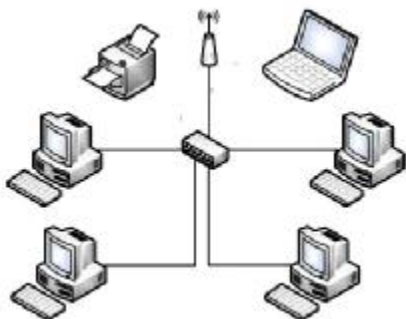




МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ  
УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ  
«МИНСКИЙ ГОСУДАРСТВЕННЫЙ ВЫСШИЙ  
РАДИОТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

## СЕТИ ЭВМ

ЛАБОРАТОРНЫЙ ПРАКТИКУМ



МИНСК 2013

## СЕТИ ЭВМ

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

для студентов специальности  
1-08 01 01 «Профессиональное обучение»  
по направлению 1-08 01 01-07 «Информатика»

Минск  
МГВРК  
2013

УДК 002.56(075)  
ББК 32.973.202я7  
С32

Рекомендовано к изданию кафедрой информатики (протокол № 7 от 28.02.2013 г.) и Научно-методическим советом учреждения образования «Минский государственный высший радиотехнический колледж» (протокол № 8 от 21.03.2013 г.)

**С о с т а в и т е л и:**

**В. Г. Лукьянец**, доцент кафедры информатики МГВРК,  
канд. техн. наук, доцент  
**Ю. А. Скудняков**, зав. кафедрой информатики МГВРК,  
канд. техн. наук, доцент

**Р е ц е н з е н т**

**М. А. Бельчик**, старший преподаватель  
кафедры информатики МГВРК

С32

**Сети ЭВМ** : лаб. практикум для студентов специальности 1-08 01 01 «Профессиональное обучение» по направлению 1-08 01 01-07 «Информатика» / сост. В. Г. Лукьянец, Ю. А. Скудняков. – Минск : МГВРК, 2013. – 76 с.  
ISBN 978-985-526-183-5

Цель практикума – предоставление студентам возможности получения навыков построения и настройки сетей ЭВМ.  
Предназначен для студентов и преподавателей.

УДК 002.56(075)  
ББК 32.973.202я7

**ISBN 978-985-526-183-5**

© Лукьянец В. Г., Скудняков Ю. А.,  
составление, 2013  
© Учреждение образования «Минский  
государственный высший радиотехнический колледж», 2013

## Предисловие

Вычислительная сеть (ВС) состоит из вычислительных машин и сети передачи данных (сети связи). ВС классифицируются по геометрическим масштабам:

- глобальные (англ. Global Area Network, GAN);
- региональные (англ. Metropolitan Area Network, MAN);
- локальные (англ. Local Area Network, LAN).

Под локальной вычислительной сетью (ЛВС) обычно понимают сеть, соединяющую близко расположенные компьютеры.

ЛВС – это система, составленная из отдельных модулей, которые можно добавлять и выстраивать в нужной конфигурации. Кроме основных компонент, сеть может включать в состав блоки бесперебойного питания, резервные приборы, современные динамически распределяемые объекты и различные типы серверов (файл-серверы, принт-серверы или архивные серверы).

Создавая ЛВС, разработчик решает следующие задачи:

- выбор архитектуры сети;
- выбор компонентов ЛВС;
- оценка показателей эффективности ЛВС;
- определение стоимости ЛВС.

Исходные данные для проектирования ЛВС могут быть получены в ходе предпроектного анализа прикладной области, для которой создается сеть. Эти данные уточняются в ходе проектирования, а затем принимается решение о построении сети. Лучшая ЛВС – это та, которая удовлетворяет всем требованиям пользователей, сформулированным в техническом задании на разработку ЛВС, при минимальном объеме капитальных и эксплуатационных затрат.

Данный лабораторный практикум посвящен изучению методов проектирования конфигурации ЛВС, а также изучению возможностей настройки и исследования параметров локальных вычислительных сетей.

## ЛАБОРАТОРНАЯ РАБОТА 1 СОЗДАНИЕ ОДНОРАНГОВОЙ СЕТИ

**Цель работы:** приобретение навыков создания одноранговой сети при использовании топологии сети типа «звезда» и с концентратором, а также с непосредственным соединением компьютер–компьютер.

### Задача лабораторной работы

В процессе выполнения работы надо научиться:

- выбирать аппаратное и программное обеспечение, необходимое для создания одноранговых сетей;
- создавать одноранговые сети;
- проводить тестирование одноранговых сетей.

### Задание для самоподготовки

Рекомендуется ознакомиться с материалами:

- встроенной помощью ОС MS Windows: **Центр справки и поддержки: Общие сведения о протоколе TCP/IP;**
- выводом справочных сведений о командах. Встроенная помощь к программам ОС MS Windows реализуется при помощи команды: **HELP [команда], конструкции [команда] /?**

### Схема лабораторной работы

Используются следующие варианты построения локальной сети:

- 1) построение локальной сети на основе концентратора;
- 2) соединение двух компьютеров напрямую, с помощью кроссовера Ethernet.

### Содержание работы

1. Собрать схему лабораторной работы.
2. Провести анализ сети.
3. Составить отчет.

## 1. Порядок выполнения работы

**Внимание!** Перед началом работы необходимо сохранить текущие настройки компьютера. Для этого через меню **Пуск** → **Программы** → **Стандартные** → **Служебные** вызвать програм-

му **Восстановление системы** и выбрать опцию **Создать точку восстановления**, задав имя **Контрольная точка** перед созданием сети. В случае неудачи всегда можно восстановить эту точку выбором опции **Восстановление более раннего состояния компьютера** и указав имя контрольной точки.

### 1.1. Соединение компьютеров при помощи хаба

Для всех компьютеров присоедините сетевые адаптеры рабочих станций к хабу (концентратору), используя кабель пятой категории с RJ-45 коннекторами.

Все компьютеры класса разделите на рабочие группы по два компьютера в группе. Запустите компьютеры, которые будут объединены в индивидуальные рабочие группы.

Для того чтобы начать создание одноранговой сети для рабочей группы, запустите **Мастер настройки сети**, выполнив следующие действия на каждом из компьютеров сети:

- 1) щелкните **Пуск**, затем – **Панель управления**;
- 2) щелкните **Сетевые подключения**, а затем на правой панели – **Установить домашнюю сеть или сеть малого офиса**;
- 3) на странице **Мастер настройки сети** (рис. 1.1) щелкните **Далее**.

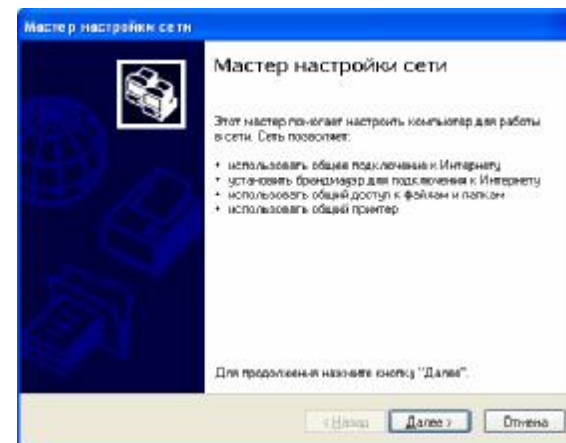


Рис. 1.1. Мастер настройки сети

Затем просмотрите требования (рис. 1.2) и, убедившись, что все правильно, щелкните **Далее**.

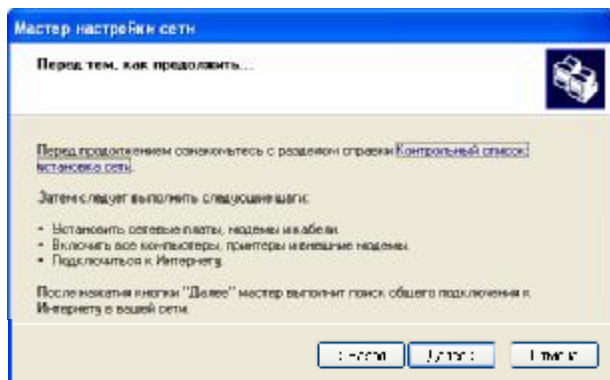


Рис. 1.2. Требования к сети

На странице **Выберите метод подключения** (рис. 1.3) щелкните **Другое** и затем – **Далее**.

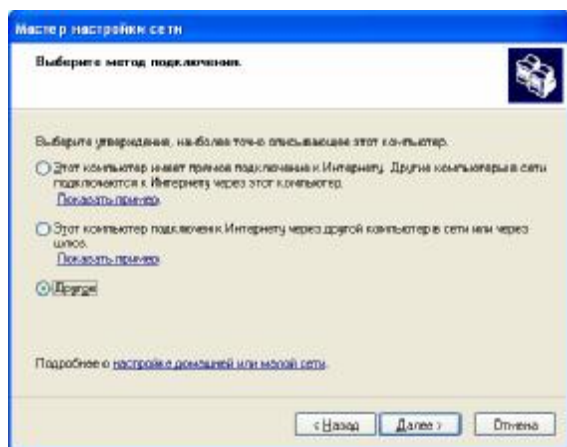


Рис. 1.3. Выбор метода подключения

На странице **Другие способы подключения к Интернету** (рис. 1.4) щелкните **Этот компьютер принадлежит к сети, не имеющей подключения к Интернету**, затем – **Далее**.

В текстовое поле **Описание** введите имя рабочей станции. В качестве имени используйте фамилии членов бригады студентов, работающих на данном компьютере, например **Боровиков\_Иванова**.

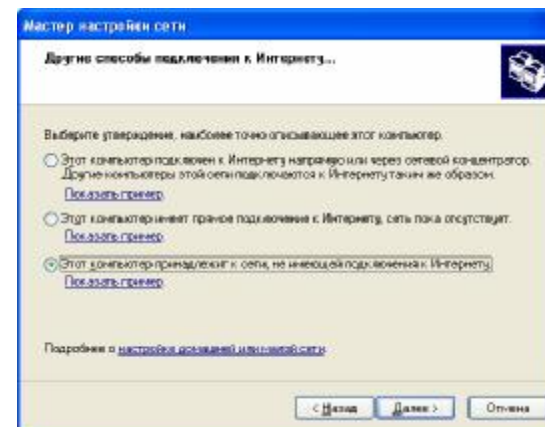


Рис. 1.4. Подключение к Интернету

В текстовое поле **Имя компьютера** введите уникальное имя (например, **Team15**, называя так свою рабочую станцию в сети), а затем щелкните **Далее** (рис. 1.5).

Замечание. Присваивая имя своему компьютеру, убедитесь, что это имя уникально в данной рабочей группе. Именуйте компьютеры по маске **Team[номер\_бригады]**, например, **Team15** для студентов бригады номер 15 по списку преподавателя.

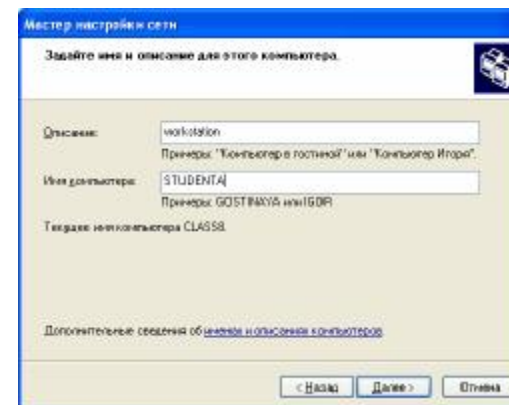


Рис. 1.5. Имя компьютера

На странице **Задайте имя для вашей сети** смените стандартное имя на согласованное с вашими партнерами (рис. 1.6).

Имя группы должно быть уникальным и совпадать для компьютеров рабочей группы, но отличаться от других групп в сети!

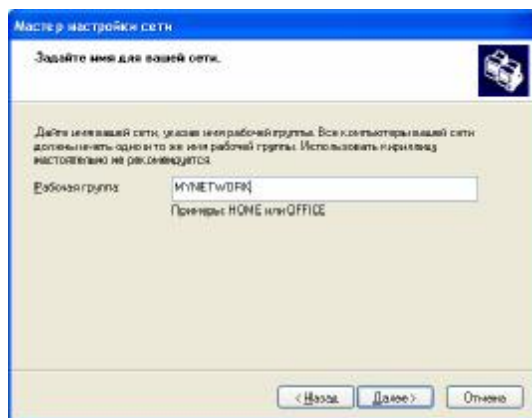


Рис. 1.6. Имя рабочей группы

На странице **Все готово для применения сетевых параметров** (рис. 1.7) проверьте установки и затем щелкните **Далее**, чтобы начать процесс создания сетевого соединения.

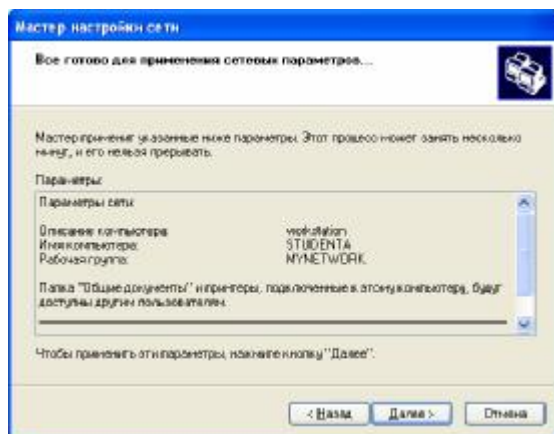


Рис. 1.7. Суммарная информация

На следующей странице (рис. 1.8) щелкните **Просто завершить работу мастера**, а затем – **Далее**.

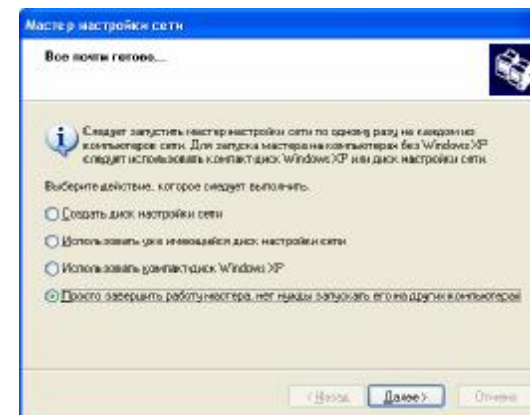


Рис. 1.8. Итоговая информация

На странице **Завершение работы мастера настройки сети** щелкните **Готово**. Если будет предложено перезагрузить ваш компьютер, то щелкните **Да**.

На этом компьютере можно начать работу.

Для проверки работы одноранговой сети необходимо создать папку для совместного использования на каждом компьютере. Выполните следующие действия на каждом компьютере. Если за компьютером работают несколько студентов, каждый из них должен выполнить нижеприведенные указания:

1) на диске **D:** в папке с именем своей группы создайте папки с именами, состоящими из слова **Папка** и фамилии студента, например, **Папка Боровикова**;

2) щелкните правой кнопкой мыши по только что созданной папке и выберите пункт меню **Общий доступ и безопасность**;

3) во вкладке **Доступ** щелкните **Открыть общий доступ к этой папке** и нажмите **ОК**;

4) в правой половине открывшегося окна дважды щелкните по только что созданной папке;

5) в открывшемся окне щелкните **Файл**, отметьте **Создать** и щелкните **Текстовый документ**;

6) введите имя документа (используйте ваше имя для названия файла) и нажмите **Enter**.

Дождитесь, пока остальные студенты создадут файлы в папках для совместного использования.

Для доступа к совместно используемым файлам, созданным на других компьютерах, необходимо следовать указаниям:

1) щелкните **Пуск**, отметьте **Все программы**, щелкните **Стандартные**, а затем – **Проводник**;

2) на левой панели щелкните **Сетевое окружение**, а затем – **Отобразить компьютеры рабочей группы**.

Замечание. Теперь можно увидеть список компьютеров вашей рабочей группы;

3) на правой панели дважды щелкните по какому-либо компьютеру (не своему), чтобы найти файлы, созданные другими учащимися для совместного пользования;

4) на правой панели дважды щелкните по одной из созданных папок для получения доступа к файлам, созданным другими студентами;

5) на правой панели дважды щелкните по имени файла, чтобы открыть его. Итак, вы получили удаленный доступ к файлам на другом компьютере.

Необходимо зафиксировать IP-адреса компьютеров вашей рабочей группы и поместить информацию о них в отчет по лабораторной работе.

## 1.2. Непосредственное соединение двух компьютеров

Если нужно соединить два компьютера между собой непосредственно, то достаточно всего лишь иметь в компьютерах сетевые карты и специальный кабель, который называется кроссовер по причине того, что две медные пары в его разъемах обжаты крест-накрест. Именно этим он отличается от кабеля, применяемого для соединения компьютера с хабом.

Замечание. Большинство современных сетевых карт поддерживают автоматическое определение полярности MDI/MDIX. Это исключает необходимость в использовании кабеля типа кроссовер. Однако при соединении компьютеров с неизвестной архитектурой, особенно если один из них работает под управлением Windows XP, лучше обжать кабель кроссовером.

Настройка сети между Windows 7 и Windows XP начинается с настройки подключения компьютера с установленной Windows XP. В первую очередь нужно создать физическое соединение между двумя компьютерами. Включите питание на двух компьютерах и вставьте кабель в разъемы на сетевых картах. Когда

кабель будет подсоединен, рядом с разъемом на сетевой карте настольного компьютера должен загореться индикатор.

