

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ

Федеральное государственное автономное
образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания
к лабораторным работам
по дисциплине
«Компьютерные сети»

для бакалавров направления
01.03.02 Прикладная математика и информатика

Ставрополь, 2026

ОГЛАВЛЕНИЕ

Введение.....	3
1 Изучение сетевых средств операционной системы.....	5
2 Изучение настроек Ethernet и способов анализа трафика	8
3 проверка наличия связи компьютеров в сети.....	12
4 Создание одноранговой сети	22
5 Основы IP - адресации.....	29
6 Изучение сетевого уровня модели OSI на примере протокола IP	32
7 Сетевые утилиты ОС Windows	37
8 Протоколы высших уровней модели OSI.....	46
9 Настройка беспроводной сети	53
10 Установка DNS сервера.....	73
11 Создание пользователей домена.....	84
12 Создание пользователей сервером	88
13 Контрольная работа	103
14 Изучение встроенных средств диагностики в ОС - WMIC	109
15 Проектирование локальной сети	112
16 Изучение маршрутизации IP.....	129
Литература	135

ВВЕДЕНИЕ

Целью освоения данной дисциплины является изучение студентами компьютерных сетей, необходимое для приобретения ими соответствующих компетенций в научно-производственной деятельности, выработки умения моделировать реальные процессы и системы.

Задачами освоения дисциплины являются:

- формирование знания теоретических и практических основ в области вычислительных сетей;
- научить подключать компьютер к сетям, и работать в сетях;
- научить использовать аппаратные, программные и информационные ресурсы сетей;
- научить работать с сетевыми прикладными программами.

Освоение дисциплины «Компьютерные сети» позволит будущему бакалавру по направлению подготовки «Прикладная математика и информатика» полноценно осуществлять свою профессиональную деятельность, в частности, обладать следующими компетенциями:

- Способен разрабатывать и реализовывать в виде программного модуля алгоритм решения поставленной теоретической или прикладной задачи на основе математической модели (ПК-2),
- Способен разрабатывать программное и информационное обеспечение компьютерных систем, сервисов, вычислительных комплексов, баз данных (ПК-2).

Студенты, овладевшие указанными компетенциями, должны:

знать:

- состав, типы, параметры и характеристики компьютерных сетей;
- параметры и характеристики компьютерных сетей;
- OSI-модель взаимодействия открытых систем.

уметь:

- использовать инструментарий для объединения компьютеров в сеть;
- создавать одноранговые компьютерные сети;
- настраивать сетевые коммутационные устройства;

владеть:

- методикой использования утилит для сетевой диагностики;
- методикой установки программного обеспечения для сетевых устройств;
- методами организации беспроводных компьютерных сетей.

Аппаратура и материалы

Лабораторный практикум выполняется в штатном компьютерном классе, оборудованном IBM-совместимыми персональными компьютерами под управлением операционной системы Windows.

Указания по технике безопасности

Указания по технике безопасности в штатном компьютерном классе разработаны и утверждены администрацией и доводятся каждому студенту под роспись. Дополнительных требований нет.

1 ИЗУЧЕНИЕ СЕТЕВЫХ СРЕДСТВ ОПЕРАЦИОННОЙ СИСТЕМЫ

Цели работы

1. Ознакомиться с встроенными инструментальными средствами ОС Windows для отладки связности и диагностики сети.
2. Собрать информацию о сетевом оборудовании, программном обеспечении и сетевых подключениях персонального компьютера, работающего под управлением ОС MS Windows.

Теоретические сведения

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

Диагностика сети позволяет выполнить различные тесты и собрать информацию о сети. В зависимости от выбранных параметров, диагностика сети тестирует сетевое взаимодействие и проверяет доступность некоторых сетевых служб и программ. Также, производится сбор основной информации о компьютере. Это средство предоставляет возможность поиска причин, вызвавших проблемы с сетью.

Диспетчер состояния - еще один ключевой компонент справочной системы Windows XP. Его назначение - 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 в центр справки и поддержки и отображают информацию, собранную службой-поставщиком Windows Management Instruments - WMI (Инструментарий управления Windows), сокращенно WMIPRVSE. Исполняемый файл HELPCTR.EXE поддерживает основной интерфейс центра справки и поддержки и использует файлы HELPHOST.EXE и HELPSVC.EXE для обеспечения работы слушателя хоста и служб поддержки соответственно.

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

Возможные проблемы связности сети:

- Оконечные нагрузки ЛВС должным образом не подключены.

- ЛВС-интерфейс не работоспособен.
- ЛВС-интерфейс имеет не правильный IP-адрес.
- Маска подсети имеет не верное 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.

Порядок выполнения работы

1. С помощью «Центра справки и поддержки» MS Windows собрать информацию о системе:

Вызовите «Центр справки и поддержки» MS Windows с помощью клавиши [F1].

Выберите меню «Использование служебных программ для просмотра информации о компьютере и диагностики неполадок», далее «Расширенные сведения о системе». После выполнения «Настроить параметры сбора информации» выберите следующую возможность диагностики MS Windows: «Диагностика сети». Диагностика сети собирает информацию об оборудовании, программном обеспечении и сетевых подключениях. Проанализировать информацию и описать: «Службы Интернета», «Информация о компьютере», «Модемы и сетевые адаптеры».

