – 272 с. – ISBN 5-8199-0294-7.
26. Паркер Тим. TCP/IP. Для профессионалов [Текст] / Тим Паркер. – СПб. : Питер, 2004. – 859 с. – ISBN 5-8046-0041-9.
27. Платонов В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей [Текст] / В. В. Платонов. – Академия, 2006. – 240 с. – ISBN 5-7695-2706-4.
28. Самарский П. А. Основы структурированных кабельных систем [Текст] / П. А. Самарский. – М. : ДМК Пресс, 2005. – 216 с. – ISBN 5-98453-014-7.

29. Семенов Л. В. Администрирование структурированных кабельных систем [Текст] / Л. В. Семенов. – М. : ДМК Пресс, 2008. – 192 с. – ISBN 978-5-94074-431-3.
30. Сергеев А. П. Офисные локальные сети [Текст] / А. П. Сергеев. – Диалектика, 2003. – 320 с. – ISBN 5-8459-0504-4.
31. Столлингс В. Современные компьютерные сети [Текст] / В. Столлингс. – 2-е издание. – СПб. : Питер, 2003. – 783 с. – ISBN 5-94723-327-4.
32. Строчников К.С. Компьютерные сети [Текст] : учебное пособие / К. С. Строчников, А. В. Велихов, Б. К. Леонтьев. – М. : Новый издательский дом, 2005. – 304 с. – ISBN 5-9643-0072-3.
33. Таненбаум Э. Компьютерные сети [Текст] / Э. Таненбаум. – 4-е издание. – СПб. : Питер, 2003. – 992 с. – ISBN 5-318-00492-X.
34. Телекоммуникационные системы и сети [Текст] : учебное пособие в 3 т. Т. 3 / В. В. Величко, Е. А. Субботин, В. П. Шувалов. А. Ф. Ярославцев. – М. : Горячая линия – Телеком, 2005. – 592 с. – ISBN 5-93517-257-7.
35. Тестовая и измерительная аппаратура. [Електронний ресурс] / Офіційний сайт російського представництва компанії Fluke – Режим доступу : http://fluke.ru. – Назва з сторінки Інтернету.
36. Фейт С. TCP/IP Архитектура, протоколы, реализация [Текст] / С. Фейт. – М. : Лори, 2000. – 424 с. – ISBN 5-85582-072-6.
37. Фролов Александр. Сети компьютеров в вашем офисе [Текст] : в 3 т. Т. 3 / А. Фролов, Г. Фролов. – М. : Диалог-МИФИ, 1995. – 272 с. – ISBN 5-86404-056-8.
38. Хант К. TCP/IP. Сетевое администрирование [Текст] / К. Хант.– 3-е издание. – М. : Символ, 2004. – 816 с. – ISBN 5-93286-056-1.
39. Чекмарев Ю.В. Локальные вычислительные сети [Текст] : учебное пособие / Ю. В. Чекмарев. – М. : ДМК, 2009. – 200 с. – ISBN: 978-5-94074-460-3.
40. 802.5w-2000 IEEE Standard for Information Technology – Token Ring Access Method and Physical Layer Specifications [Електронний ресурс] / Standard. – 2000. – Режим доступу : http://standards.ieee.org/getieee802/index.html. – Назва з сторінки Інтернету.
41. A TCP/IP Tutorial [Електронний ресурс] / Protocol specification. Request for Comments: 1180. – January 1991. – Режим доступу : http://tools.ietf.org/html/rfc1180. – Назва з сторінки Інтернету.
42. An Ethernet Address Resolution Protocol [Електронний ресурс] / Protocol specification. Request for Comments: 826. – November 1982. – Режим доступу : http://tools.ietf.org/html/rfc826. – Назва з сторінки Інтернету.
43. Cisco Systems, Inc. [Електронний ресурс] / Офіційний сайт компанії Cisco Systems – Режим доступу : http://cisco.com. – Заголовок с екрана.