Следующее действие по настройке локальной сети между двумя компьютерами – настройка сетевой карты. Настраивать сетевые карты компьютеров на получение IP-адресов будем вручную.

Для этого в Windows XP нажмите **Пуск** → **Настройка** → **Панель управления**. Если на экране появилось окно с видом по категориям, нажмите **Переключение к классическому виду** (рис. 1.9).

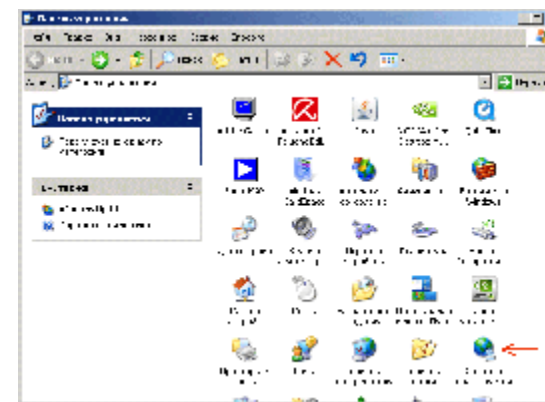
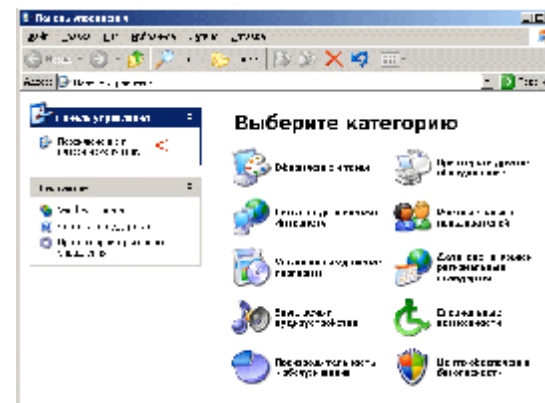


Рис. 1.9. Панель управления Windows XP

Нажмите **Сетевые подключения** (рис. 1.10).

Наведите курсор мыши на **Подключение по локальной сети** и нажмите правую кнопку мыши (рис. 1.11). Выберите **Свойства**.

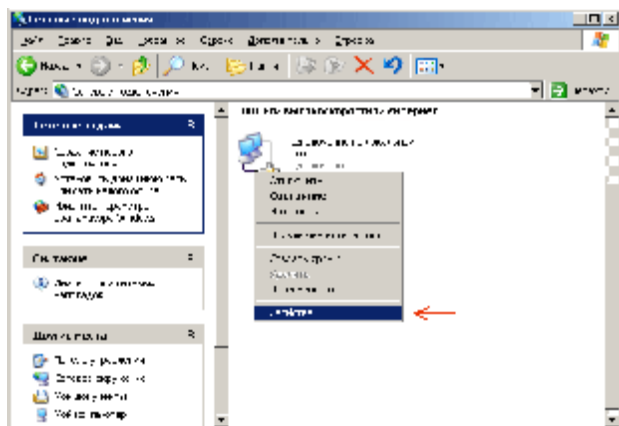


Рис. 1.10. Окно Сетевые подключения

Выберите пункт **Протокол Интернета TCP/IP** (рис. 1.12), нажмите **Свойства**.



Рис. 1.11. Окно свойств сетевых подключений



Рис. 1.12. Окно свойств протокола TCP/IP

В появившемся окне укажите требуемый IP-адрес, маску подсети, адрес шлюза и адреса DNS-серверов, используя следующие настройки сетевых карт (табл. 1.1):

Таблица 1.1

Параметр	Компьютер 1	Компьютер 2
IP-адрес	192.168.0.1	192.168.0.2
Маска подсети	255.255.255.0	255.255.255.0
Основной шлюз	192.168.0.1	192.168.0.1
Предпочитаемый DNS-сервер	192.168.0.1	192.168.0.1
Альтернативный DNS-сервер	Не заполняем	Не заполняем

Нажмите **ОК** и закройте все относящиеся к сетевым настройкам окна. Локальная сеть из двух компьютеров настроена!

Для проверки связи откройте командную строку (**Пуск** → **Выполнить** → **cmd** → **Enter**) и наберите команду **ping 192.168.0.1**. Должен получиться примерно такой результат:

Обмен пакетами с 192.168.0.1 по 32 байт:

Ответ от 192.168.0.1: число байт=32 время=1мс TTL=64

Ответ от 192.168.0.1: число байт=32 время=1мс TTL=64

Ответ от 192.168.0.1: число байт=32 время<1мс TTL=64

Ответ от 192.168.0.1: число байт=32 время=1мс TTL=64

Статистика Ping для 192.168.0.1:

Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),

Приблизительное время приема-передачи в мс:

Минимальное = 0 мсек, Максимальное = 1 мсек, Среднее = 0 мсек

Наберите команду **ping 192.168.0.2**. Должен получиться примерно такой результат:

Обмен пакетами с 192.168.0.2 по 32 байт:

Ответ от 192.168.0.2: число байт=32 время=1мс TTL=64

Ответ от 192.168.0.2: число байт=32 время=1мс TTL=64

Ответ от 192.168.0.2: число байт=32 время<1мс TTL=64

Ответ от 192.168.0.2: число байт=32 время=1мс TTL=64

Статистика Ping для 192.168.0.2:

Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь)

Приблизительное время приема-передачи в мс:

Минимальное = 0 мсек, Максимальное = 1 мсек, Среднее = 0 мсек

Если результат выполнения команды был таким, то соединение двух компьютеров в локальную сеть реализовано.

### 1.3. Передача файлов с компьютера на компьютер

*При работе под управлением Windows XP.* Для перекачки файлов с одного компьютера на другой в локальной сети компьютер-компьютер необходимо настроить на двух компьютерах одинаковые рабочие группы и дать двум компьютерам отличающиеся

имена в локальной сети. Выполните этот пункт при текущих настройках.

После перезагрузки двух компьютеров зайдите в **Сетевое окружение** и нажмите **Отобразить компьютеры рабочей группы**. Если на предыдущих этапах все сделано правильно, то отобразятся иконки двух компьютеров.

**При работе под управлением Windows 7.** В целом настройка сети в Windows 7 несущественно отличается от настройки сети Windows XP: в основном изменен интерфейс панели управления и соответствующих ее пунктов для доступа к нужным параметрам сети. В остальном – настройка IP-адресов, маски подсети практически не изменились (рис. 1.13).

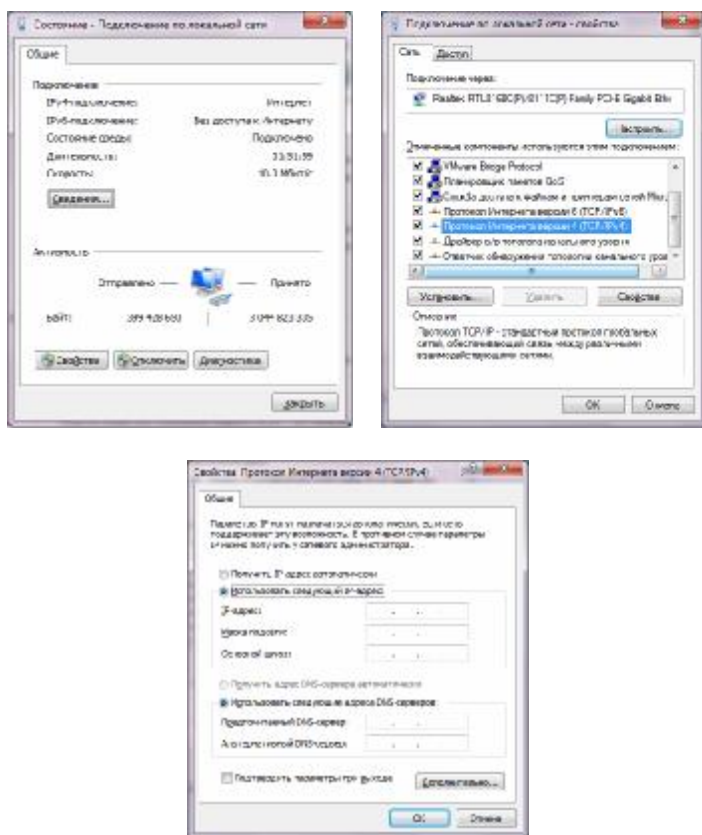


Рис. 1.13. Настройка свойств протокола TCP/IP

В Windows 7 кроме протокола IPv4 был добавлен протокол IPv6, значительно расширяющий диапазон используемых IP-адресов, однако насколько скоро он будет реально использован провайдерами, сказать тяжело.

### Содержание отчета

Опишите полученные результаты: информацию о порядке подключения и настройках компьютеров по каждому из вариантов создания сети.

### Контрольные вопросы

1. Что такое топология «звезда»?
2. Какая сеть называется одноранговой?
3. Что называют доменом компьютеров в сетях?
4. Что такое рабочая группа?
5. Как задать имя компьютера и рабочую группу?
6. Как обеспечить доступ к файлам на своем компьютере?

## ЛАБОРАТОРНАЯ РАБОТА 2

### СОЕДИНЕНИЕ ДВУХ КОМПЬЮТЕРОВ ПО WiFi

**Цель работы:** приобретение навыков непосредственного соединения компьютер–компьютер через WiFi.

### Задача лабораторной работы

В процессе выполнения работы надо научиться:

- выбирать аппаратное и программное обеспечение, необходимое для создания беспроводных сетей;
- создавать беспроводные сети;
- проводить тестирование беспроводных сетей.

### Задание для самоподготовки

Рекомендуется ознакомиться с материалами:

- встроенной помощью ОС MS Windows: **Центр справки и поддержки: Общие сведения о протоколе TCP/IP;**
- выводом справочных сведений о командах. Встроенная помощь к программам ОС MS Windows реализуется при помощи команды: **HELP [команда], конструкции [команда] /?**



## Схема лабораторной работы

Для выполнения лабораторной работы используется построение локальной сети типа компьютер–компьютер по WiFi.

## Содержание работы

1. Собрать схему лабораторной работы.
2. Провести анализ сети.
3. Составить отчет.

## 1. Порядок выполнения работы

**Внимание!** Перед началом работы необходимо сохранить текущие настройки компьютера. Для этого через меню **Пуск** → **Программы** → **Стандартные** → **Служебные** вызовите программу **Восстановление системы** и выберите опцию **Создать точку восстановления**, задав имя **Контрольная точка** перед созданием сети. В случае неудачи всегда можно восстановить эту точку, выбрав опции **Восстановление более раннего состояния компьютера** и указав имя контрольной точки.

### 1.1. Соединение двух компьютеров по WiFi (режим Ad-hoc) под управлением Windows XP

Для организации сети с помощью этого метода, называемого **Ad-hoc**, дополнительных устройств таких, как точка доступа не требуется. Единственным условием соединения двух компьютеров по **WiFi** является наличие в данных устройствах сетевого адаптера стандарта **WiFi**. Рассмотрим вначале настройку на машинах с операционной системой Windows XP.

#### 1.1.1. Активация сетевой карты WiFi

Для этого нужно попасть в папку **Сетевые подключения**. В зависимости от настроек ОС, сделать это можно несколькими способами:

- 1) **Пуск** → **Сетевое окружение** → **Свойства**;
- 2) **Пуск** → **Подключение** → **Отобразить все подключения**;
- 3) **Пуск** → **Панель управления** → **Сетевые подключения**.

Если все сделано правильно, появится следующее изображение (рис. 2.1):

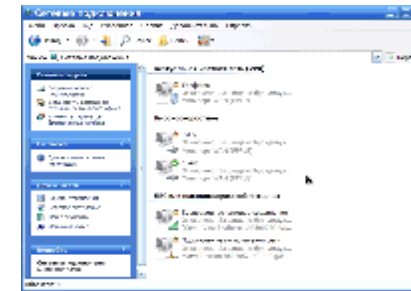


Рис. 2.1. Окно сетевых подключений

Из всех перечисленных подключений нас интересует **Беспроводное сетевое соединение**. Двойной щелчок мыши по этой иконке активирует сетевой адаптер WiFi. Нужно отметить, что многие ноутбуки имеют дополнительные возможности включения–отключения WiFi (обычно это специальная клавиша или комбинация клавиш), так называемое, аппаратное управление. Проверьте, не задействована ли подобная функция в вашем устройстве.

#### 1.1.2. Установка параметров сети WiFi

В папке **Сетевые подключения** щелкните правой кнопкой мыши на иконке **Беспроводное сетевое соединение** и выберите **Свойства**. Откроется следующее окно (рис. 2.2):

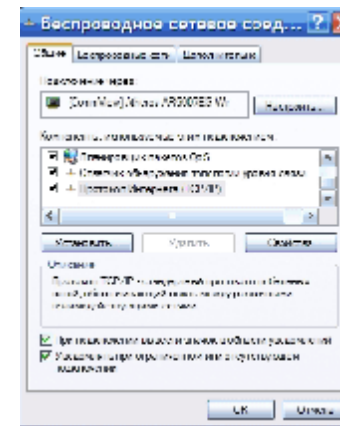


Рис. 2.2. Свойства беспроводного соединения

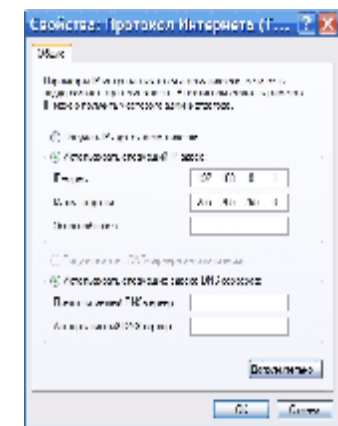


Рис. 2.3. Свойства протокола Интернет

Выберите **Протокол Интернета (TCP/IP)**, нажмите **Свойства**. Заполните поля открывшегося окна (рис. 2.3).

При заполнении свойств необходимо обеспечить разделение сетей. Для этого каждая бригада должна вводить собственные параметры сети. IP-адрес формируем по следующей маске: 192.168.[трехзначный номер группы в потоке].[трехзначный номер студента по журналу]. Например, студент группы 5381 (первая группа в потоке) Абелин А. А., числящийся в журнале под номером 1, должен использовать IP-адрес 192.168.001.001. Маска подсети 255.255.00. Нажмите **ОК**.

### 1.1.3. Создание сети WiFi

В окне свойств беспроводного сетевого соединения (рис. 2.4) переходим на вкладку **Беспроводные сети**.

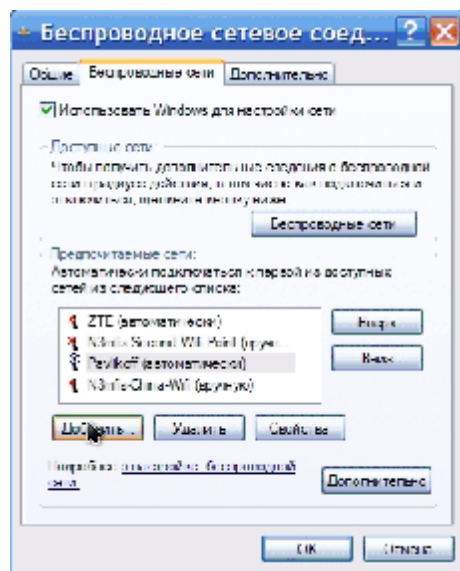


Рис. 2.4. Настройка беспроводного соединения

Здесь видны сети WiFi, находящиеся в радиусе действия нашего адаптера. В настоящий момент нас интересует создание собственной сети WiFi – поставьте галочку в поле **Использовать Windows для настройки сети**, нажмите **Добавить**. Появится следующая вкладка (рис. 2.5).

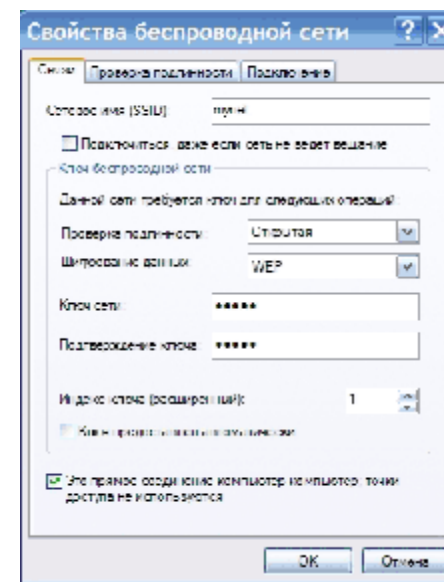


Рис. 2.5. Добавление нового беспроводного соединения

В поле **Сетевое имя (SSID)** введите название нашей будущей сети, которая под этим именем будет отображаться в списке доступных сетей. Имя сети формируем по номеру бригады, например, 5381\_1\_net. **Проверка подлинности** → **Открытая**, **Шифрование данных** → **WEP**.

Снимите отметку в поле **Ключ предоставлен автоматически** и введите пять произвольных символов в поле **Ключ сети**. Эта последовательность символов будет являться своеобразным паролем для остальных устройств при подключении к нашей сети. Дублируем ключ в поле **Подтверждение ключа**.

Перейдите на вкладку **Подключение**, где поставьте отметку в поле **Подключаться, если сеть находится в радиусе действия**. Нажмите везде **ОК**.

### 1.1.4. Настройка второго устройства

Настройте второй компьютер так же как и первый.