2. С помощью программы MS Windows «Сведения о системе» и systeminfo собрать информацию о системе:

Запустить командный процессор: «Пуск»//»Выполнить»//»cmd

Выполнить команду: `cd C:\Program Files\Common Files\Microsoft Shared\MSInfo\`

Выполнить команду: `msinfo32`

Выполнить команду: `systeminfo`

Проанализировать информацию, дополнить недостающие данные, полученные в п. 1

3. Проанализировать связность сети, к которой подключен компьютер. С помощью команд MS Windows просмотреть и описать подключение к локальной сети. С командной строки выполните команды, указанные в таблице 1.1.

Таблица 1.1 – Команды диагностики сети

Команды	Содержание команды
<code>C:\>netstat.exe -rn</code>	Просмотреть записи в локальной таблице IP-маршрутизации

netstat.exe -s	Просмотреть статистические данные протоколов
netstat.exe -a	Просмотреть все подключения и ожидающие порты
net /help	Просмотреть команды сетевых служб
tracert	Проверить TCP/IP-соединения с помощью команд
ipconfig.exe / all	Вывод IP-адреса, маски подсети и основного шлюза для каждого сетевого адаптера
nslookup	Диагностировать инфраструктуру DNS (выйти из nslookup ,exit или Ctrl-C)
ping	Проверить TCP/IP-соединения с помощью команд
arp -a	Просмотр записей кэш, использующихся для хранения IP-адресов и соответствующих им физических адресов

Содержание отчета

Из теоретических сведений - «Возможные проблемы связности сети».

В отчете описать полученные результаты: «Информация о компьютере», «Модемы и сетевые адаптеры», информация о сетевых настройках, о подключениях компьютера.

Составить таблицу аналогичную 1.1 с фиксацией основных результатов исполнения команд скриншотами.

Контрольные вопросы

- 1.Что определяет связность сети?
- 2.Какие утилиты используются в ОС Windows для анализа сетевых подключений компьютера?

2 ИЗУЧЕНИЕ НАСТРОЕК ETHERNET И СПОСОБОВ АНАЛИЗА ТРАФИКА

Цель работы

Ознакомиться с настройками сетевой платы и встроенными инструментальными средствами ОС MS Windows анализа трафика на сетевых интерфейсах.

Теоретические сведения

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

Для просмотра состояния взаимодействия компьютера с локальной сетью различные разработчики операционных систем представляют средства диагностик.

Средства диагностики могут быть графическими или использовать командную строку (так называемый CLI - Command lininterface). Диагностика с помощью CLI позволяет создавать скрипты или программы для включения их в приложения занимающиеся мониторингом или анализом сети в целом.

В данной работе необходимы следующие понятия:

- Скрипт (script) - небольшая программа для выполнения средствами операционной системы 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 путём 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 операционной системы Windows.

Порядок выполнения работы

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

1. Описание свойств сетевой платы.

Выполнить в следующей последовательности доступ к настройкам сетевой платы:

Пуск - панель управления - подключение к локальной сети (сетевые подключения) – вызов контекстного меню- свойства- настроить.

Сохранить в отчет все свойства сетевой платы в виде таблицы 2.1.

Таблица 2.1 – Свойства сетевой платы
<Название сетевой платы>

Свойство	Установленное значение	Возможные значения
Скорость и дуплекс	Автосогласование	От 10Мбит/с дуплекс...до 100Мбит/с полудуплекс
Wake Up Capabilities Magic packet	None,	Wake Up Frame, Both,

2. Изучить возможность консоли управления ММС по встроенной справке (Консоль - действия – справка). Кратко отразить полученные сведения в отчете.

3. Настройка консоли ОС MS Windows для анализа трафика сетевого интерфейса.

Панель управления – Администрирование – Производительность - контекстное меню – добавить счетчики - объект - сетевой интерфейс - добавить счетчики: «отправлено байт/сек», «получено байт/сек». В свойствах графика указать диапазон вертикальной шкалы =5. Вывести заголовок над динамическим графиком- «Сетевой трафик».

4. В окне командного процессора выполнить команду:
ping -l 10000 127.0.0.1 -t (Выход – ctrl+c)

В течении ~1 минуты снять статистику, проанализировать, сделать вывод. В отчет вставить формат отклика.

5. В окне командного процессора выполнить команду:
ping -l 65500 127.0.0.1 -t

В течении ~1 минуты снять статистику, проанализировать сделать вывод. В отчет вставить формат отклика.

Данные процедуры позволяют рассмотреть скорее качественное состояние статистики интерфейса, чем количественное.

Это связано с тем, что ping отправляет 1 пакет/сек, а статистика собирается за секунду. Т.о. статистика отображает среднюю за секунду величину, а не текущую.

6. Определение размера ICMP-пакетов.

Подобрать значение длины пакетов, чтобы не было сообщений ошибок пакетов. Для этого в текстовом редакторе создать командный файл proba.bat следующего содержания:

```
@echo off
for /L %%i in (1000#,100#,100000#) do (
for /F «usebackqdelims=< tokens=2» %%a IN (
`ping -l %%i 127.0.0.1 -n 1`) DO @echo Размербуфера
отправки=%%i.....Время отклика=%%a)
```

В отчете дать объяснения остановки команды ping и при какой величине.

Подобрать значение длины пакетов, чтобы не было сообщений ошибок при фрагментации пакетов.

В текстовом редакторе создать командный файл proba_2.bat следующего содержания:

```
@echo off
for /L %%i in (1000#,1#,10000#) do (
for /F «skip=2 usebackqdelims=< tokens=2» %%a IN (
`ping -f -l %%i 127.0.0.1 -n 1`) DO @echo Размербуфера
отправки=%%i.....Время отклика=%%a)
```

В отчете дать объяснения остановки команды ping и при какой величине.