44. Cisco Systems, Inc. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство [Текст] : пер. с англ. / Cisco Systems, Inc. – М. : ООО “И.Д. Вильямс”, 2007. – 994 с. – ISBN –5-8459-1120-6.
45. Domain names – implementation and specification [Електронний ресурс] / Standard. Request for Comments: 1035. – November 1987. – Режим доступу : http://tools.ietf.org/html/rfc1035. – Назва з сторінки Інтернету.
46. Hypertext Transfer Protocol – HTTP/1.1 [Електронний ресурс] / Standard. Request for Comments: 2616. – June 1999. – Режим доступу : http://tools.ietf.org/html/rfc2616. – Назва з сторінки Інтернету.
47. Internet control message protocol [Електронний ресурс] / Protocol specification. Request for Comments: 792. – September 1981. – Режим доступу : http://tools.ietf.org/html/rfc792. – Назва з сторінки Інтернету.
48. Internet protocol [Електронний ресурс] / Protocol specification. Request for Comments: 791. – September 1981. – Режим доступу : http://tools.ietf.org/html/rfc791. – Назва з сторінки Інтернету.
49. Internet Standard Subnetting Procedure [Електронний ресурс] / Standard. Request for Comments: 950. – August 1985. – Режим доступу : http://tools.ietf.org/html/rfc950. – Назва з сторінки Інтернету.
50. ISO 9314-1:1989. Information processing systems – Fibre Distributed Data Interface (FDDI) – Part 1: Token Ring Physical Layer Protocol (PHY) [Електронний ресурс] / Standard. – 1998. – Режим доступу : http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm ?csnumber=16973. – Назва з сторінки Інтернету.
51. OSPF Version 2 [Електронний ресурс] / Standard. Request for Comments: 2328. – April 1998. – Режим доступу : http://tools.ietf.org/html/rfc2328. – Назва з сторінки Інтернету.
52. Reichle & De-Massari AG (R&M) [Електронний ресурс] / Офіційний сайт компанії Reichle & De-Massari – Режим доступу : http://.rdm.com. – Заголовок с екрана.
53. Requirements for Internet Hosts – Communication Layers [Електронний ресурс] / Standard. Request for Comments: 1122. – October 1989. – Режим доступу : http://tools.ietf.org/html/rfc1122#section-3. – Назва з сторінки Інтернету.
54. RIP Version 2 [Електронний ресурс] / Standard. Request for Comments: 2453. – November 1998. – Режим доступу : http://tools.ietf.org/html/rfc2453. – Назва з сторінки Інтернету.
55. Transmission control protocol [Електронний ресурс] / Protocol specification. Request for Comments: 793. – September 1981. – Режим доступу : http://tools.ietf.org/html/rfc793. – Назва з сторінки Інтернету.
56. User Datagram Protocol [Електронний ресурс] / Protocol specification. Request for Comments: 768. – August 1980. – Режим доступу : http://tools.ietf.org/html/rfc768. – Назва з сторінки Інтернету.

Навчальне видання

Укладачі:
Гордєєв Олександр Олександрович
Гордєєва Дар'я Валеріївна
Колдовський Микола Васильович

КОМП'ЮТЕРНІ МЕРЕЖІ

Навчальний посібник
для студентів вищих навчальних закладів

Редактор *Н.І. Козьменко*

Комп'ютерна верстка *Н.А. Височанська*

Підписано до друку 05.04.2011. Формат 60х90/16. Гарнітура Times.
Обл.-вид. арк. 12,3. Умов. друк. арк. 15,8. Тираж 300 пр. Зам. № 1011

Державний вищий навчальний заклад
“Українська академія банківської справи Національного банку України”
40000, м. Суми, вул. Петропавлівська, 57
Свідоцтво про внесення до Державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції: серія ДК, № 3160 від 10.04.2008

Надруковано на обладнанні Державного вищого навчального закладу
“Українська академія банківської справи Національного банку України”
40000, м. Суми, вул. Петропавлівська, 57