В свойствах **Протокола Интернета (TCP/IP)** в поле **IP-адрес** введите IP-адрес второго студента, остальное то же, что и для первого устройства.

В окне свойств беспроводного сетевого соединения на вкладке **Беспроводные сети** нажмите кнопку **Беспроводные сети**. Выберите свою сеть, нажмите **Подключить**. Введите **Ключ** сети. Сеть работает.

На этом соединении двух компьютеров по WiFi закончено.

### 1.1.5. Передача файлов с компьютера на компьютер

Напомним общие правила локальных сетей:

- необходимо, чтобы оба компьютера принадлежали к одной **Рабочей группе**, изменить название которой можно выполнив следующие действия: **Мой компьютер** → **Свойства** → **Имя компьютера** → **Изменить**;

- чтобы получить доступ к ресурсам одного компьютера с другого, их необходимо расшарить (предоставить общий доступ). Для какой-либо папки это делается так: **Свойства папки** → вкладка **Доступ** → **Открыть общий доступ к этой папке**.

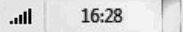
Эти действия надо выполнить, но для новой сети.

## 1.2. Настройка сети WiFi в Windows 7 и Windows XP для подключения компьютер–компьютер

Рассмотрим вариант соединения в сеть WiFi двух компьютеров, один из которых работает под управлением Windows 7, а второй – под управлением Windows XP.

### 1.2.1. Проверка наличия драйверов для беспроводной сети

Вначале убедимся, что на обоих компьютерах установлены драйверы для WiFi-адаптера. В правом нижнем углу экрана

(трее) находится иконка, похожая на лесенку: .

Вы видите ее на обоих компьютерах? Теперь переходите к следующему пункту. В противном случае необходимо проверить, что в системе установлены драйверы для всего оборудования.

Откройте **Пуск** и щелкните правой кнопкой мыши на пункте **Компьютер**. Выберите **Свойства**. В открывшемся окне выберите **Диспетчер устройств**. Убедитесь, что в списке устройств отсутствуют записи с иконкой в виде желтого вопросительного знака. Если такие записи есть, значит в системе установлены не все драйверы и надо посетить сайт производителя оборудования, чтобы скачать свежие драйверы для своего компьютера.

Если установка драйверов не требуется, адаптер отсутствует и в трее нет значка выбора беспроводной сети, то следует задуматься: есть ли в вашем компьютере беспроводной адаптер и нормально ли он работает.

### 1.2.2. Создание точки подключения на «ведущем» компьютере

Сеть для объединения компьютеров будем настраивать на компьютере под управлением Windows 7.

Нажмите на значок выбора беспроводной сети в правом нижнем углу (лесенка) и выберите **Центр управления сетями и общим доступом**. В открывшемся окне выберите **Настройка нового подключения или сети**.

В открывшемся списке (рис. 2.6) выберите пункт **Настройка беспроводной сети компьютер–компьютер**.

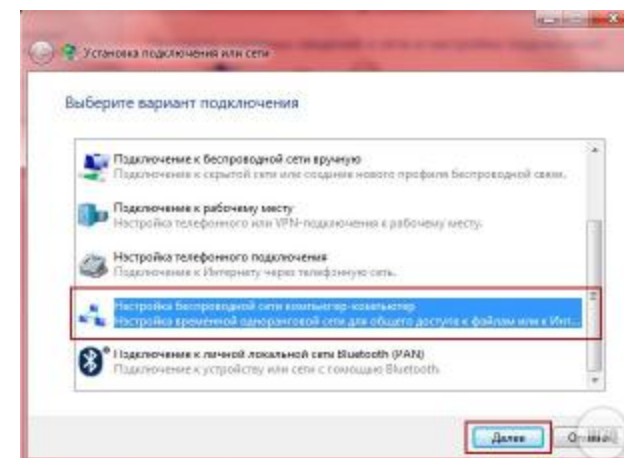


Рис. 2.6. Выбор настроек

Затем нажмите **Далее** (рис. 2.7).

Выбор пунктов в этом случае напрямую зависит от того, какая операционная система установлена на втором компьютере. Если там установлена Windows 7, то заполняйте форму, показанную на рис. 2.8.

В поле **Имя сети (SSID)** введите название нашей будущей сети. Под этим именем она будет отображаться в списке доступных сетей. Имя сети формируем по номеру бригады, например

5381\_1\_net. Шифрование данных – WEP. Введите пять произвольных символов в поле **Ключ сети**. Нажмите **Далее** и **Закрыть** (рис. 2.9).

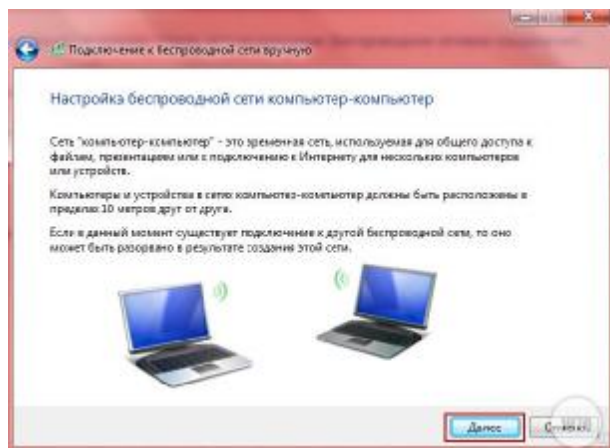


Рис. 2.7. Процесс подключения

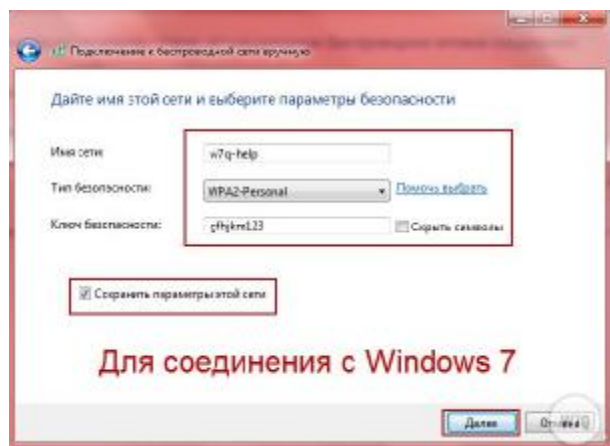


Рис. 2.8. Параметры подключения

Теперь настроим сеть на втором компьютере. В нашем примере на втором компьютере установлен Windows XP, но последовательность действий для Windows 7 ничем не отличается (разве что окна выглядят немного иначе).

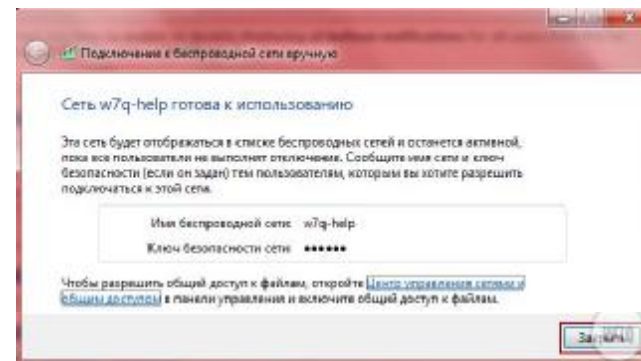


Рис. 2.9. Подключение к сети

Щелкните мышкой по значку **Подключение к беспроводной сети** и в списке сетей найдите созданную сеть (рис. 2.10).

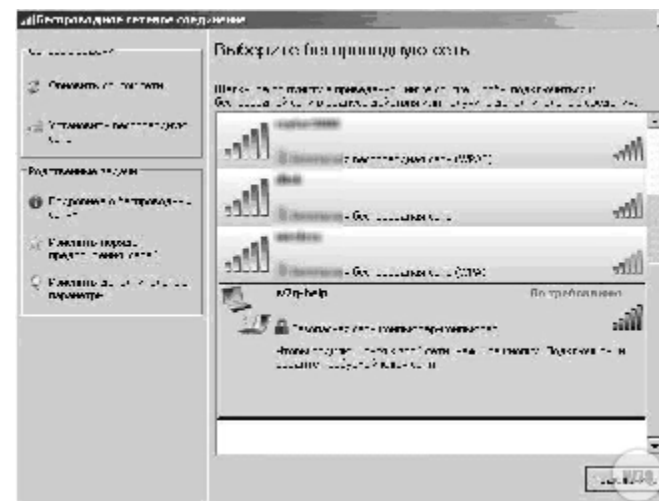


Рис. 2.10. Беспроводные соединения

Выделите название сети мышкой и нажмите **Подключить**. Теперь введите ключ безопасности, который мы задали ранее (рис. 2.11).

Некоторое время надо подождать, пока компьютеры получат адреса и можно проверять установленное соединение.

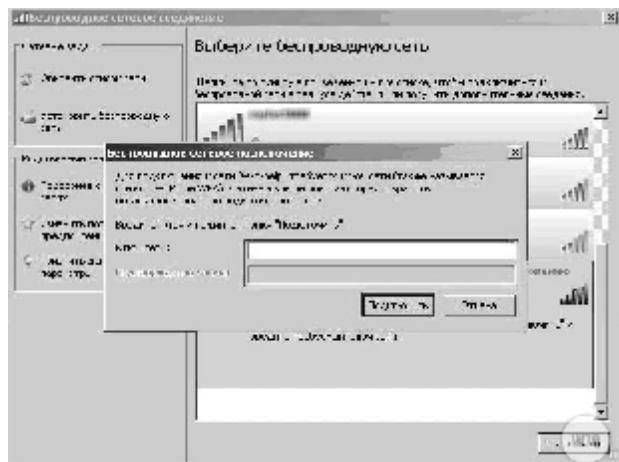


Рис. 2.11. Ввод пароля для беспроводного соединения

### 1.2.3. Проверка соединения между компьютерами

Снова откроем **Центр управления сетями и общим доступом** (щелкните на значке выбора беспроводных соединений).

Затем щелкните на значке с именем сети, как показано на рис. 2.12.

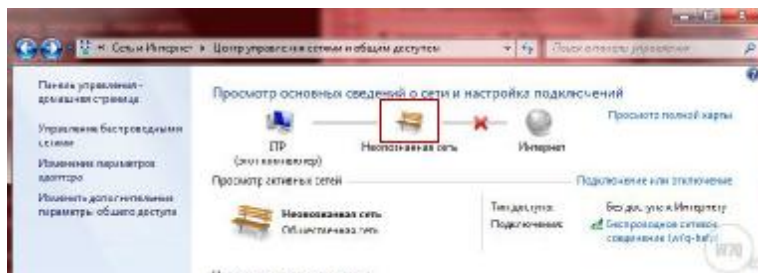


Рис. 2.12. Окно центра управления сетями и общим доступом

Должно открыться окно с перечнем компьютеров в сетевом окружении (рис. 2.13). Один из этих компьютеров ваш, второй – это удаленный компьютер, который присоединился к вам.

Имена компьютеров в конкретном случае будут естественно другими. Если вы увидите такую картинку, значит получилось соединение двух компьютеров по WiFi в сеть напрямую.

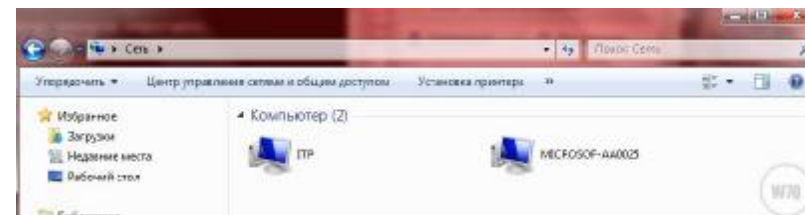


Рис. 2.13. Окно с перечнем компьютеров в сетевом окружении

### 1.2.4. Передача файлов с компьютера на компьютер

Для перекачки файлов с одного компьютера на другой в локальной сети компьютер–компьютер необходимо на двух компьютерах настроить одинаковые рабочие группы и дать двум компьютерам отличающиеся имена в локальной сети.

### Содержание отчета

Опишите полученные результаты: информация о порядке подключения и настройках компьютеров по каждому из вариантов создания сети.

### Контрольные вопросы

1. Какими способами можно создать локальную беспроводную сеть WiFi?
2. Что такое главный компьютер сети WiFi?
3. Какие методы шифрования используются в сетях WiFi?
4. Для каких целей может быть применена технология WiFi?

## ЛАБОРАТОРНАЯ РАБОТА 3 ДИАГНОСТИКА СЕТИ СРЕДСТВАМИ ОС

**Цель работы:** ознакомление со встроенными инструментальными средствами ОС MS Windows для отладки связи и диагностики сети; приобретение знаний о сетевом оборудовании, программном обеспечении и сетевых подключениях персонального компьютера, работающего под управлением ОС MS Windows.

### Задача лабораторной работы

Диагностика сети собирает информацию о компьютере для решения сетевых проблем. Чаще всего диагностика сети выполняется администратором сети или пользователем под руководством специалиста службы технической поддержки по телефону либо через Интернет.

Диагностика сети позволяет выполнить различные тесты. В зависимости от выбранных параметров диагностика сети тестирует сетевое взаимодействие и проверяет доступность некоторых сетевых служб и программ, а также производит сбор основной информации о компьютере. Это средство предоставляет пользователю или специалисту службы технической поддержки информацию, необходимую для поиска причин, вызвавших проблемы с сетью. Диспетчер состояния – еще один ключевой компонент справочной системы Windows XP, назначение которого – собирать данные, позволяющие выявить существующие или возможные неполадки, такие как некорректная загрузка или нехватка свободного пространства на диске. Система обрабатывает эту информацию и отображает ее в консоли центра справки и поддержки.

Работу диспетчера состояния обеспечивает служба Help and Support (Справка и поддержка). Она запускает исполняемый файл SVCHOST.EXE, который в свою очередь взаимодействует с файлом WMIPRVSE.EXE, собирающим информацию о системе. Еще несколько исполняемых файлов передают информацию в центр справки и поддержки и отображают информацию, собранную службой-поставщиком Windows Management Instruments (WMI), (Инструментарий управления Windows).

Не всегда проблемы связности очевидны, и выявить их инструментальными средствами не всегда сразу удается. Часто наблюдаются только симптомы, которые необходимо интерпретировать. Приходится поэтапно в логической последовательности использовать ряд инструментальных средств, следовательно, пользователь должен быть осведомлен относительно принципов организации сетей и возможностей каждого сетевого инструментального средства.

Возможные проблемы сети:

- оконечные нагрузки ЛВС должным образом не подключены;
- ЛВС-интерфейс неработоспособен;
- ЛВС-интерфейс имеет неправильный IP-адрес;
- маска подсети имеет неверное значение;

- тот же IP-адрес используется другой системой;
- конфигурация таблицы маршрутизации настроена неправильно;
- маршрутизатор выключен;
- кабель ЛВС поврежден;
- длина сегмента ЛВС слишком велика;
- неправильно указан DNS-сервер.

### Задание для самоподготовки

Рекомендуется ознакомиться с материалами:

- встроенной помощью ОС MS Windows **Центр справки и поддержки: Общие сведения о протоколе TCP/IP;**
- выводом справочных сведений о командах. Встроенная помощь к программам ОС MS Windows реализуется при помощи команды: **HELP [команда], конструкции [команда] /?**

### Схема лабораторной работы

Для выполнения лабораторной работы достаточно одного компьютера, подключенного к сети, или двух компьютеров, соединенных в сеть.

### Содержание работы

1. Собрать схему лабораторной работы.
2. Провести анализ связности сети.
3. Составить отчет.

## 1. Порядок выполнения работы

**Внимание!** Перед началом выполнения работы на диске **D:** должна быть создана рабочая папка. В ней накапливается информация по ходу выполнения работы и формируются отчеты. Имя рабочей папки должна совпадать с именем группы.

**Внимание!** При работе с утилитами командной строки для сохранения информации, выводимой на экран, следует переадресовать вывод, например, после команды вызова утилиты добавляем **>D:\5386\Result1.txt**. Для каждой команды необходимо указывать свое имя файла, в противном случае файл будет перезаписан. С помощью текстового редактора можно просмотреть этот файл и использовать его в отчете. Следует иметь в виду, что зачастую информация сохраняется без форматирования и после

создания файла следует его отредактировать: указать тип сохраненной информации и отформатировать. Можно отправлять данные и в один и тот же файл, добавляя к нему новые строчки. Для этого используется вариант команды `>>D:\5386\Result.txt`.

Например, подаем команду `ping 192.168.0.1>>D:\5386\Result.txt` и результат смотрим в файле `Result.txt` на диске `D:` в папке `5386`.

При просмотре результатов могут возникнуть проблемы с кодировкой выводимой информации на русском языке.