7. Просмотр статистики Ethernet интерфейса и протоколов IP стека.
Работа и оформление отчета в виде таблицы 2.2.

Таблица 2.2 - Отчет

Описание действий	Команды
Просмотреть MAC-адреса Ethernet	getmac
С помощью утилит собрать статистику Ethernet интерфейса и протоколов стека IP	netstat
Ознакомление с командами	netstat -s -p ICMP 1
	netstat -s -p UDP 1
	netstat -s -p TCP 1

В отчете описать имеющуюся статистику.

Содержание отчета

1. Характеристики сетевой платы по таблице 2.1.
2. Возможности консоли управления ММС. Анализ статистики, выводы, формат отклика по п. 4-6.
3. Статистика Ethernet интерфейса по таблице 2.2.

Контрольные вопросы

1. Характеристики сетевой платы.
2. Рассказать о способах диагностики сетевых подключений в ОС MS Windows.

3 ПРОВЕРКА НАЛИЧИЯ СВЯЗИ КОМПЬЮТЕРОВ В СЕТИ

Цель работы

Научиться применять команды Ping для проверки наличия связи компьютеров в сети и для анализа качества связи ПК, научиться пользоваться командами PathPing, Ipconfig, Net view и Tracert.

Теоретические сведения

Наиболее быстрым способом проверки работоспособности локальной можно назвать системную команду PING, которая посылает сетевой запрос на заданный IP-адрес компьютера, получает ответ и выводит отчет на экран. Если посланный запрос получен обратно - связь физически существует, то ваша сеть настроена и работает корректно. Если же на экране вы увидите надпись «Превышен интервал ожидания запрос» - вы допустили ошибку либо в настройках, либо в подключении компьютеров. Перед запуском команды Ping необходимо посмотреть доступные компьютеры в сети. Заходим в **Компьютер** и видим, что в нашей рабочей группе 110 имеется четыре ПК (рисунок 3.1).



Рисунок 3.1 - В рабочей группе 110 мы видим 4 ПК

Для того чтобы воспользоваться командой ping, откройте окно командной строки командой **Пуск-Все программы-Стандартные-Командная строка** и введите там команду ping, укажите имя или IP-адрес удаленного

компьютера (или его ИМЯ»/»>) (рисунок 3.2). По умолчанию утилита ping отправляет 4 пакета и ожидает каждый ответ в течение четырех секунд. По умолчанию команда посылает пакет 32 байта. За размером тестового пакета отображается время отклика удаленной системы (в нашем случае - меньше 1 миллисекунды»/»>).

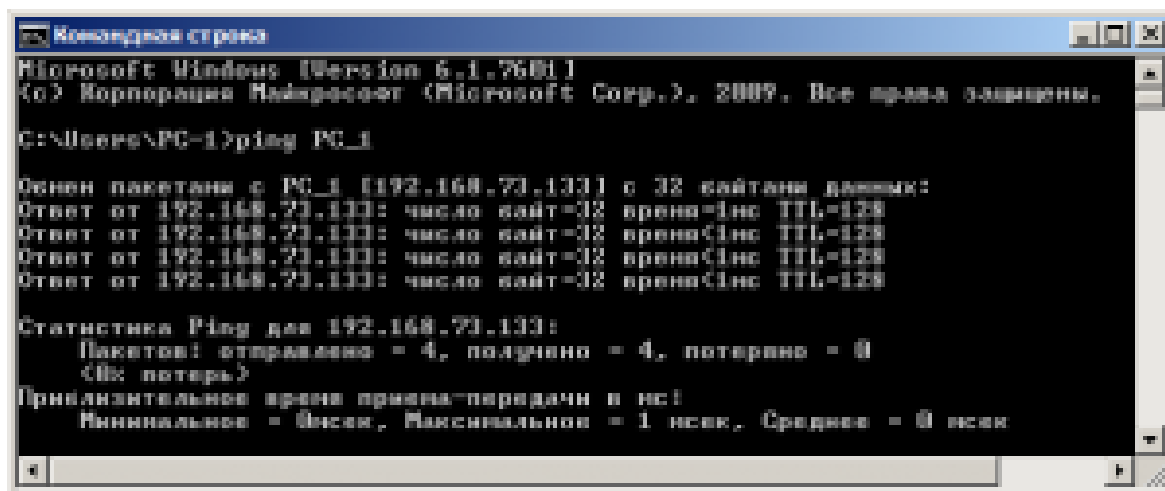


Рисунок 3.2 - Пингование машины PC_1 с IP-адресом 192.168.73.133

При необходимости для этой команды вы можете использовать следующие параметры:

- t. Данный параметр указывает на то, что производится проверка связи с указанным узлом до прекращения вручную;
- n. Текущий параметр определяет количество отправляемых Echo-запросов;
- f. Этот параметр устанавливает бит «не фрагментировать» на ping-пакете. По умолчанию фрагментация разрешается;
- w. Данный параметр позволяет настроить тайм-аут для каждого пакета в миллисекундах (по умолчанию установлено значение 4000»/»>);
- a. Текущий параметр определяет имена узлов по адресам;
- l. При помощи этого параметра вы можете указать размер буфера отправки;
- i. Использование данного параметра позволяет вам задать срок жизни пакета;
- v. Этот параметр задает тип службы для IPv4 и не влияет на поле TOS в IP-заголовке;
- r. Текущий параметр записывает маршрут для указанного числа прыжков;
- s. Данный параметр позволяет отмечать время для указанного числа прыжков;
- j. Используя этот параметр, вы можете указать свободный выбор маршрута по списку узлов;
- k. При помощи данного параметра вы можете определить жесткий выбор маршрута по списку узлов;
- R. Текущий параметр позволяет использовать заголовок для проверки

- также и обратного маршрута только для IPv6;
- S. Данный параметр указывает используемый адрес источника;
 - 4. Параметр определяет принудительное использование протокола IP версии 4;
 - 6. Параметр определяет принудительное использование протокола IP версии 6.