### 1.1. Сбор информации о системе

С помощью программы MS Windows **Сведения о системе** запустите командный процессор: **Пуск** → **Выполнить** → `cmd`. Последовательно выполните команды: `cd C:\Program Files\Common Files\Microsoft Shared\MSInfo\msinfo32\systeminfo`

### 1.2. Анализ связности сети, к которой подключен компьютер

С помощью команд MS Windows просмотрите и опишите подключение к локальной сети. Выполните из командной строки команды MS Windows для сбора информации о системе, указанные в табл. 3.1:

Т а б л и ц а 3.1

Команда	Содержание команды
<code>netstat.exe-rn route print</code>	Просмотреть записи в локальной таблице IP-маршрутизации
<code>netstat.exe-s</code>	Просмотреть статистические данные протоколов
<code>netstat.exe-a</code>	Просмотреть все подключения и ожидающие порты
<code>net /help</code>	Просмотреть команды сетевых служб
<code>ping tracert</code>	Проверить TCP/IP-соединения с помощью команд
<code>ipconfig.exe /all</code>	Вывести IP-адрес, маски подсети и основного шлюза для каждого сетевого адаптера
<code>nslookup</code>	Диагностировать инфраструктуру DNS (выйти из <code>nslookup</code> , <code>&gt;exit</code> или <code>Ctrl-C</code> )
<code>arp-a</code>	Просмотреть записи кэш, использующиеся для хранения IP-адресов и соответствующих им физических адресов Ethernet

### 1.3. Просмотр файлов, содержащих номера портов стандартных служб и файл сопоставления IP-адресов именам узлов

Последовательно выполните следующие команды:

```
more C:\WINDOWS\system32\drivers\etc\services
more C:\WINDOWS\system32\drivers\etc\services | find "http"
type C:\WINDOWS\system32\drivers\etc\services | find "ftp"
type C:\WINDOWS\system32\drivers\etc\services | find "tcp" |more
type C:\WINDOWS\system32\drivers\etc\services | find "udp" |
more
```

Ознакомьтесь с образцом файла HOSTS

```
cd C:\WINDOWS\system32\drivers\etc\
more hosts
```

#### Содержание отчета

Опишите полученные результаты: информация о сетевых настройках и подключениях компьютера.

#### Контрольные вопросы

1. Что определяет связность сети?
2. Какие утилиты используются в ОС Windows для анализа сетевых подключений компьютера?
3. Перечислите возможные проблемы при создании компьютерной сети и методы их устранения.

## ЛАБОРАТОРНАЯ РАБОТА 4 УПРАВЛЕНИЕ СЕТЕВЫМИ УЗЛАМИ

**Цель работы:** приобретение навыков применения различных технологий управления сетевыми узлами, такими как удаленное управление сетевыми устройствами, консоль Microsoft Management Console (MMC), технология удаленного рабочего стола (Remote Desktop Protocol).

#### Задачи лабораторной работы

В процессе выполнения работы изучить возможности:

- 1) консоли управления компьютером;
- 2) использования удаленного помощника;
- 3) использования удаленного рабочего стола.

### Задание для самоподготовки

Рекомендуется ознакомиться с материалами:

- встроенной помощью ОС MS Windows – **Центр справки и поддержки** возможностей консоли управления компьютером;
- возможностями использования удаленного помощника и удаленного рабочего стола.

### Содержание работы

Удаленное управление сетевыми устройствами – важная часть работы сетевого администратора. В данной работе на примере систем семейства Windows изучаются различные технологии управления сетевыми узлами. Применение консоли **Управление компьютером** позволяет решать многие задачи удаленного управления Windows-системами. Использование консоли ММС позволит создавать свои собственные консоли для решения различных задач удаленного управления.

Технология удаленного рабочего стола использована в двух инструментах: **Удаленный помощник** (предназначенный, в основном, для управления рабочими станциями) и **Удаленный рабочий стол** (называемый также службой терминалов). Данная технология дает возможность подключаться к рабочему столу удаленным компьютерам и работать с ними так же, как при локальном интерактивном входе в систему.

В Windows 7 (так же как и в предыдущих версиях Windows, начиная с XP) присутствует возможность работы на компьютере удаленно, используя запущенную службу терминальных подключений. Для доступа к компьютеру с работающей службой применяется программа **Доступ к удаленному рабочему столу**, присутствующая по умолчанию во всех версиях Windows, начиная с XP.

При работе используется последняя на сегодняшний день версия протокола RDP (Remote desktop protocol v.7), в котором была существенно изменена работа с мультимедиа данными (передача видео и звука), а также увеличена производительность.

**Внимание!** Следует помнить, что одновременно на компьютере может работать только один пользователь (включая удаленного), поэтому при подключении удаленного пользователя, все другие активные пользователи будут отключены!

**Внимание!** Доступ к компьютеру возможен в любой редакции Windows 7. А вот открыть доступ можно только на компьютере с профессиональной или максимальной редакцией Windows 7.

### Схема лабораторной работы

Собрать схему лабораторной работы, представляющую собой сеть, состоящую из двух компьютеров, соединенных кроссовером либо через WiFi.

## 1. Порядок выполнения работы

### 1.1. Консоль управления ММС

#### 1.1.1. Создание пользовательской консоли

В меню **Пуск** в поле поиска введите **mmc** и нажмите **Enter**. ММС выведет на экран пустую консоль. Разверните окно на весь экран. Чтобы просмотреть текущие параметры консоли, в меню **Файл** выберите команду **Параметры**. Заметьте, что по умолчанию используется авторский режим консоли. Помните, что данный режим предоставляет пользователям полный доступ ко всей функциональности ММС. Убедитесь, что в списке **Режим консоли** выбран пункт **Авторский режим**, и щелкните **ОК**.

В меню **Файл** выберите команду **Добавить/удалить оснастку**. Откроется диалоговое окно добавления и удаления оснасток. Обратите внимание на список доступных оснасток. ММС позволяет добавлять в консоль оснастки и создавать собственные средства управления.

Выберите **Управление компьютером** и щелкните кнопку **Добавить**. Откроется одноименное диалоговое окно.

Щелкните переключатель **Локальным компьютером**: (консоль того компьютера, на котором выполняется эта программа), а затем – кнопку **Готово**. В окне **Добавить/удалить оснастку** появился элемент **Управление компьютером (локальным)**.

Щелкните **ОК**, чтобы закрыть диалоговое окно.

В меню **Файл** выберите команду **Сохранить как**. Откроется одноименное диалоговое окно. В поле **Имя файла** введите **All Events** и щелкните кнопку **Save (ОК)**. Имя созданной консоли появится в заголовке окна ММС.

#### 1.1.2. Проверка местоположения пользовательской консоли

**Внимание!** Убедитесь, что консоль сохранена в папке **Административные средства**: закройте и повторно откройте созданную консоль.



В меню **Файл** выберите команду **Выход**. На данный момент вы создали и сохранили пользовательскую консоль All Events.

В меню **Пуск** в поле поиска введите **mmc** и щелкните **ОК**.

В меню **Файл** выберите команду **Открыть**. Откроется одноименное диалоговое окно. Заметьте, что созданная консоль **All Events.msc** находится в папке **Администрирование**.

Выберите файл **All Events** и щелкните кнопку **Открыть**. Windows XP откроет консоль All Events.

### 1.1.3. Добавление в консоль оснастки Event Viewer (Просмотр событий)

В меню **Файл** выберите команду **Добавить или удалить оснастку**. Откроется одноименное диалоговое окно. Заметьте, что загружена лишь оснастка **Управление компьютером**. Далее добавьте оснастку в корень консоли.

В диалоговом окне выберите оснастку **Просмотр событий** и щелкните кнопку **Добавить**. Откроется диалоговое окно. Подтвердите, что журналы будут просматриваться на локальном компьютере.

**Внимание!** Можно добавить оснастку Event Viewer для работы с локальным или удаленным компьютером, если локальный компьютер является частью сети. Чтобы добавить оснастку Event Viewer для работы с удаленным компьютером, щелкните переключатель **Другим компьютером**, а затем кнопку **Обзор**. В диалоговом окне **Выбор: компьютер** укажите удаленный компьютер и щелкните **ОК**. Теперь добавьте оснастку Event Viewer для работы с локальным компьютером.

В диалоговом окне **Добавить или удалить оснастку** нажмите **ОК**. Теперь в дереве консоли появился еще один узел **Просмотр событий (локальных)**.

### 1.1.4. Определение времени последнего запуска компьютера

В дереве консоли раскройте узел **Просмотр событий (локальных)**, и в окне **Обзор и сводка** в разделе **Сводка журнала** выберите журнал **Система**, щелкнув по нему мышкой. В правой панели появятся сведения о последних системных событиях.

Дважды щелкните в правой панели в разделе **Система** вариант **Просмотр событий**.

Установите курсор на самом последнем событии, которое будет первым в списке в верхней части окна, и в правой панели выберите действие **Поиск**. В открывшемся диалоговом окне введите **Запущена служба журнала событий**. Щелкните **Найти далее**.

Самое последнее событие, для которого в столбце **Источник** указано **Eventlog**, будет отображено в нижней части окна. Это и есть время последнего запуска компьютера. Зафиксируйте информацию о нем для помещения в отчет по лабораторной работе. Запишите, когда еще сегодня перезагружался компьютер.

В меню **Файл** выберите команду **Выход**, чтобы закрыть консоль All Events. В ответ на предложение сохранить консоль, щелкните кнопку **Нет**.

### 1.1.5. Удаление оснастки

В меню **Пуск** в поле поиска введите **mmc** и нажмите **Enter**. Откроется пустая консоль.

В меню **Файл** выберите команду **Открыть**.

Найдите созданную ранее оснастку All Events, щелкните правой клавишей мыши и выберите **Удалить**.

## 1.2. Работа с программой Удаленный помощник

Пользователи, особенно неопытные в техническом плане, часто не могут правильно настроить параметры или задают вопросы об использовании ПО, на которые специалисту поддержки трудно ответить по телефону. Удаленный помощник (Remote Assistance) предоставляет пользователям возможность получить помощь, облегчает и удешевляет работу корпоративных служб поддержки.

Сначала пользователю, которому нужна помощь, необходимо разрешить работу удаленного помощника: **Мой компьютер** → **Свойства системы** → **Настройка удаленного доступа** → **Удаленный доступ** (рис. 4.1). Поставьте галочку на **Разрешить подключение удаленного помощника к этому компьютеру**, потом можно нажать кнопку **Дополнительно** и разрешить удаленному помощнику управлять компьютером вместе с вами, иначе он будет только видеть ваш рабочий стол и писать советы, где и что вам делать.

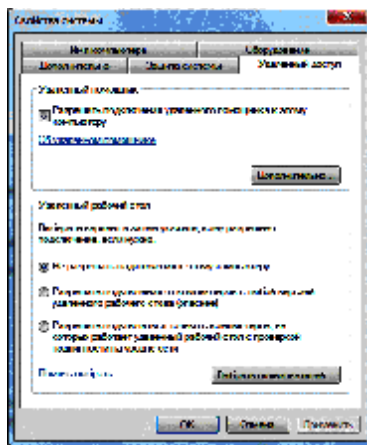


Рис. 4.1. Разрешение подключения

Если используется стандартный брандмауэр, встроенный в Windows 7, то зайдите **Панель управления** → **Система и безопасность** → **Брандмауэр Windows** → **Разрешить запуск программы или компонента через брандмауэр Windows** и на вкладке **Разрешить связь для программ через брандмауэр Windows** разрешите **Удаленный помощник** (рис. 4.2) или **Дистанционное управление рабочим столом**.

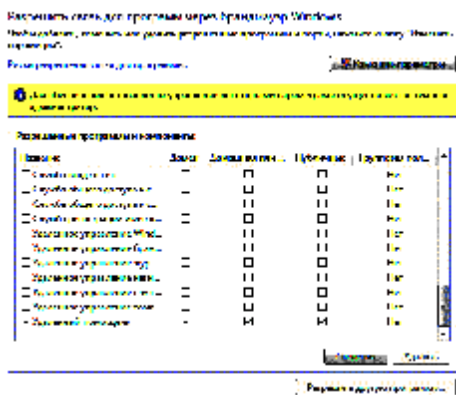


Рис. 4.2. Настройка брандмауэра

Далее для вызова помощника зайдите в **Пуск** → **Справка и поддержка**. Там в разделе **Спросить** нажмите ссылку **Обраще-**

ние за помощью к другому лицу → **Доступ через Интернет к своему компьютеру с помощью удаленного помощника Windows** (рис. 4.3).

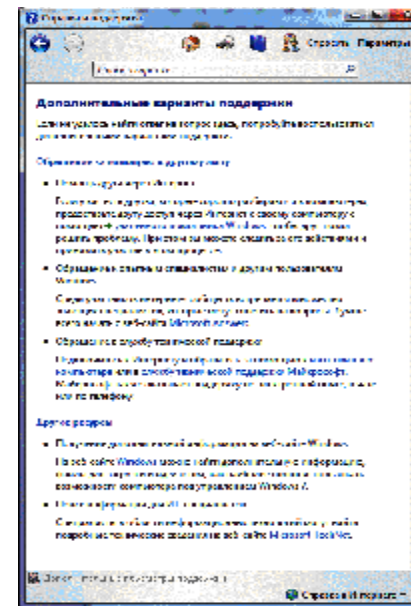


Рис. 4.3. Варианты поддержки

Далее выберите ссылку **Пригласить того, кому доверяете, для оказания помощи** (рис. 4.4).

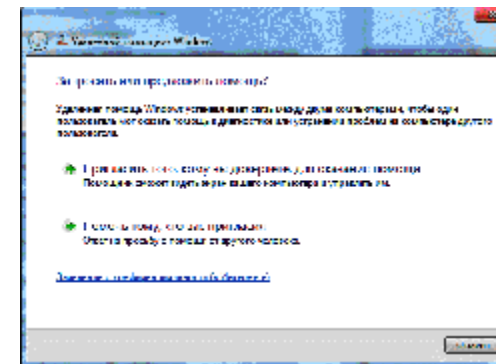


Рис. 4.4. Выбор помощника

Будет предложено использовать пересылку по электронной почте либо сохранить в файл. Приглашение – это обычный файл с IP-адресом того, кому нужна помощь (рис. 4.5).

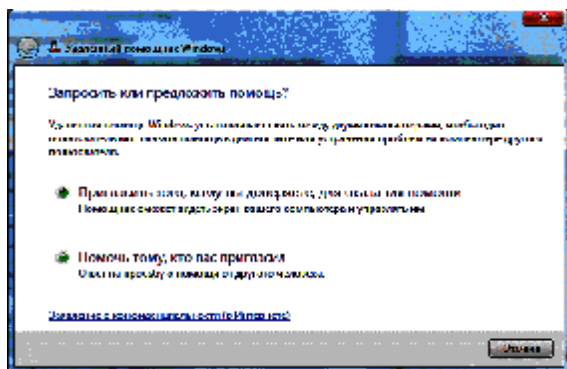


Рис. 4.5. Создание приглашения

Для простоты и надежности выберите ссылку **Сохранить приглашение в файл**. Далее вводим пароль (рис. 4.6).

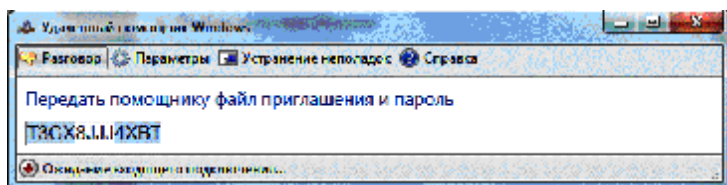


Рис. 4.6. Создание пароля

Нажмите кнопку **Сохранить приглашение**. Приглашение будет сохранено в виде файла с расширением **.msrcincident**. Все окна можно закрывать. А файл приглашения и пароль к нему надо передать любым способом тому, кто будет вам помогать.

После получения файла приглашения удаленный помощник человек, который будет вам помогать, должен запустить в **Проводнике** или любым другим доступным способом этот файл (рис. 4.7).

При необходимости помощник может не только наблюдать, но и тоже управлять компьютером. Для этого ему надо нажать кнопку **Взять управление**, после чего вам будет предложено разрешить ему управление.

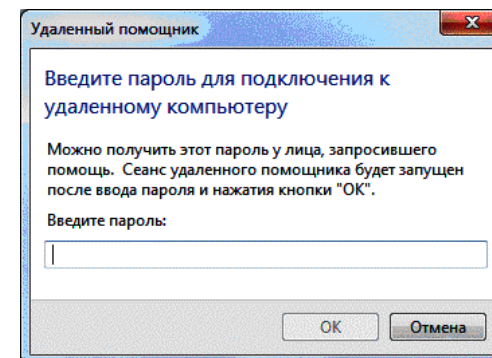


Рис. 4.7. Ввод пароля

После установления связи обменяйтесь несколькими сообщениями и сохраните копии экранных форм для помещения в отчет.

### 1.3. Использование удаленного рабочего стола

#### 1.3.1. Включение удаленного доступа на компьютере под управлением Windows 7

Прежде всего на компьютере, к которому будем подключаться (назовем его сервером), необходимо создать нового пользователя с обычным доступом и несложным паролем. Например, **Пользователь с паролем 1-2-3: Пуск → Панель управления → Учетные записи пользователей → Управление другой учетной записью → Создание учетной записи**.

Зайдите в свойства компьютера (или перейдите в **Панель управления → Система**) и выберите пункт **Дополнительные параметры системы** (рис. 4.8).

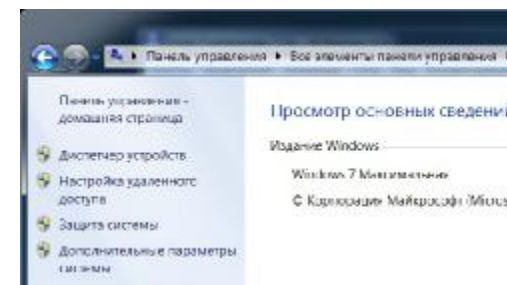


Рис. 4.8. Дополнительные параметры системы

В открывшемся окне выберите пункт **Удаленный доступ** (рис. 4.9).

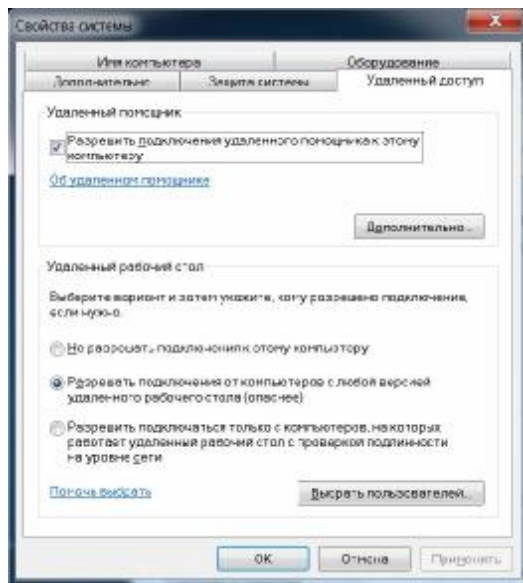


Рис. 4.9. Настройка терминального доступа к Windows 7

Поставьте галочку напротив пункта **Разрешить подключения удаленного помощника к этому компьютеру**. Это автоматически добавит исключение в брандмауэр Windows.

Выбрав **Дополнительно**, можно настроить разрешать или нет удаленное управление компьютером (по умолчанию **Разрешать**) и срок, в течение которого будет поддерживаться подключение сеанса (по умолчанию 6 часов).

Если удаленное управление компьютером запретить, то после подключения вы не сможете никаким образом управлять содержимым компьютера, а будете только видеть переданное вам изображение.

В разделе **Удаленный рабочий стол** выберите **Разрешать подключения от компьютеров с любой версией...**

Нажмите кнопку **Выбрать пользователей** и в открывшемся окне – кнопку **Дополнительно** и осуществите поиск зарегистрированных на компьютере пользователей (тип объекта **Пользователи**). Добавьте пользователей, которые будут иметь удаленный доступ к компьютеру (рис. 4.10–4.11).

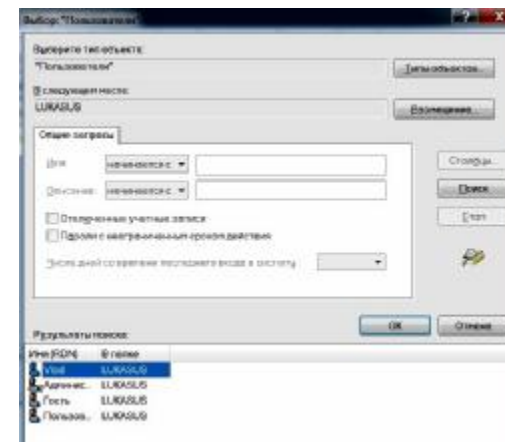


Рис. 4.10. Поиск пользователей на компьютере

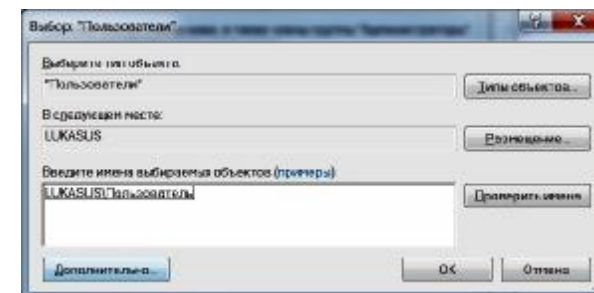


Рис. 4.11. Выбор пользователя

Обратите внимание, что пользователи с «пустыми» паролями запрещены при удаленном подключении независимо от установленных разрешений. Задайте такому пользователю пароль или создайте отдельного пользователя с паролем для этих целей. Нажмите **ОК** для завершения настроек.

### 1.3.2. Подключение к компьютеру с включенным удаленным доступом

Чтобы подключиться к такому компьютеру (серверу), необходимо знать IP-адрес компьютера или имя компьютера в сети.

Запустите на компьютере, с которого хотите получить удаленный доступ, программу **Подключение к удаленному рабочему столу** (**Пуск** → **Стандартные**).

В открывшемся окне (рис. 4.12) задайте адрес компьютера, к которому планируете подключение (IP-адрес или имя) и нажмите **Подключить** для проверки связи.

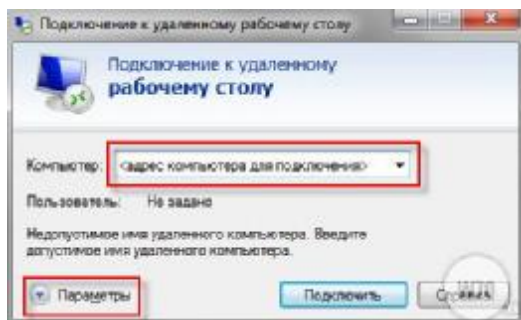


Рис. 4.12. Настройка подключения доступа к удаленному рабочему столу

Если все настройки сделаны правильно, то появится окно с предложением ввести логин и пароль для подключения к компьютеру.

Перед подключением можно настроить разнообразные параметры, нажав на соответствующую кнопку (рис. 4.12). В этом случае откроется панель настроек удаленного доступа (рис. 4.13).

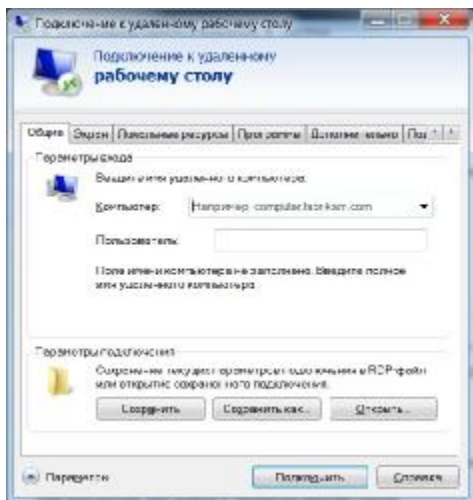


Рис. 4.13. Настройка параметров подключения

### Сведения о закладках

**Общие.** Здесь можно задать имя и адрес подключения, а также сохранить настройки в виде файла. В последнем случае вам не придется каждый раз запускать программу, достаточно будет запустить сохраненный файл со всеми настройками.

**Экран.** Задаются свойства экрана: разрешение (по умолчанию полный экран), количество цветов.

**Локальные ресурсы.** Здесь можно настроить передачу звука по сети (по умолчанию разрешено), использовать сочетания клавиш и самое интересное: есть доступ к локальным ресурсам компьютера, с которого происходит подключение. В последнем случае можно разрешить доступ к принтерам, дисководам и жестким дискам, которые будут доступны при работе на удаленном компьютере. Например, если разрешить доступ к диску C, то после установки соединения он появится на удаленном компьютере в списке устройств, и вы сможете обмениваться файлами с удаленным компьютером.

**Программы** служат для настройки автоматического запуска программ после подключения.

**Дополнительно.** Можно задать профили для подключений и вручную настроить визуальные эффекты, доступные после подключения.

**Подключение.** Можно изменить настройки оповещений и безопасности.

При подключении на экране клиента появится сообщение:

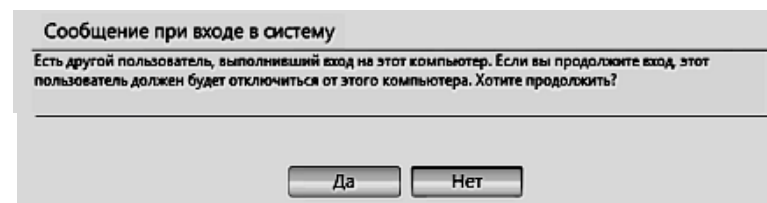


Рис. 4.14. Окно сообщения при входе в систему

Ответьте **Да**. После этого на сервере появится окно с предупреждением (рис. 4.15).

Согласитесь с отключением пользователя сервера и на экране клиента увидите удаленное окно сервера.

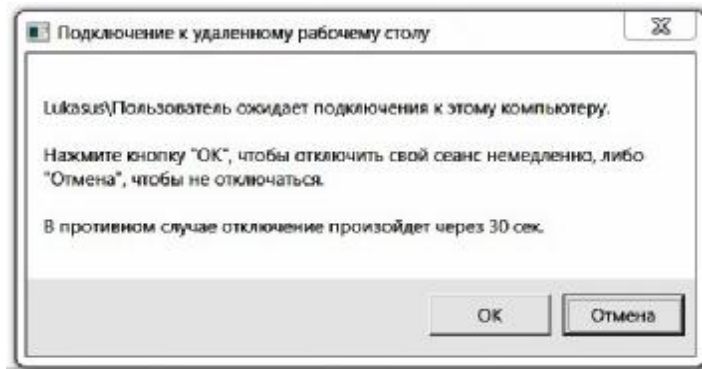


Рис. 4.15. Окно с предупреждением

### Содержание отчета

Отразите последовательность действий по настройке и использованию консоли управления MMC. Укажите, когда перезагружался компьютер, и приведите данные, подтверждающие это. Выделите время последней перезагрузки.

Приведите последовательность настройки **Удаленного помощника** и покажите экранные формы работы с соответствующими пояснениями.

### Контрольные вопросы

1. Пользовательский интерфейс MMC.
2. Как создать пользовательскую консоль?
3. Для чего нужна собственная консоль?
4. Какую пользу приносит использование программы **Удаленный помощник**?
5. Через какой порт осуществляется связь с **Удаленным помощником**?

## ЛАБОРАТОРНАЯ РАБОТА 5

### ИЗУЧЕНИЕ ПРОТОКОЛА УПРАВЛЕНИЯ СЕТЬЮ SNMP

**Цель работы:** ознакомление с системой мониторинга ОС MS Windows по протоколу Simple Network Management Protocol (SNMP).

### Задача лабораторной работы

Провести мониторинг ОС MS Windows по протоколу SNMP.

### Задание для самоподготовки

Встроенная помощь ОС MS Windows **Центр справки и поддержки** поиск по ключу **snmp**: %windir%\Help\snmpconcepts.chm

### Содержание работы

Протокол SNMP обеспечивает способ управления узлами сети (рабочие станции, серверы, маршрутизаторы, мосты и концентраторы) с центрального компьютера, на котором выполняется программное обеспечение управления сетью. SNMP выполняет функции службы управления с использованием распределенной архитектуры систем управления и агентов.

Поскольку управление сетью критично как для аудита, так и для управления ресурсами, SNMP может использоваться для реализации следующих задач:

- настройки удаленных устройств. Из системы управления можно отправить сведения о настройке на каждый узел сети;
- наблюдения за производительностью сети. Существует возможность отслеживать скорость обработки и передачи данных, а также собирать сведения об успешной передаче данных;
- определения сбоев сети или неправильного доступа. На сетевых устройствах можно настроить триггеры, срабатывающие при возникновении конкретных событий;
- аудита использования сети. Существует возможность наблюдения как за общим использованием сети для определения доступа пользователей или групп, так и за типами использования для сетевых устройств и служб.

### Схема лабораторной работы

Для выполнения лабораторной работы достаточно одного компьютера без подключения к какой-либо сети.

## 1. Порядок выполнения работы

Для выполнения работы установите на компьютере с помощью **Мастера компонентов Windows** службу SNMP:

- для Windows XP: **Панель управления** → **Установка и удаление программ** → **Установка компонентов Windows** →

**Средства управления и наблюдения** или в командной строке наберите **control.exe appwiz.cpl,@0,2;**

- для Windows 7: **Панель управления** → **Все элементы панели управления** → **Программы и компоненты** → **Включение или отключение компонентов Windows**.

Далее отметьте компоненты, устанавливаемые в ОС MS Windows (SNMP-протокол и WMI поставщик SNMP) и установите их.

Далее выполните следующие команды:

1) общий синтаксис команды:

**wmic service where (Name="snmp") get Caption,Name,Description,State /value**

2) проверка типа запуска службы. Опция **StartMode** должна быть **Auto** или **Manual**. Для команды **sc** соответственно – **AUTO\_START** или **DEMAND\_START**:

**wmic service snmp get StartMode /value**

3) извлечение параметров и получение информации о конфигурации установленной службы. Поместите результаты в отчет:

**sc qc snmp**

4) установка типа запуска службы – вручную:

**sc config snmp start= demand**

5) запуск сервиса, если он не запущен:

**sc start snmp**

6) проверка запущенных snmp-процессов:

**tasklist /svc**

7) если эта политика отключена или не задана, служба SNMP принимает допустимые сообщества, сконфигурированные на локальном компьютере. Для локального компьютера необходимо указать состояние политик: **Не задано**

**start gpedit.msc**

Далее: **Групповая политика** → **Административные шаблоны** → **Сеть** → **SNMP**

8) появление ветви в реестре при добавлении сообщества. Если политика SNMP не задана, данный раздел отсутствует в реестре. Поместите результаты в отчет:

**reg query HKLM\SOFTWARE\Policies\SNMP\Parameters /s**

9) запуск **Сведения о системе**, сделать поиск по ключу snmp. Просмотр упоминаний, связанных с SNMP:

**C:\Program Files\Common Files\MicrosoftShared\MSInfo\MS-Info32.exe**

10) запуск любого демона для захвата ловушек (трапов). В лабораторной работе используется часть приложений программного продукта **ucd-snmp (snmpwalk.exe и libsnmp.dll)**:

**mkdir c:\temp\snmp**

**cd c:\temp\snmp**

Скопируйте в эту папку файл **snmpwalk.exe** и библиотеку:

**libsnmp.dll**

**dir /b**

11) проверка работы службы SNMP:

**snmpwalk.exe -Pev 1 -c public 127.0.0.1**

Поместите результат в отчет.

12) установка SNMP параметров:

**services.msc**

**Служба SNMP** → **Свойства**:

а) вкладка **Агент SNMP**

**Контактное лицо**: **Заполнить** Фамилия студента (латиницей)

**Размещение**: **Заполнить** (латиницей)

**Службы**: **Отметить все**.

б) вкладка **Безопасность** → **Приемлемые имена сообщества** → **Изменить**

Изменить имя сообщества **public** на имя **labuser**.

13) перезапуск службы:

**net stop snmp && net start snmp**

**sc query snmp**

**snmpwalk.exe -Pev 1 -c labuser 127.0.0.1**

**mkdir c:\temp\snmp\mib**

Поместите результаты в отчет.

Скопируйте в эту директорию файлы **RFC1155-SMI.MIB** и **RFC1213-MIB-II.MIB**

**cd c:\temp\snmp**

**dir /S/B**

**snmpwalk.exe -Pe -M ./mib -v1 -c labuser 127.0.0.1 system**

Поместите результаты в отчет.

14) просмотр переменных дерева RFC1213.MIB с помощью протокола SNMP:

**type mib\RFC1213-MIB-II.MIB | find /i "OBJECT-TYPE" | more**

15) просмотр ветви дерева MIB, какую поддерживает данное устройство. В нашем случае данный компьютер 127.0.0.1.

**snmpwalk.exe -Pe -M ./mib -v1 -c labuser 127.0.0.1 sysObjectID**

16) опрос базы MIB компьютера (может быть любое устройство), при этом определится, какие ветви MIB использует данное устройство:

**snmpwalk.exe -Pe -M ./mib -v1 -c labuser 127.0.0.1 | more**

### Содержание отчета

Данные, полученные по SNMP-протоколу.

### Контрольные вопросы

1. Протокол SNMP и его возможности.
2. Для чего нужно настраивать агент SNMP на маршрутизаторе?
3. Что используется как пароль доступа между агентом SNMP на маршрутизаторе и диспетчером SNMP?
4. Что необходимо настроить на агенте SNMP для усиления защиты доступа?

## ЛАБОРАТОРНАЯ РАБОТА 6

### ИЗУЧЕНИЕ НАСТРОЕК ETHERNET И АНАЛИЗ ТРАФИКА

**Цель работы:** ознакомление с настройками сетевой платы и встроенными инструментальными средствами ОС MS Windows анализа трафика на сетевых интерфейсах.

### Задача лабораторной работы

Правильная настройка сетевой платы позволяет не только обеспечить соединение с сетью, улучшить производительность сетевого подключения, но и получить необходимое качество сервиса предоставляемого локальной сетью.

Для просмотра состояния взаимодействия компьютера с локальной сетью различные разработчики ОС предоставляют средства диагностики, которые могут быть графическими или использовать командную строку (так называемый интерфейс Command line interface (CLI)). Диагностика с помощью CLI позволяет создавать скрипты или программы для включения их в приложения, занимающиеся мониторингом или анализом сети в целом.

В данной работе вводятся следующие понятия:

**Скрипт (script)** – небольшая программа для выполнения средствами ОС и для расширения ее возможностей;

**Loopback** (обратная, возвратная петля) – тип диагностического интерфейса, при котором сигнал возвращается передающему устройству, пройдя по коммуникационному каналу в обоих направлениях;

**GUI** (Graphical User Interface) – графический пользовательский интерфейс;

**CLI** (Command Line Interface) – интерфейс командной строки, в котором инструкции компьютеру даются только путем ввода с клавиатуры текстовых строк (команд), также известен под названием консоль;

**MMC** (Microsoft Management Console) – средство для создания, сохранения и открытия средств администрирования (называемых консолями MMC), которые управляют оборудованием, программными и сетевыми компонентами ОС Windows.