Итак, выше было показано, что утилита **Ping** используется в том случае, когда необходимо проверить, может ли компьютер подключиться к сети ТСР/IP или сетевым ресурсам. Иначе говоря, мы пингуем для того, чтобы проверить, что отправляемые пакеты доходят до получателя. ПК-отправитель отправляет Echo-запрос, а ПК-получатель, в ответ должен отправить ICMP-сообщение с ответом. Если удаленный компьютер реагирует на запрос ping, то подключение к удаленному компьютеру работает. Также, утилита ping ведет статистику, из которой понятно, сколько пакетов получено, а сколько потеряно. Но, это еще не все.

Применение команды Ping для анализа качества связи ПК в сети

Для тестирования качества связи запустите Ping со следующими параметрами: **ping.exe -l 16384 -w 500 -n 100 192.168.73.133**. Это обеспечит отправку 100 запросов (n) пакетами по 16 килобайт (l) на заданный IP адрес с интервалом ожидания ответа в 0,5 секунды (w). То есть:

L – размер буфера отправки.

N – число отправляемых запросов,

W – время ожидания ответа на запрос в миллисекундах,

Подождите, пока пройдут все 100 пакетов. Ответ должен будет быть приблизительно такой (рисунок 3.3).

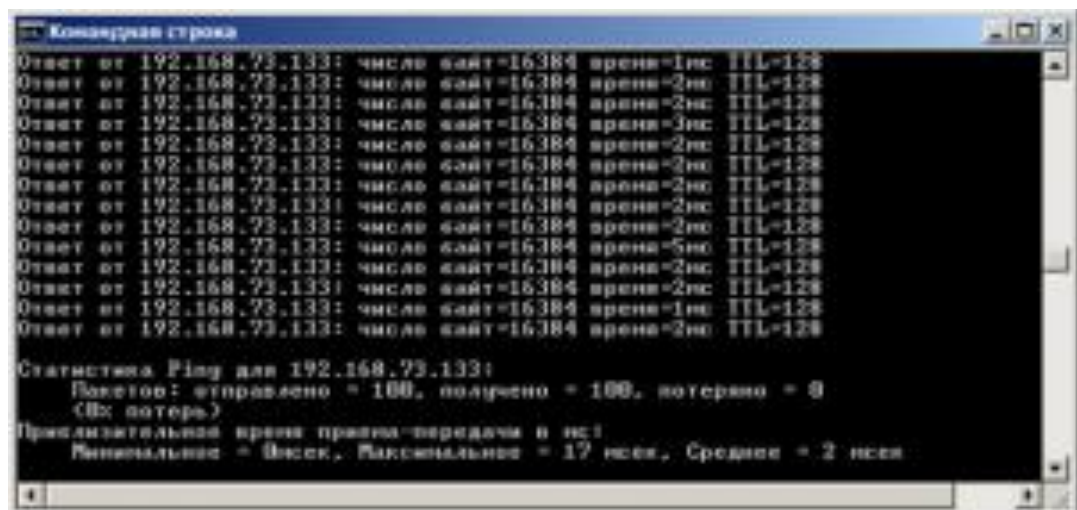


Рисунок 3.3 - Ответ на команду ping.exe с ключами

Проанализируем результат выполнения команды:

0% потеря – сеть работает отлично.

Если потери информации составили не более 3%, то сеть работает хо-

рошо.

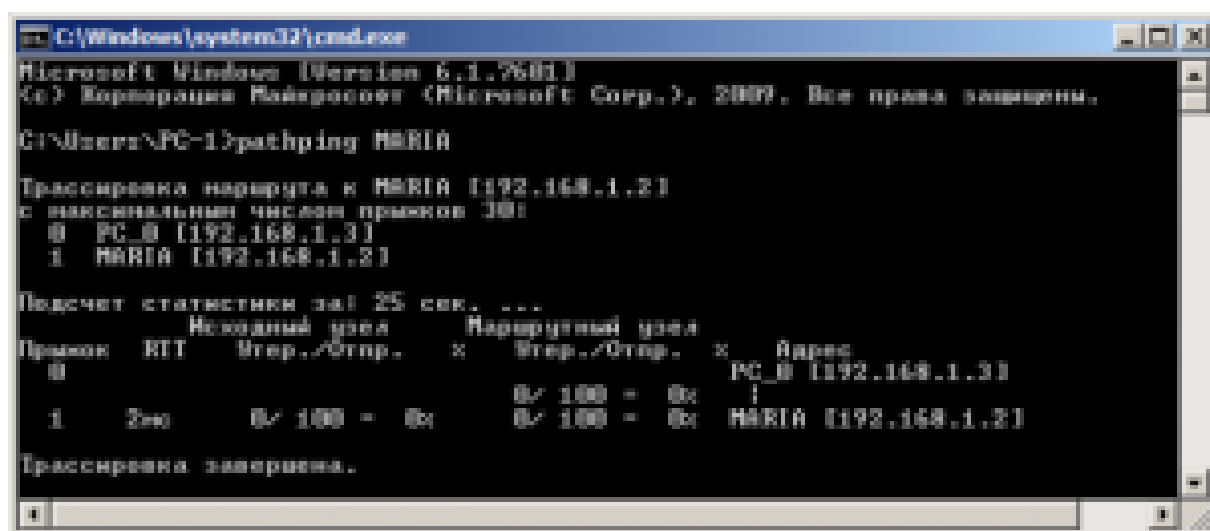
При потерях 3-10% дошли не все пакеты, но сеть, благодаря алгоритмам коррекции ошибок, работает удовлетворительно. Из-за необходимости повторной доставки потерянной информации снижается эффективная скорости работы сети – сеть тормозит.