### Задание для самоподготовки

Рекомендуется ознакомиться с материалами:

- встроенной помощью ОС MS Windows: **Центр справки и поддержки: Подключение по локальной сети turereperf;**

- выводом справочных сведений о командах. Встроенная помощь к программам ОС MS Windows реализуется при помощи команды: **HELP [команда], конструкции [команда] /?**

### Схема лабораторной работы

Для выполнения лабораторной работы достаточно одного компьютера с подключением к какой-либо сети.

### Содержание работы

1. Провести анализ трафика сетевых интерфейсов.
2. Составить отчет.

## 1. Порядок выполнения работы

### 1.1. Описание свойств сетевой платы

Выполните в следующей последовательности доступ к настройкам сетевой платы: **explorer.exe** (можно по горячим клавишам **Win + E**) → **Сетевое окружение (Alt + Enter)** → **Подключение по локальной сети (Alt + Enter)** → **Подключение через:** (укажите сетевую плату) → **Настроить** → **Дополнительно.**



Сохраните в отчете все свойства сетевого интерфейса в виде табл. 6.1.

Т а б л и ц а 6.1

Название сетевой платы		
Свойство	Установленное значение	Возможные значения
Wake Up Capabilities	Magic packet	Wake Up Frame, Both, None,

## 1.2. Настройка MMC консоли ОС MS Windows для анализа трафика сетевого интерфейса

Запустите MMC-консоль **Производительность**. Для этого выполните следующие действия: **Win + E** → **Панель\_управления** → **Администрирование** → **Производительность** (или из командной строки набрать `%SystemRoot%\system32\perfmon.msc`).

Установите новый набор счетчиков: **Ctrl + E**. Далее добавьте счетчики: **Объект: Сетевой интерфейс**.

Выберите: вхождения из списка: **MS TCP Loopback interface**; счетчики из списка: **Отправлено байт/сек, Получено байт/сек**. В свойствах графика укажите диапазон вертикальной шкалы = 5.

В другом окне командного процессора наберите команду:  
**ping -l 10000 127.0.0.1 -t**

В течение приблизительно одной минуты снимите статистику. Данные в отчет не сохраняйте.

## 1.3. Настройка CLI ОС MS Windows для анализа трафика сетевого интерфейса

Просмотрите все доступные счетчики производительности ОС MS Windows и сохраните их в файл **list\_perf.txt**

**typeperf -qx > list\_perf.txt**

В одном окне наберите команду (или скопируйте из файла **list\_perf.txt** указанный счетчик производительности):

**typeperf** → **Сетевой интерфейс (MS TCP Loopback interface)** / **Получено байт/сек** → **Сетевой интерфейс (MS TCP Loopback interface)** / **Отправлено байт/сек**.

В другом окне командного процессора наберите команду:  
**ping -l 65500 127.0.0.1 -t**

В течение приблизительно одной минуты снимите статистику. Данные в отчет не сохраняйте.

## 1.4. Определение размера ICMP-пакетов

Подберите такое значение длины пакетов, чтобы не было сообщений об ошибках пакетов.

В текстовом редакторе создайте командный файл **proba.bat** следующего содержания:

```
@echo off
for /L %%i in (1000#,100#,1000000#) do (for /F "usebackq delims=< tokens=2" %%a IN (^ping -l %%i 127.0.0.1 -n 1`) DO @echo Размер буфера отправки=%%i....Время отклика=%%a)
```

В отчете дайте объяснение остановки команды **ping** и укажите, при каких параметрах произошла остановка.

Подберите такое значение длины пакетов, чтобы не было сообщений об ошибках при фрагментации пакетов.

В текстовом редакторе создайте командный файл **proba\_2.bat** следующего содержания:

```
@echo off
for /L %%i in (1000#,1#,10000#) do (for /F "skip=2 usebackq delims=< tokens=2" %%a IN (^ping -f -l %%i 127.0.0.1 -n 1`) DO @echo Размер буфера отправки=%%i.....Время отклика=%%a)
```

В отчете дайте объяснение остановки команды **ping** и укажите, при каких параметрах произошла остановка.

## 1.5. Просмотр статистики Ethernet-интерфейса и протоколов IP-стека

Просмотрите MAC-адрес Ethernet-интерфейса и поместите в отчет.

**getmac**

С помощью утилит соберите статистику Ethernet-интерфейса и протоколов IP-стека.

**netstat**

Ознакомьтесь с командами:

```
netstat -e
netstat -s -p ICMP 1
netstat -s -p UDP 1
netstat -s -p TCP 1
netstat -s -p IP 1
```

В течение приблизительно одной минуты снимите статистику. Внимательно рассмотрите статистику, особенно обратите внимание на количество ошибок. В отчете опишите имеющуюся статистику.

#### **Содержание отчета**

1. Запишите полученные результаты.
2. Опишите характеристики сетевой платы.
3. Проанализируйте параметры сетевой платы.
4. Сделайте анализ трафика сетевого интерфейса.
5. Сравните полученные результаты и сделайте выводы.

#### **Контрольные вопросы**

1. Опишите характеристики сетевой платы.
2. Расскажите о способах диагностики сетевых подключений в ОС MS Windows.
3. Использование CLI для анализа трафика сетевого интерфейса.

## **ЛАБОРАТОРНАЯ РАБОТА 7 ИЗУЧЕНИЕ TELNET-СОЕДИНЕНИЙ**

**Цель работы:** ознакомление со средствами терминального соединения ОС MS Windows, приобретение навыков настройки доступа по сети к другим компьютерам, используя telnet – стандартный протокол стека TCP/IP.

#### **Задача лабораторной работы**

Служба ОС MS Windows tlntsrv (telnet) позволяет удаленному пользователю входить в систему и запускать программы, поддерживает различных клиентов TCP/IP telnet, включая компьютеры с ОС UNIX и Windows. С помощью клиента telnet пользователи Windows могут подключаться к удаленному компьютеру, на котором запущен сервер telnet, и запускать приложения или выполнять административные задачи на этом компьютере.

#### **Задание для самоподготовки**

Рекомендуется ознакомиться с материалами:

- встроенной помощью ОС MS Windows **Центр справки и поддержки: Использование клиента telnet, Команды telnet, Общие сведения о сервере telnet, Доступ к серверу telnet, Сервер telnet;**

- встроенной помощью ОС MS Windows:  
**C:\WINDOWS\Help\telnet.hlp; C:\WINDOWS\Help\telnet.chm.**

#### **Схема лабораторной работы**

Для выполнения лабораторной работы достаточно одного компьютера с настроенным подключением к какой-либо сети.

#### **Содержание работы**

1. Собрать схему лабораторных работ.
2. Установить telnet-соединение со своим компьютером или с другим компьютером.
3. Составить отчет.

### **1. Порядок выполнения работы**

**Внимание!** Microsoft в Windows 7 убрала запуск клиента telnet по умолчанию из ОС, аргументируя это соображениями безопасности. Чтобы вернуть стандартного клиента в нашу систему, выберите **Панель управления → Программы → Включение и отключение компонентов Windows**. В появившемся списке найдите **Клиент telnet** и **Сервер telnet** и пометьте их галочкой, нажмите **ОК**. Далее необходимо запустить эти службы: выберите **Панель управления → Администрирование** и откройте окно **Службы**. На вкладке **Стандартные** для службы telnet установите **Свойства → Тип запуска → Вручную**. Далее запустите вручную службу telnet.

Протокол telnet обеспечивает передачу потока байтов между процессами, а также между процессом и терминалом. Наиболее часто этот протокол используется для эмуляции терминала удаленной ЭВМ.

#### **1.1. Определение учетной записи на компьютере для разрешения работы сервера службы telnet**

Просмотрите учетные записи пользователей вашего компьютера:

**net user**

Добавьте пользователя test с паролем test:

```
net user test test /add
```

Задайте сервису автозагрузку:

```
sc config tlntsvr start= auto
```

Далее выполните задание по вариантам.

**Вариант 1.** С помощью командной строки создайте группу пользователей службы telnet:

```
net localgroup TelnetClients /add
```

Просмотрите пользователей службы telnet:

```
net localgroup TelnetClients
```

Добавьте пользователя test в группу службы telnet:

```
net localgroup TelnetClients test /add
```

**Вариант 2.** С помощью графического интерфейса выполните: **Панель управления** → **Администрирование** → **Управление компьютером** → **Локальные пользователи** → **Пользователи**.

Создайте группу: **Имя группы** → **TelnetClients**

## 1.2. Проверка состояние telnet-службы

С помощью командной строки проверьте настройки службы telnet:

```
sc query tlntsvr
```

```
sc stop tlntsvr
```

```
sc query tlntsvr
```

```
sc start tlntsvr
```

Сохраните в отчет состояние службы:

```
type %SystemRoot%\system32\login.cmd
```

Службу telnet можно также настроить с помощью графического интерфейса: **Панель управления** → **Администрирование** → **Службы** → **telnet**.

Установите ручной запуск службы.

## 1.3. Установление telnet-соединения

Откройте *два окна* командного процессора:

**Пуск** → **Выполнить** → **cmd**.

В *одном* окне установить telnet-соединение:

```
telnet 127.0.0.1
```

Выполните любую команду, например, **dir**.

В *другом окне* командного процессора проверьте telnet-сессии, установленные с компьютером, и сохраните в отчет состояние подключения telnet-клиента:

```
tlntadmn -s
```

В окне telnet-сессии выполните команду:

```
shutdown -r -t 0
```

## Содержание отчета

Запишите полученные результаты.

## Контрольные вопросы

1. Расскажите о стандартных стеках коммутационных протоколов.

2. Расскажите об уровне приложения стека TCP/IP.

3. Объясните понятие socket (сокет).

## ЛАБОРАТОРНАЯ РАБОТА 8

### ИЗУЧЕНИЕ TFTP-СОЕДИНЕНИЙ

**Цель работы:** ознакомление с возможностью передачи файлов по протоколу Trivial File Transfer Protocol (TFTP).

## Задача лабораторной работы

В стеке TCP/IP протокол FTP предлагает наиболее широкий набор услуг для работы с файлами, однако он является и самым сложным для программирования. Приложения, которым не требуются все возможности FTP, могут использовать другой, более экономичный протокол – простейший протокол пересылки файлов TFTP. Этот протокол реализует только передачу файлов, причем в качестве транспорта используется более простой, чем TCP, протокол без установления соединения – UDP.

В силу своей простоты протокол TFTP используется не только для передачи файлов, но и для загрузки X-терминалов при использовании протоколов RARP, TFTP и BOOTP.

Администраторам сети часто приходится сохранять файлы конфигурации, системное программное обеспечение (IOS) или восстанавливать их на коммуникационное оборудование. Возможны два способа копирования образа IOS во флэш-память:

через консоль по протоколу Xmodem или через порт Ethernet по протоколу TFTP. Первый способ характеризуется огромным временем выполнения операции (часы). Второй способ предполагает наличие TFTP-сервера.

Встроенная поддержка TCP/IP MS Windows позволяет использовать протокол TFTP в цифровых сетях для передачи файлов между устройствами.

### Схема лабораторной работы

Для выполнения работы необходимы два компьютера, программа **tftpd.exe** и «исходник» следующего пакетного файла **make\_10M.txt**. (прил. 1).

Установите tftp-соединение со своим или с другим компьютером.

### Задание для самоподготовки

Рекомендуется ознакомиться с материалами:

- встроенной помощью ОС MS Windows: **Центр справки и поддержки: поиск по ключу tftp**;

- встроенной помощью к программам ОС MS Windows при помощи команды: **tftp /?**

### Содержание работы

1. Собрать схему лабораторных работ.
2. Установить tftp-сервер.
3. Передать и принять файлы на loopback и соседний компьютер.
4. Составить отчет.

## 1. Порядок выполнения работы

### 1.1. Сохранение на TFTP-сервере рабочей конфигурации маршрутизации компьютера

Запустите командный процессор: **Пуск → Выполнить → cmd**.

Создайте рабочие каталоги:

```
mkdir d:\[номер_группы]\temp\down
mkdir d:\[номер_группы]\temp\up
cd d:\[номер_группы]\temp\up
```

В папке **d:\[номер\_группы]\temp\up** создайте файл конфигурации таблицы маршрутизации **up.cnf**  
**netstat -rn > d:\[номер\_группы]\temp\up\up.cnf**  
**type d:\[номер\_группы]\temp\up\up.cnf**

В папке **d:\[номер\_группы]\temp\down** создайте файл текущих параметров сети TCP/IP **down.cnf**  
**ipconfig /all > d:\[номер\_группы]\temp\down\down.cnf**  
**type d:\[номер\_группы]\temp\down\down.cnf**

Запустите демон **tftpd** – программа для передачи файлов по протоколу TFTP.

В окне программы TFTPД установите корневую папку:

```
d:\[номер_группы]\temp\down
```

Для передачи файлов между компьютерами выполните следующие команды, где в качестве IP-адреса может использоваться **127.0.0.1** или адрес соседнего компьютера:

```
dir /c/d d:\[номер_группы]\temp\up
d:\[номер_группы]\temp\down
cd d:\[номер_группы]\temp\up
tftp 127.0.0.1 put up.cnf
dir /c/d d:\[номер_группы]\temp\up
d:\[номер_группы]\temp\down
```

Получите файл со своего компьютера. Результат запишите в отчет.

Отправьте файл на свой компьютер:

```
tftp 127.0.0.1 get down.cnf
```

Результат запишите в отчет.

Отправьте и получите файлы с соседнего компьютера:

```
tftp X.X.X.X put up.cnf
```

```
tftp X.X.X.X get down.cnf
```

Результат запишите в отчет.

### 1.2. Сохранение бинарного файла на TFTP-сервере

В этом режиме файл передается в неизменном виде по байтам.

Создайте с помощью пакетного файла текстовый файл размером 10 Мб. Командный файл имеется на диске, а его код приведен в прил. 1. Для создания тестового файла:

- скопируйте программу **make\_10M.txt** в папку:

```
d:\[номер_группы]\temp\up\;
```

- переименуйте **make\_10M.txt** в **make\_10M.bat**;

- запустите **make\_10M.bat**.

В результате этого в папке **d:\[номер\_группы]\temp\up\** должен создаваться файл **test\_10.Mb** (10000001 байт).

Выполните в папке **d:\[номер\_группы]\temp\up\** передачу бинарного файла на **loopback** и на другой компьютер:

```
tftp -i 127.0.0.1 put test_10.Mb
```

```
tftp -i X.X.X.X put test_10.Mb
```

```
tftp -i 127.0.0.1 get test_10.Mb
```

```
tftp -i X.X.X.X get test_10.Mb
```

Результаты запишите в отчет.

В другом окне командного процессора просмотрите результаты подключений по TFTP-протоколу. Данные запишите в отчет.

```
netstat -an 1 | find "69"
```

```
netstat -a 1 | find "tftp"
```

### Содержание отчета

Запишите полученные результаты передачи файлов на Loopback и на другой компьютер. Проведите анализ скорости передачи и качества, опишите возникшие ошибки передачи.

### Контрольные вопросы

1. Зачем нужен протокол TFTP?
2. Какую функцию реализует протокол TFTP?
3. Назначение пакета, если код операции в заголовке TFTP равен 1, 2, 3 или 4?

## Приложение 1

### Создание бинарного файла

```
rem --< ##### -< пакетный файл make_10M.bat >- #####
rem --< Программа создания файла test_10.Mb размером 10Mb.
rem --< #####
del *.*
echo 12345678901234567890123 > 1_
copy * _2_ & copy * _3_ & copy * _4_ & copy * _5_ & copy * _6_ &
copy * _7_
copy * _8_ & copy * _9_ & copy * _10_ & copy * _11_ & copy * _12_
& copy * _13_
copy * _14_ & copy * _15_ & copy * _16_ & copy * _17_ & copy * _
18_ & copy * _19_ & copy * _20_
copy 20_+19_+14_+13_+11_+9_ test_10.Mb
del *.*
```

## ЛАБОРАТОРНАЯ РАБОТА 9

### ИЗУЧЕНИЕ ВСТРОЕННЫХ СРЕДСТВ ДИАГНОСТИКИ WMIС

**Цель работы:** изучение возможностей встроенных средств управления рабочей станцией с использованием подсистемы Windows Management Instrumentation (WMI).

### Задача лабораторной работы

Просмотреть базовые настройки персонального компьютера. Проанализировать сетевые настройки компьютера, представленные в html-формате. Сохранить сетевые настройки, используя встроенную программу архивирования **makecab**. Извлечь файл конфигурации из сжатого файла.

### Задание для самоподготовки

Рекомендуется ознакомиться с материалами:

- встроенной помощью ОС MS Windows **Центр справки и поддержки**: поиск по ключу **wmic**, **makecab**, **expand**.

- встроенной помощью к программам ОС MS Windows, команда **wmic /?**

### Содержание работы

Программа WMIС (WMI Command-line) предоставляет простой интерфейс командной строки для работы с подсистемой WMI (инструментарий управления Windows). Это позволяет воспользоваться преимуществами WMI для управления компьютерами с ОС Microsoft Windows. WMIС взаимодействует с существующими оболочками и служебными программами, а также может быть легко расширена с помощью сценариев или других административных приложений.