Если число потерянных пакетов превышает 10-15%, то необходимо принять меры по устранению неисправности. Качество связи ПК неудовлетворительное.

Далее: как видим, время отклика удаленной системы среднее 2 мсек, а максимальное 17 мсек. Анализируя отклик по миллисекундам, надо иметь ввиду следующее. По стандарту, нормальное время отклика 16-килобайтного пакета для 100-мегабитной сети - 3-8 мс. Для 10-мегабитной - 30-80 мс. Получается, что у нас сеть работает на скорости порядка 100 мбит/сек.

Использование утилиты PathPing

Pathping это утилита, которая позволяет обнаружить потери пакетов на маршруте между вашим компьютером и заданным адресом IP. Потери пакетов могут сильно повлиять на работу сети, например, когда вы играете в видеоигру. Иначе говоря, утилита PathPing отправляет многочисленные сообщения с Echo-запросом каждому маршрутизатору, который находится между исходным пунктом и пунктом назначения, после чего, на основании пакетов, полученных от каждого из них, вычисляет процентное соотношение пакетов, возвращаемых в каждом прыжке. Поскольку утилита PathPing показывает степень потери пакетов на каждом маршрутизаторе или узле, то с ее помощью вы можете точно определить маршрутизаторы и узлы, на которых возникают сетевые проблемы. Пример использования данной команды приведен на рисунке 3.4.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\PC-1>pathping MARIA

Трассировка маршрута к MARIA [192.168.1.2]
с максимальным числом прыжков 30:
  0  PC_0 [192.168.1.3]
  1  MARIA [192.168.1.2]

Подсчет статистики займ 25 сек. ...

Прыжок  RTT  Исходный узел  Маршрутный узел
Прыжок  RTT  Утер./Отпр.  %  Утер./Отпр.  %  Адрес
0        200  0/ 100 = 0%  0/ 100 = 0%  PC_0 [192.168.1.3]
1        200  0/ 100 = 0%  0/ 100 = 0%  MARIA [192.168.1.2]

Трассировка завершена.
```

Рисунок 3.4 - Поиск потерь пакетов на маршруте от ПК PC_0 до ПК MAIRIA

Итак, в строке поиска наберем **CMD**, чтобы вызвать командную строку (рисунок 3.5).

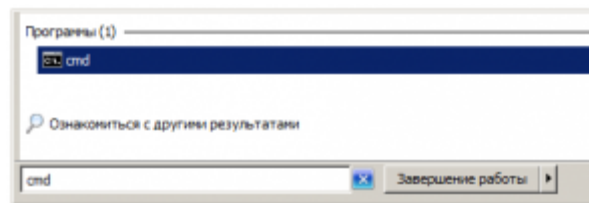


Рисунок 3.5 - Один из способов вызова командной строки в ОС Windows

Далее произведет трассировку маршрута от нашего ПК до поискового сервера Яндекс (рисунок 3.6).

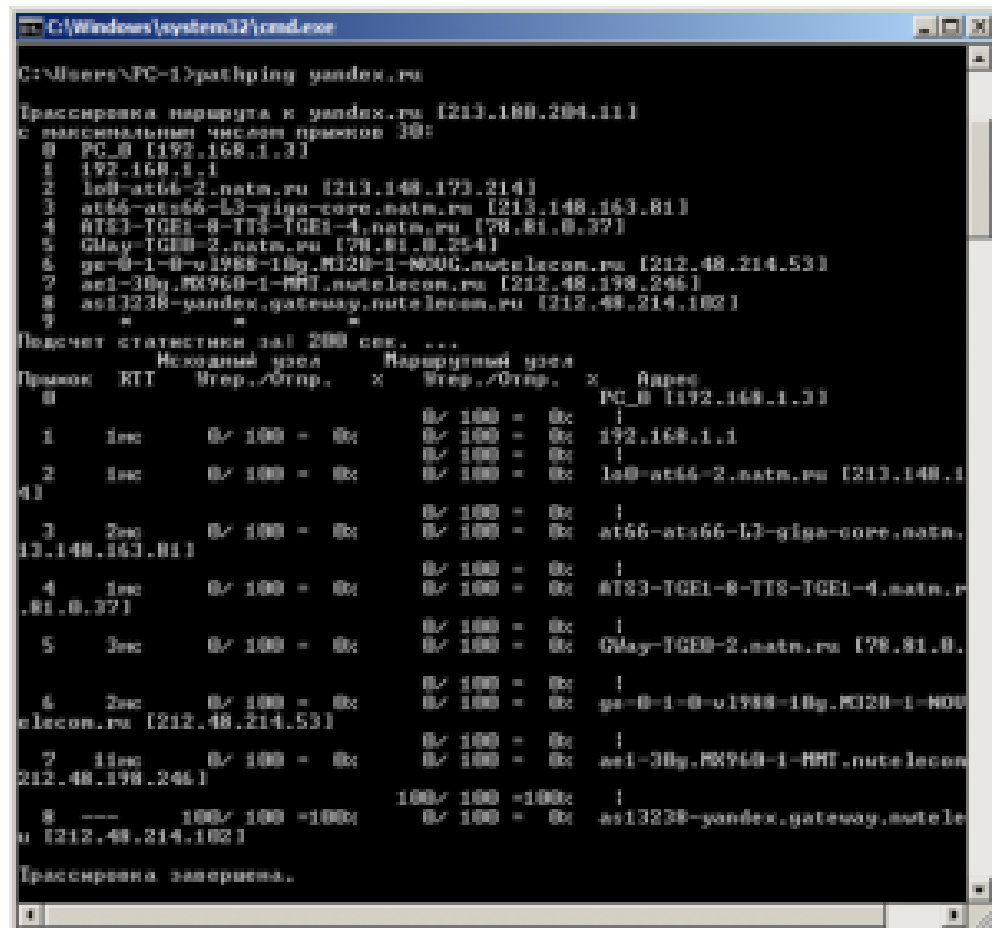


Рисунок 3.6 - Пример использования утилиты Pathping

Проанализируем результат:

Первый блок информации представляет собой трассировку. Вы можете пропустить его и перейти ко второму блоку информации, в котором будет указано процентное отношение потерь пакетов.

Если пакеты не терялись на данном маршруте подключения, то вы увидите 0% потерь пакетов. Если вы увидите значения, отличающиеся от 0%, это означает, что на пути к нашим серверам были потери пакетов. Потери выше 1% начиная с первого шага, могут указывать на некорректную работу узлов сети или маршрутизаторов. Если эти устройства вам доступны, то нужно попробовать обновить их программное обеспечение или полностью заменить их. Иначе, о потерях, возникших после первого шага и до последне-

го шага, следует сообщить вашему Интернет провайдеру.

Примечание

Если последние строки указывают на 100% потерь, то это не является показателем проблемы, а происходит потому, что сервера защищены от нежелательного трафика и атак.

С данной командой вы можете использовать следующие параметры:

- g. Данный параметр определяет использование параметра свободной маршрутизации в IP-заголовке с набором промежуточных мест назначения для сообщений с Echo-запросом, который указывается в списке компьютеров.
- h. Данный параметр задает максимальное количество переходов на пути при поиске конечного объекта;
- i. Этот параметр указывает IP-адрес источника;
- n. Текущий параметр предотвращает попытки сопоставления IP-адресов промежуточных маршрутизаторов с их именами, что существенно ускоряет вывод результатов;
- p. Используя данный параметр, вы можете задать время ожидания между последовательными проверками связи, где значением по умолчанию указано 250 миллисекунд;
- q. При помощи текущего параметра вы можете указать количество сообщений с Echo-запросом, отправленных каждому маршрутизатору пути (по умолчанию - 100);
- w. Данный параметр определяет время ожидания для получения Echo-ответов протокола ICMP или ICMP-сообщений об истечении времени в миллисекундах, которые соответствуют данному сообщению Echo-запроса. Значение по умолчанию 4 секунды;
- 4. Параметр определяет принудительное использование протокола IP версии 4;
- 6. Параметр определяет принудительное использование протокола IP версии 6.

Другие команды командной строки.

Отображение параметров TCP/IP-протокола командой `Ipconfig`

Команда **IPCONFIG** используется для отображения текущих настроек протокола TCP/IP и для обновления некоторых параметров, задаваемых при автоматическом конфигурировании сетевых интерфейсов при использовании протокола DHCP. Предположим, что у нас имеется сеть, изображенная на рисунке 4.7.

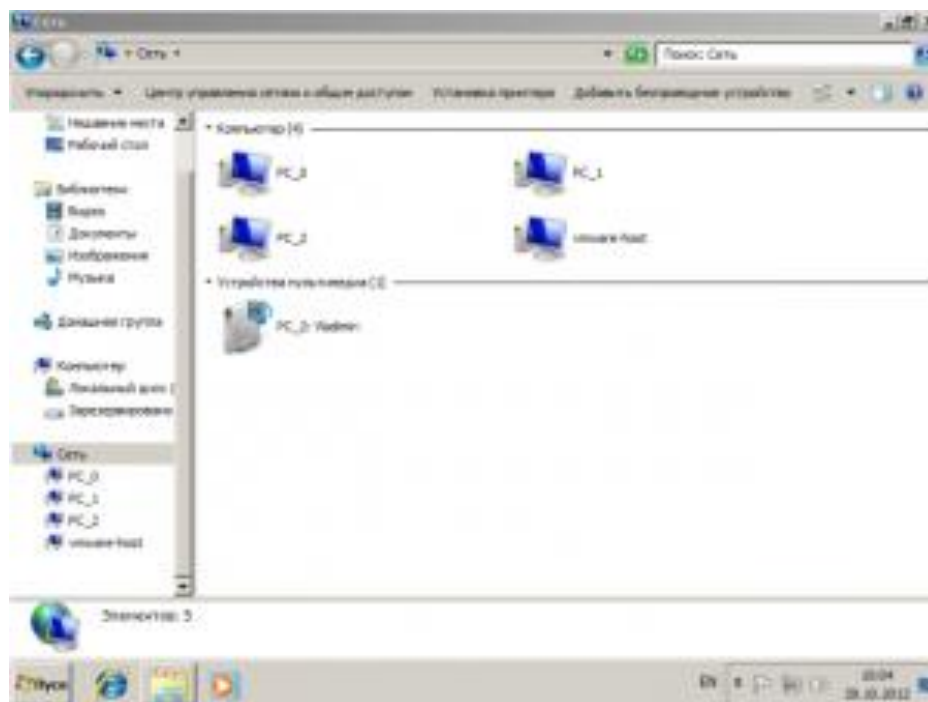


Рисунок 3.7 - Небольшая локальная сеть

Выполним команду командой Ipconfig на PC_2 (рисунок 3.8).