WMIС позволяет выполнять следующие задачи:

- просматривать схемы WMI и запрашивать их классы и экземпляры (обычно с использованием псевдонимов, упрощающих работу с WMI);

- работать с локальным компьютером, удаленными компьютерами или выполнять команды сразу для нескольких компьютеров;

- настраивать псевдонимы и форматы вывода в соответствии с имеющимися потребностями;

- создавать и выполнять сценарии на основе WMIС.

Поставщики WMI позволяют управлять различными аппаратными компонентами, подсистемами ОС и прикладными системами. WMIC можно использовать со всеми схемами, внедряемыми поставщиками WMI, с любого компьютера, на котором включена WMIC, для удаленного управления любым компьютером с WMI. При этом наличие WMIC на удаленно управляемом компьютере необязательно.

В следующих типичных сценариях WMIC позволяет упростить выполнение задач:

- локальное управление компьютером – оператор находится на компьютере и использует WMIC для управления им;

- удаленное управление компьютером – оператор находится на одном компьютере и использует WMIC для управления другим компьютером;

- удаленное управление несколькими компьютерами – оператор находится на одном компьютере и использует WMIC для управления несколькими компьютерами общей командой;

- удаленное управление компьютером (с использованием удаленного сеанса) – оператор использует технологию сеансов удаленного доступа (такую как telnet или службы терминалов) для подключения к удаленному компьютеру и управления им при помощи WMIC;

- автоматизированное управление с использованием сценариев администрирования – оператор использует WMIC для написания простого сценария, автоматизирующего управление компьютером (локальным, удаленным или несколькими компьютерами – поочередно или одновременно).

### Схема лабораторной работы

Для выполнения лабораторной работы достаточно одного компьютера без подключения к какой-либо сети.

## 1. Порядок выполнения работы

### 1.1. Просмотр параметров компьютера, используя командную строку и программу wmic

Ознакомьтесь с командами WMIC:

```
wmic /?
```

Управление системной платой:

```
wmic BASEBOARD get /value | more
```

Управление базовой системой ввода-вывода (BIOS):

```
wmic BIOS get /value | more
```

Управление конфигурацией загрузки:

```
wmic BOOTCONFIG get /value | more
```

Управление компьютером:

```
wmic COMPUTERSYSTEM get /value | more
```

Управление центральным процессором:

```
wmic CPU get /value | more
```

Сохраните непустые данные в отчет.

### 1.2. Просмотр параметров сетевого подключения компьютера в html-формате

Выполните следующие команды:

```
wmic /RECORD:nic.htm nic get /value /format:mof & Start nic.htm
```

```
wmic /RECORD:nicconfig.htm nicconfig get /value /format:mof & Start nicconfig.htm
```

```
wmic /RECORD:Protocol.htm netprotocol get /value /format:mof & Start Protocol.htm
```

```
wmic /RECORD:netuse.htm netuse get /value /format:mof & Start netuse.htm
```

```
wmic /RECORD:Protocol.htm netprotocol get Description,ConnectionlessService /format:mof & Start Protocol.htm
```

```
wmic /RECORD:address.htm nicconfig get Description,IPAddress,DefaultIPGateway,MACAddress /format:mof & Start address.htm
```

```
wmic /RECORD:nic.htm nic get Description,AdapterType,Manufacturer,NetConnectionID,SystemName /format:mof & Start nic.htm
```

### 1.3. Подготовка файла с параметрами сетевой платы для отправки Администратору сети

Определите параметры сетевой платы:

```
wmic PATH
```

```
"Win32_Environment.Name='PROCESSOR_IDENTIFIER'"
```

```
GET VariableValue > Ethernet.htm
```

```
wmic nic where (NetConnectionID ="Подключение по локальной сети") get /format:mof >> Ethernet.htm
```

Определите индекс сетевой платы:

```
wmic nic where (AdapterType ="Ethernet 802.3") get Index,NetConnectionID
```

В следующей строке замените XX на реальное значение и выполните такую командную строку:

```
wmic nicconfig where ( Index= XX ) get /format:mof >> Ethernet.htm & start Ethernet.htm
```

#### 1.4. Архивация полученных данных средствами ОС MS Windows

Выполните следующие команды:

```
makecab Ethernet.htm wmi_log.cab  
expand -r wmi_log.cab
```

Процедуру сбора данных и архивирования можно выполнить, используя скрипт **log\_wmic.bat** (прил. 2).

Файл **Ethernet.htm** поместите в отчет.

#### Содержание отчета

Проведите анализ сетевых настроек и поместите результаты в отчет.

#### Контрольные вопросы

1. WMIC: возможности получения информации и управления настройками компьютера.

2. Как при помощи утилиты WMIC:

- получить имя компьютера в сети;
- узнать серийный номер компьютера?

#### Приложение 2

#### Скрипт log\_wmic.bat

```
rem Определить индекс сетевой платы:  
rem wmic nic where (AdapterType ="Ethernet 802.3") get Index,NetConnectionID  
rem Ввести Index=XX и NetConnectionID  
wmic PATH  
"Win32_Environment.Name='PROCESSOR_IDENTIFIER'" GET VariableValue > Ethernet.htm  
wmic nic where (NetConnectionID ="Подключение по локальной сети") get /format:mof >> Ethernet.htm  
wmic nicconfig where (Index=XX) get /format:mof >> Ethernet.htm  
makecab Ethernet.htm wmi_log.cab
```

## ЛАБОРАТОРНАЯ РАБОТА 10 ИСПОЛЬЗОВАНИЕ КОМАНДЫ NETSH

*Цель работы:* ознакомление с системой команд netsh и исследование сетевых параметров локального компьютера.

#### Задача лабораторной работы

С помощью команд netsh для интерфейса IP отобразить сведения о конфигурации и данных статистики настройки протокола TCP/IP (адресов, основных шлюзов, служб DNS и серверов WINS).

Используя команды сетевой диагностики netsh, рассмотреть наличие неполадок ОС и параметров сети на локальном компьютере.

#### Задание для самоподготовки

Ознакомиться с материалами встроенной помощи ОС MS Windows **Центра справки и поддержки** (клавиша **F1** на основном экране), используя поиск по ключевым словам **netsh**, **mstsc**).

#### Содержание работы

Система команд netsh представляет собой поддерживающую сценарий программу с командной строкой, позволяющую локально или удаленно отображать и изменять параметры сети текущего компьютера, а также обеспечивает средства написания сценариев для запуска группы команд в пакетном режиме на определенном компьютере. Программа netsh может равным образом сохранять сценарии конфигурации в текстовом файле для помещения в архив или для настройки других серверов.

Система команд netsh взаимодействует с другими компонентами ОС с помощью файлов библиотеки динамической компоновки (DLL). Команда **netsh show helper** перечисляет все модули поддержки верхнего уровня. Каждая библиотека модуля поддержки netsh содержит широкий набор средств, или контекст, представляющий собой группу команд, относящуюся к конкретному сетевому компоненту. Эти контексты расширяют возможности netsh, обеспечивая поддержку настройки и наблюдения за одной или несколькими службами, служебными программами или протоколами. Например, файл Dhcpmon.dll обеспечивает для netsh контекст и набор команд, необходимых для настройки и управления серверами DHCP. Команды netsh для

интерфейса IP используются для настройки протокола TCP/IP (адресов, основных шлюзов, служб DNS и серверов WINS), а также для отображения сведений о конфигурации и данных статистики. Для запуска этих команд netsh на удаленном сервере под управлением Windows 2000 Server необходимо подключиться к серверу, на котором запущен *сервер терминалов*, с помощью программы **Подключение к удаленному рабочему столу (mstsc.exe)**.

Команда **Mstsc** обеспечивает создание подключений к серверам терминалов или другим удаленным компьютерам, редактирование существующего файла конфигурации подключения к удаленному рабочему столу (.rdp) и перенос подключений Windows XP (подключения, созданные с помощью диспетчера клиентских подключений) в новые файлы .rdp.

Администрирование серверов маршрутизации из командной строки происходит быстрее, чем при использовании консоли. Эта возможность особенно важна в сетевых соединениях с низкой скоростью передачи данных, например, подключение по глобальной сети (WAN).

Объединяя команды в сценарий, который выполняется на нескольких серверах, можно администрировать серверы маршрутизации согласованно.

Функции команд netsh для Windows XP и Windows 7 могут различаться.

### **Схема лабораторной работы**

Для выполнения лабораторной работы достаточно одного компьютера без подключения к какой-либо сети.

## **1. Порядок выполнения работы**

### **Внимание!**

Запустите netsh из командной строки интерпретатора **Cmd.exe** и перейдите к контексту, который содержит нужную команду. Доступность контекстов зависит от того, какие сетевые компоненты были установлены. Например, при вводе **dhcp** в командной строке netsh происходит переход в контекст DHCP, но если не был установлен компонент DHCP, появляется следующее сообщение: **Команда не найдена: dhcp**.

При работе под управлением Windows 7 интерпретатор командной строки должен быть запущен от имени администратора. Для этого в строке поиска введите CMD, в появившемся списке команд щелкните правой клавишей мыши по соответствующей команде и выберите **Запуск от имени администратора** либо нажмите сочетание клавиш **Ctrl + Shift + Enter**.

### **1.1. Подготовка к тестированию (для Windows XP и Windows 7)**

Отправьте пользователю, работающему в данный момент на компьютере, сообщение:

```
msg "пользователь" НА ВАШЕМ КОМПЬЮТЕРЕ ПРОИЗВОДИТСЯ ДИАГНОСТИКА ПАРАМЕТРОВ – Администратор сети
```

Формат команды:

```
msg {имя_пользователя|имя_сеанса| код_сеанса|@имя_файла|*} [/server:имя_сервера] [/time:секунды] [/v] [/w] [сообщение] – позволяет отправлять сообщения на другой компьютер.
```

### **1.2. Изучение параметров настройки сети (для Windows XP и Windows 7)**

Рассмотрите контексты команд и сохраните ключевые моменты настройки сценария конфигурации сети в отчет, выполнив следующие команды:

```
netsh interface
```

```
netsh dump | more
```

Изучите следующие параметры интерфейсов:

```
netsh interface show interface /?
```

```
netsh interface show interface
```

```
netsh interface show interface внутренний
```

```
netsh interface show interface подключение
```

Изучите следующие параметры IP-настроек:

```
netsh interface ip show address – отображение конфигурации IP-адресов;
```

```
netsh interface ip show config – отображение IP-адреса и дополнительных сведений;
```

```
netsh interface ip show dns – отображение адресов DNS-сервера;
```



**netsh interface ip show interface** – отображение статистики IP-интерфейса;

**netsh interface ip show ipaddress** – отображение IP-адресов текущих;

**netsh interface ip show ipnet** – отображение сопоставления сетей IP и физических носителей;

**netsh interface ip show ipstats** – отображение статистики IP;

**netsh interface ip show joins** – отображение присоединенных многоадресных групп;

**netsh interface ip show offload** – отображение информации разгрузки;

**netsh interface ip show tcpconn** – отображение TCP-подключений;

**netsh interface ip show tcpstats** – отображение статистики TCP;

**netsh interface ip show udpconn** – отображение UDP-подключений;

**netsh interface ip show udpstats** – отображение статистики UDP;

**netsh interface ip show wins** – отображение адресов WINS-сервера.

### 1.3. Диагностика сети (для Windows XP)

Проанализируйте информацию об оборудовании, программном обеспечении и сетевых подключениях. Изучите следующие команды:

**netsh diag ping adapter** – проверка связи со всеми адаптерами;

**netsh diag ping dhcp** – проверка связи с DHCP-серверами для каждого адаптера;

**netsh diag ping dns** – проверка связи с DNS-сервером для каждого адаптера;

**netsh diag ping gateway** – проверка связи со шлюзами по умолчанию для каждого адаптера;

**netsh diag ping ieproxy** – проверка связи с прокси для Internet Explorer;

**netsh diag ping ip** – проверка связи со всеми IP-адресами для каждого адаптера;

**netsh diag ping iphost** – проверка связи с узлом по указанному IP-адресу или имени;

**netsh diag ping loopback** – проверка связи при замыкании на себя (127.0.0.1);

**netsh diag ping mail** – проверка связи с почтовым сервером для Outlook Express;

**netsh diag ping news** – проверка связи с сервером службы новостей;

**netsh diag ping wins** – проверка связи с основным и вспомогательным WINS-серверами для каждого адаптера.

### 1.4. Диагностика служб и настроек (для Windows XP)

Проанализируйте сведения о службе новостей, почтовой службе, компьютере, ОС, сетевом адаптере, модеме и клиенте сети. Изучите следующие команды:

**netsh diag show adapter** – отображение сведений обо всех адаптерах;

**netsh diag show all** – отображение сведений обо всех категориях;

**netsh diag show client** – отображение сведений обо всех клиентах сети;

**netsh diag show computer** – отображение сведений о компьютере;

**netsh diag show computer /p | more** – режим подробного протоколирования, отображаются все поля;

**netsh diag show computer /v | more** – режим указания свойств, отображаются только поля со значениями;

**netsh diag show dhcp** – отображение сведений о DHCP-серверах для каждого адаптера;

**netsh diag show dns** – отображение сведений о DNS-серверах для каждого адаптера;

**netsh diag show gateway** – отображение сведений о шлюзах по умолчанию для каждого адаптера;

**netsh diag show ieproxy** – отображение имени сервера Internet Explorer и номера порта;

**netsh diag show ip** – отображение сведений о IP-адресах для каждого адаптера;

**netsh diag show mail** – отображение имени почтового сервера и номера порта;

**netsh diag show modem** – отображение сведений обо всех модемах;

**netsh diag show modem /?** – вызов справки;

**netsh diag show modem 1 /v | more** – режим подробного протоколирования, отображаются все поля;

**netsh diag show news** – отображение имени сервера службы новостей и номера порта;

**netsh diag show os** – отображение сведений об ОС;

**netsh diag show test** – отображение всех категорий и выполнение всех тестов;

**netsh diag show version** – отображение сведений о версии Windows и WMI;

**netsh diag show wins** – отображение сведений об основном и вспомогательном WINS-серверах для каждого адаптера.

## 1.5. Реализация Virtual WiFi (для Windows 7)

### 1.5.1. Теоретические предпосылки

Беспроводные сети могут работать в двух режимах:

1) когда два и более устройства соединены непосредственно между собой;

2) «точка–точка», когда они подключены через точку доступа (Access Point-AP).

В первом случае говорят о простой сети (ad-hoc mode). Данный режим работы встречается достаточно редко и применяется, в основном, для обмена данными, когда нет возможности использовать точку доступа.

Второй режим, с использованием точки доступа, называется инфраструктурным (infrastructure mode) и в большинстве случаев применяется совместно с беспроводным маршрутизатором, подключенным к Интернету. Но одновременная реализация двух режимов работы на одном физическом беспроводном адаптере не предусмотрена самой концепцией WiFi.

В поисках новых способов использования беспроводных сетей была предложена концепция виртуализации, которая снимает определенные ограничения с применения таких сетей и тем самым расширяет их возможности. Данный подход к использованию беспроводных адаптеров был реализован несколькими компаниями со своими названиями технологий. В Intel – это Intel My WiFi, а в Microsoft – это Virtual WiFi. Одной из особенных

возможностей MS Virtual WiFi, по сравнению с Intel My WiFi, является максимальное количество подключаемых клиентов, их до 100. Конечно, с практической стороны, цифра почти недостижимая; но вполне возможно, что в ограничение всего в 8 клиентов можно «упереться» при использовании Intel My WiFi.

Virtual WiFi представляет собой программную прослойку, которая абстрагирует беспроводную сетевую карту и создает несколько виртуальных адаптеров. Каждый виртуальный адаптер может быть отдельно сконфигурирован для подключения к разным беспроводным сетям, но при этом все они будут использовать ресурсы только одного физического беспроводного адаптера.

В Windows 7 технология Virtual WiFi была включена в состав ОС и реализована на уровне ядра. Сеть, созданная с помощью технологии Virtual WiFi, обозначается как Wireless Hosted Network, в русском переводе от Microsoft звучит как *размещенная сеть*. В связи с введением технологии Virtual WiFi в новых ОС от Microsoft, в network shell были добавлены новые команды для управления распределенной сетью. Приведем некоторые из них:

**netsh wlan set hostednetwork [mode=]allowed|disallowed** – разрешение или запрет использования сети;

**netsh wlan set hostednetwork [ssid=]<идентификатор\_SSID> [key=]<парольная\_фраза> [keyUsage=]persistent|temporary** – настройка параметров размещенной сети, где SSID – идентификатор SSID сети; key – ключ безопасности пользователя, используемый сетью; keyUsage – указывает, является ключ безопасности постоянным или временным;

**netsh wlan show settings** – показ свойств сети и ее состояния;

**netsh wlan show hostednetwork settings=security** – отображение параметров безопасности размещенной сети и показ, в том числе, пароля, заданного в key при настройке netsh wlan set hostednetwork);

**netsh wlan start hostednetwork** – запуск сети;

**netsh wlan stop hostednetwork** – остановка сети.

### 1.5.2. Установка и настройка Virtual WiFi

На практике требуется ноутбук или обычный персональный компьютер с беспроводным устройством, Windows 7 и драйвер, поддерживающий Virtual WiFi (существует большая вероятность того, что загруженный драйвер беспроводного адаптера с Windows Update уже имеет поддержку Virtual WiFi).