```
Администратор: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 5.1.7600]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Users\Vladimir>ipconfig

Настройка протокола IP для Windows

Ethernet adapter Подключение по локальной сети1:

   DNS-суффикс подключения . . . . . : localdomain
   Локальный IPv6-адрес канала . . . . : fe80::1179:c14a:c226:201c::11
   IPv4-адрес . . . . . : 192.168.73.133
   Маска подсети . . . . . : 255.255.255.0
   Основной шлюз . . . . . : 192.168.73.2

Туннельный адаптер isatap.localdomain:

   Состояние среды . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . : localdomain

Туннельный адаптер Подключение по локальной сети4:

   DNS-суффикс подключения . . . . . : 
   IPv6-адрес . . . . . : 2001::0:5ef5:79fd:c437:379d:3f57:b67a
   Локальный IPv6-адрес канала . . . . : fe80::4247:299d:3f57:b67a::13
   Основной шлюз . . . . . : ::
```

Рисунок 3.8 - Отображение параметров TCP/IP-протокола командой Ipconfig

Из отчета мы видим такую информацию:

DNS-суффикс подключения -localdomain (из настроек сетевого подключения)

Локальный IPv6-адрес канала - локальный IPv6 адрес, если используется адресация IPv6

IPv4-адрес - используемый для данного адаптера IPv4 – адрес

Маска подсети - 255.255.255.0

Основной шлюз - IP-адрес маршрутизатора, используемого в качестве шлюза по умолчанию.

Примечание

Туннельный адаптер `isatap.localdomain` это эмуляция IPV6 в сетях IPV4. ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) - Протокол автоматической внутрисайтовой адресации туннелей, позволяющий передавать между сетями IPv6 пакеты через сети IPv4

Ключи команды:

`/all` Отображение полной информации по всем адаптерам.

`/release [адаптер]` Отправка сообщения DHCPRELEASE серверу DHCP для освобождения текущей конфигурации DHCP и удаления конфигурации IP-адресов для всех адаптеров (если адаптер не задан) или для заданного адаптера. Этот ключ отключает протокол TCP/IP для адаптеров, настроенных для автоматического получения IP-адресов.

`/renew [адаптер]` Обновление IP-адреса для определённого адаптера или если адаптер не задан, то для всех. Доступно только при настроенном автоматическом получении IP-адресов.

`/flushdns` Очищение DNS кэша.

`/registerdns` Обновление всех зарезервированных адресов DHCP и перерегистрация имен DNS.

`/displaydns` Отображение содержимого кэша DNS.

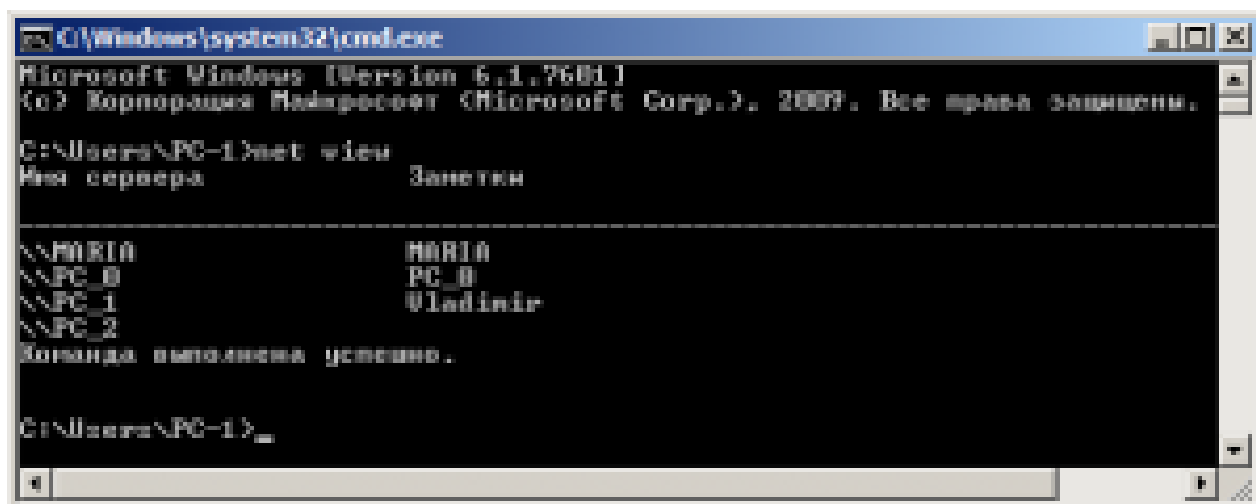
`/showclassid адаптер` Отображение кода класса DHCP для указанного адаптера. Доступно только при настроенном автоматическом получении IP-адресов.

`/setclassid адаптер [код_класса]` Изменение кода класса DHCP. Доступно только при настроенном автоматическом получении IP-адресов.

`/?` Справка. TCP/IP: значения IP адреса, маски и шлюза.

Команда вывода списка компьютеров рабочей группы Net view

В командной строке введите команду **netview**, и вы увидите список компьютеров своей рабочей группы (рисунок 3.9).



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\PC-1>net view
Имя сервера          Заметки
-----
\\MARIA               MARIA
\\PC_0                PC_0
\\PC_1                Vladimir
\\PC_2
\\PC_3
Команда выполнена успешно.

C:\Users\PC-1>
```