Если описанные выше условия выполняются, то вызовите командную строку с правами администратора и выполните в ней следующую команду (рис. 10.1):

**netsh wlan set hostednetwork mode=allow ssid="MS Virtual WiFi" key="Pass for virtual WiFi" keyUsage=persistent**

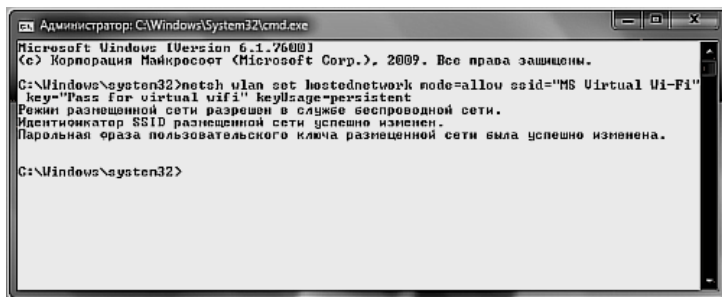


Рис. 10.1. Настройка виртуальной сети

В данном примере "MS Virtual WiFi" – имя беспроводной сети, "Pass for virtual WiFi" – пароль для доступа к этой сети (можно задать эти значения по своему усмотрению).

После выполнения данной команды система найдет новое оборудование (рис. 10.2), и в диспетчере устройств появится новый виртуальный сетевой адаптер – **Адаптер мини-порта виртуального WiFi Microsoft** (Microsoft Virtual WiFi miniport adapter). Данный виртуальный адаптер появится только в том случае, если драйвер беспроводного адаптера имеет поддержку Virtual WiFi.

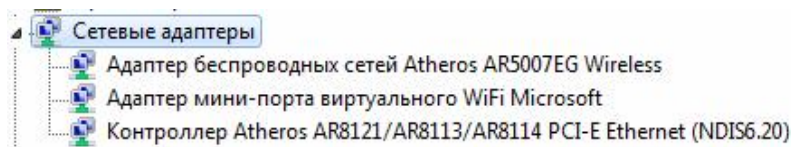


Рис. 10.2. Адаптер виртуальной сети

Перейдя в **Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера**, увидим новое соединение Wireless Network Connection 2, которое будет показывать статус – нет подключения.

Поэтому следующим этапом будет запуск сети: в командной строке, также запущенной с правами администратора, выполнить команду (рис.10.3):

**netsh wlan start hostednetwork**

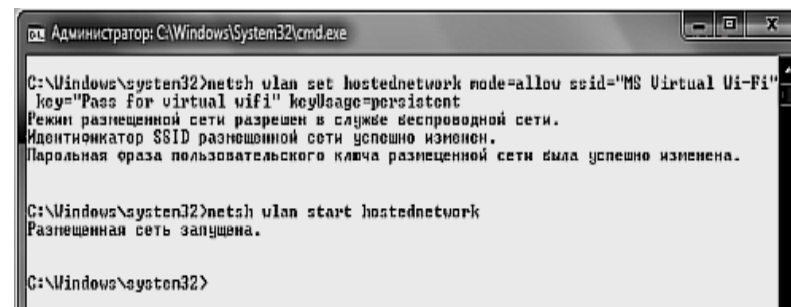


Рис. 10.3. Запуск виртуальной сети

После этого сеть запустится, и заработает программная точка доступа (SoftAP). В этом можно убедиться, перейдя в **Панель управления → Центр управления сетями и общим доступом** (рис. 10.4). Так как уже используется подключение к Интернету по WiFi, то обнаружим, что Windows 7 подключена одновременно к нескольким беспроводным сетям. Теперь другие беспроводные устройства могут подключаться к нашей точке доступа.

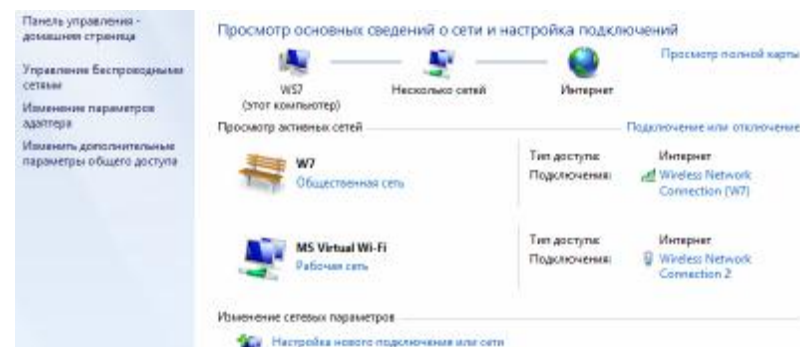


Рис. 10.4. Проверка виртуальной сети

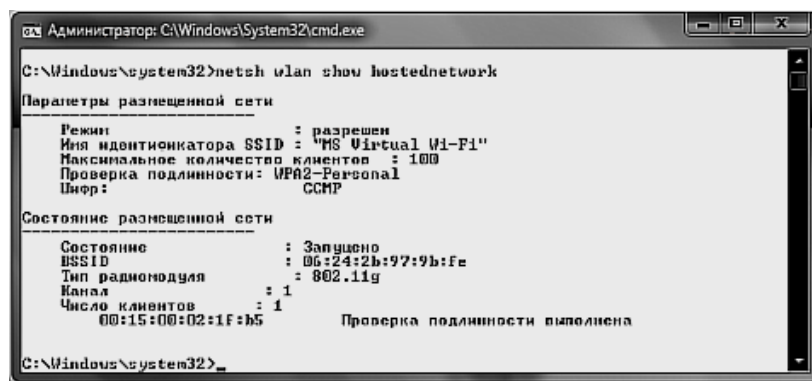
Если мы хотим предоставить доступ к Интернету другим беспроводным устройствам, которые подключены к нашей про-

граммной точке доступа (то есть организовать Хотспот (Hot-spot)), необходимо перейти в закладку **Панель управления** → **Центр управления сетями и общим доступом** → **Изменение параметров адаптера** и в свойствах соединения, через которое ноутбук получает Интернет (в нашем случае это подключение по WiFi, но оно может быть любым: ethernet, 3G, WiMax и т. п.), в закладке доступ поставить флажок **Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера**, а в **Подключение домашней сети** указать, на какой сетевой адаптер предоставить доступ (расшарить) Интернета. В нашем случае это будет Wireless Network Connection 2, который относится к виртуальному беспроводному адаптеру.

Со стороны клиента можно увидеть несколько беспроводных сетей, и при подключении к организованной нами точке доступа клиент автоматически получит IP-адрес с внутреннего DHCP сервера и будет отделен от внешней сети NAT (Network address translation).

Посмотреть состояние размещенной сети (количество клиентов, параметры соединений, протокол работы) можно следующей командой (рис. 10.5):

**netsh wlan show hostednetwork**



```
Администратор: C:\Windows\System32\cmd.exe
C:\Windows\system32>netsh wlan show hostednetwork
Параметры размещенной сети
-----
Режим                               : разрешен
Имя идентификатора SSID             : "MS Virtual Wi-Fi"
Максимальное количество клиентов    : 100
Проверка подлинности: WPA2-Personal
Шифр:                                CCMP

Состояние размещенной сети
-----
Состояние                           : Запущено
BSSID                                : 06:24:2b:97:9b:fe
Тип радиомодуля                      : 802.11g
Канал                                : 1
Число клиентов                       : 1
00:15:00:02:1f:b5                   Проверка подлинности выполнена

C:\Windows\system32>
```

Рис. 10.5. Состояние виртуальной сети

Далее необходимо отобразить параметры безопасности размещенной сети (показать, в том числе, пароль, заданный в key при настройке **netsh wlan set hostednetwork**). После этого необходимо остановить размещенную сеть.

## 1.6. Трассировка сети средствами Netsh.exe (для Windows 7)

### 1.6.1. Теоретические предпосылки

Windows 7 включает новый контекст утилиты Netsh.exe – netsh trace, служащий для трассировки сети. Команды в этом контексте позволяют выборочно включать трассировку провайдеров или сценариев. Провайдер – это отдельный компонент в стеке сетевых протоколов, такой как Winsock, TCP/IP, службы беспроводной локальной сети или NDIS. Сценарий трассировки – это набор провайдеров, реализующих одну функциональность, например совместный доступ к файлам или беспроводную локальную сеть. Чтобы избавиться от несущественных подробностей и уменьшить размер ETL-файла, можно применять фильтры.

Как правило, для выполнения детального анализа неполадок сети нужно предоставлять сотрудникам отдела поддержки или службе поддержки клиентов Microsoft как информацию о трассировке компонента, так и запись сетевого трафика во время проявления неполадки. До Windows 7 для получения этих данных приходилось выполнять две различных процедуры: использовать команды Netsh.exe для включения и отключения трассировки и задействовать сетевой анализатор, такой как сетевой монитор, для записи сетевого трафика. После этого предстояло решить нелегкую задачу синхронизации информации из этих двух источников, чтобы определить, как сетевой трафик соотносится с событиями в журналах трассировки.

В Windows 7 при выполнении трассировки сети в контексте netsh trace ETL-файлы могут последовательно содержать информацию и сетевого трафика, и трассировки компонента. Полученные ETL-файлы можно изучать средствами сетевого монитора версии 3.3, который предоставляет намного более эффективный интерфейс анализа и исследования сетевых неполадок. Эта новая возможность позволяет не требовать от конечных пользователей или сотрудников отдела поддержки для записи сетевого трафика устанавливать и использовать сетевой монитор на компьютере, где наблюдаются неполадки. По умолчанию ETL-файлы, созданные в сеансах диагностики неполадок приложения **Устранение неполадок компьютера** (Troubleshooting), не содержат данных сетевого трафика.

При использовании Netsh.exe в Windows 7 могут создаваться два файла. ETL-файл содержит события трассировки компонентов Windows и, если требуется, сетевого трафика. По умолчанию ETL-файл называется Nettrace.etl и размещается в папке %TEMP%\NetTraces. Можно указать другое имя и место, задав параметр **tracefile=**. Необязательный САВ-файл может содержать файлы нескольких типов, в том числе текстовые файлы, файлы реестра Windows, XML и другие, которые содержат дополнительную информацию для поиска неполадок. САВ-файл также включает копию ETL-файла. По умолчанию САВ-файл называется Nettrace.cab и размещается в папке %TEMP%\NetTraces.

### 1.6.2. Трассировка сети и создание отчета

Чтобы запустить трассировку сети в Netsh.exe, прежде всего надо открыть окно командной строки с дополнительными правами. Для получения списка провайдеров трассировки выполните команду **netsh trace show providers**. Получить список сценариев можно командой **netsh trace show scenarios**. Чтобы получить список провайдеров в сценарии, выполните команду **netsh trace show scenario ScenarioName**.

Можно запустить трассировку одного или нескольких провайдеров или сценариев. Например, трассировка сценария **InternetClient** запускается командой **netsh trace start scenario=InternetClient**. Чтобы запустить трассировку нескольких сценариев, надо последовательно их задать: **netsh trace start scenario=FileSharing scenario=DirectAccess**.

Чтобы создать САВ-файл с форматированным отчетом, добавьте параметр **report=yes**. Для задания имени и местоположения ETL- и САВ-файлов служит параметр **tracefile=parameter**. Если в ETL-файле нужно записать еще и сетевой трафик, добавьте параметр **capture=yes**.

Вот пример команды, которая запустит трассировку сценария WLAN, создаст САВ-файл с форматированным отчетом, запишет сетевой трафик и сохранит файлы под именем WLANTest в папке, например, C:\Tshoot:

```
netsh trace start scenario=WLAN capture=yes report=yes tracefile=c:\tshoot\WLANtest.etl.
```

Чтобы остановить трассировку, используйте команду **netsh trace stop**

Отчет располагается в архиве **cab** под именем **Report.html**. Этот отчет необходимо оформить в виде приложения к отчету по работе.

Окно команд приведено на рис. 10.6, а фрагмент отчета – на рис. 10.7.

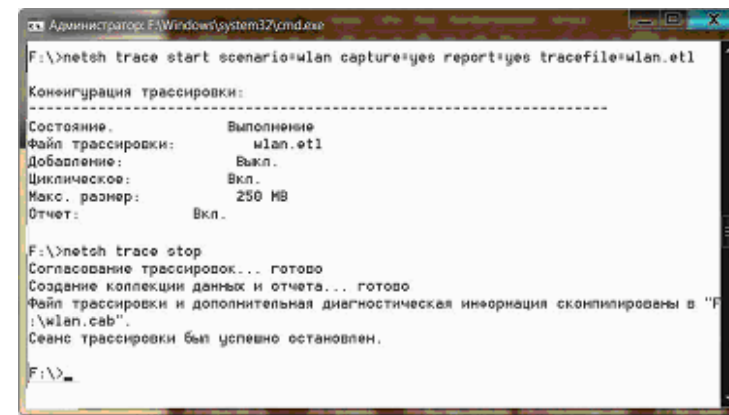


Рис. 10.6. Окно командного интерпретатора

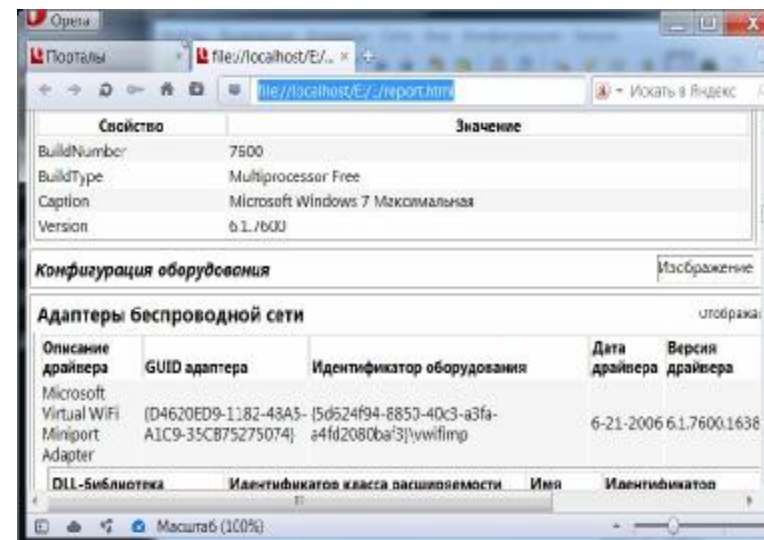


Рис. 10.7. Фрагмент отчета

### Содержание отчета

Проведите анализ полученных данных и отразите только те параметры, которые непосредственно влияют на работу локального компьютера в сети и предоставляют пользователю услуги сети.

### Контрольные вопросы

1. Какие параметры сети позволяют просмотреть встроенные средства диагностики netsh ОС MS Windows?
2. Как измерить с помощью netsh свой IP-адрес?
3. Как при помощи netsh сохранить и восстановить конфигурацию DHCP?

### Рекомендуемая литература

1. Борисенко, А. А. Локальная сеть. Просто как дважды два / А. А. Борисенко. – М. : Эксмо, 2007.
2. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник / В. Г. Олифер, Н. А. Олифер. – 3-е изд.– СПб. : Питер, 2006.
3. Олифер, В. Г. Основы компьютерных сетей : учеб. пособие / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2009.
4. Таненбаум, Э. Компьютерные сети / Э. Таненбаум. – 4-е изд. – СПб. : Питер, 2005.

### Содержание

Предисловие . . . . .	3
Лабораторная работа 1	
<b>Создание одноранговой сети . . . . .</b>	<b>4</b>
Лабораторная работа 2	
<b>Соединение двух компьютеров по WiFi . . . . .</b>	<b>15</b>
Лабораторная работа 3	
<b>Диагностика сети средствами ОС . . . . .</b>	<b>25</b>
Лабораторная работа 4	
<b>Управление сетевыми узлами . . . . .</b>	<b>29</b>
Лабораторная работа 5	
<b>Изучение протокола управления сетью SNMP . . . . .</b>	<b>42</b>
Лабораторная работа 6	
<b>Изучение настроек Ethernet и анализ трафика . . . . .</b>	<b>46</b>
Лабораторная работа 7	
<b>Изучение telnet-соединений . . . . .</b>	<b>50</b>
Лабораторная работа 8	
<b>Изучение TFTP-соединений . . . . .</b>	<b>53</b>
Лабораторная работа 9	
<b>Изучение встроенных средств диагностики WMIC . . . . .</b>	<b>57</b>
Лабораторная работа 10	
<b>Использование команды netsh . . . . .</b>	<b>61</b>
<b>Рекомендуемая литература . . . . .</b>	<b>75</b>

Учебное издание

## **СЕТИ ЭВМ**

### **ЛАБОРАТОРНЫЙ ПРАКТИКУМ**

**для студентов специальности  
1-08 01 01 «Профессиональное обучение»  
по направлению 1-08 01 01-07 «Информатика»**

Составители:

**Лукьянец Владимир Григорьевич  
Скудняков Юрий Александрович**

Ответственный за выпуск О. П. Козельская  
Редактор Г. Л. Говор  
Корректор Ю. С. Гришкевич  
Компьютерная верстка В. Ч. Николаевич, Г. Л. Говор

Подписано в печать 15.05.2013. Формат 60×84<sup>1</sup>/<sub>16</sub>. Бумага писчая.  
Ризография. Усл. печ. л. 4,42. Уч.-изд. л. 3,21. Тираж 70 экз. Заказ 57.

Издатель и полиграфическое исполнение:  
учреждение образования  
«Минский государственный высший радиотехнический колледж»  
ЛИ № 02330/0494033 от 08.01.2009.  
Пр. Независимости, 62, 220005, Минск.