Трассировка

Запуск программы производится из командной строки. Для этого вы должны войти в неё. Для операционной системы Windows 7 существует несколько способов запуска командной строки:

Пуск - Все программы- Стандартные - Командная строка.

В открывшемся окне мы напомним **tracert ya.ru**. Принцип действия этой программы схож с принципом действия программы **ping**. Команда отправляет на сервер данные и при этом фиксирует все промежуточные маршрутизаторы, через которые проходят эти данные на пути к серверу (целевому узлу). Если при доставке данных до одного из узлов происходит проблема, программа определяет участок сети, на котором возникли неполадки. Время отклика показывает загруженность канала. А вот если вместо времени отклика вы видите надпись **«Превышен интервал ожидания для запроса»**, это значит, что на данном узле связи происходит потеря данных, а значит, проблема именно в нем – рисунок 3.10.

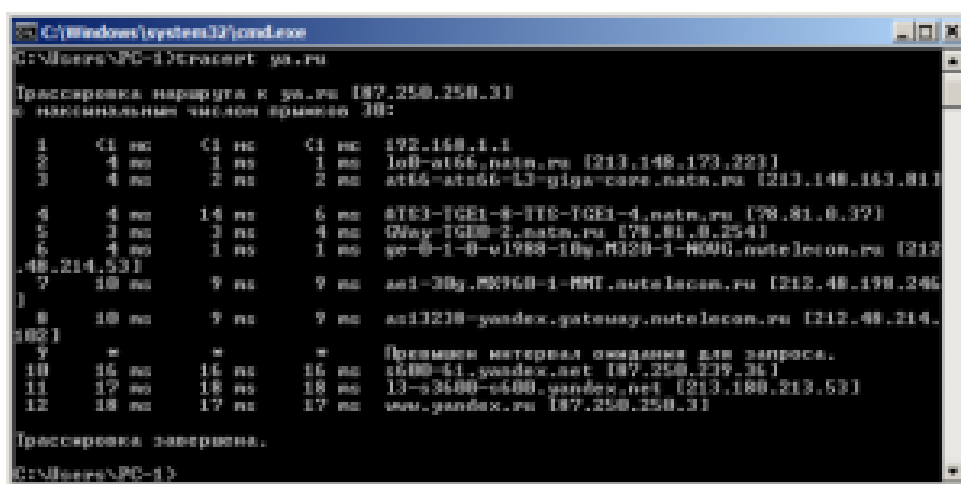


Рисунок 3.10 - Пример трассировки домена ya.ru

- d не определять доменные имена маршрутизаторов
- h <значение> установить максимальное количество переходов
- w <значение> установить максимальное время ожидания ответа (в

миллисекундах)

Итак, трассировка маршрута помогает определить проблемный узел. Если данные проходят нормально и «стопорятся» на самом пункте назначения, то проблема действительно с сайтом. Если трассировка маршрута прекращается на середине пути, то проблема в одном из промежуточных маршрутизаторов. Если прохождение пакетов прекращается в пределах сети вашего провайдера - то и проблему нужно решать «на местном уровне». Попутно хочется отметить, что программа работает только в направлении от источника пакетов и является весьма грубым инструментом для выявления неполадок в сети.

Содержание отчета

В лабораторной работе рассмотрено применение команды Ping для проверки наличия связи компьютеров в сети и для анализа качества связи ПК, а также команд PathPing, Ipconfig, Net view и Tracert; тема, цель, скриншоты основных результатов по применению команд.

4 СОЗДАНИЕ ОДНОРАНГОВОЙ СЕТИ

Цель работы

Научиться создавать одноранговую сеть.

Аппаратное и программное обеспечение для проведения работы:

1. Рабочий компьютер с сетевым адаптером для каждого учащегося или для группы учащихся.
2. Присвойте каждому компьютеру уникальное имя.
3. На каждом компьютере должно быть установлена операционная система MicrosoftWindows.
4. Необходим один хаб на группу.
5. Сетевой кабель «витая пара» пятой категории с RJ-45 коннекторами для каждого компьютера.

Пошаговое создание сети - Ход работы:

Для всех компьютеров присоедините сетевые адаптеры рабочих станций, входящих в рабочую группу, к хабу рабочей группы, используя кабель пятой категории с RJ-45 коннекторами.



Рисунок 4.1 - Схема одноранговой сети

Запустите те компьютеры, которые будут объединены в индивидуальные рабочие группы.

Для того, чтобы начать создание одноранговой сети для рабочей группы, запустите «Мастер настройки сети», выполните следующие действия на

одном компьютере каждой сети:

Щелкните **Пуск**, затем щелкните **Панель управления**.

Щелкните **Сетевые подключения**, а затем на правой панели щелкните **Установить домашнюю сеть или сеть малого офиса**.

На странице **Мастер настройки сети** щелкните **Далее**.

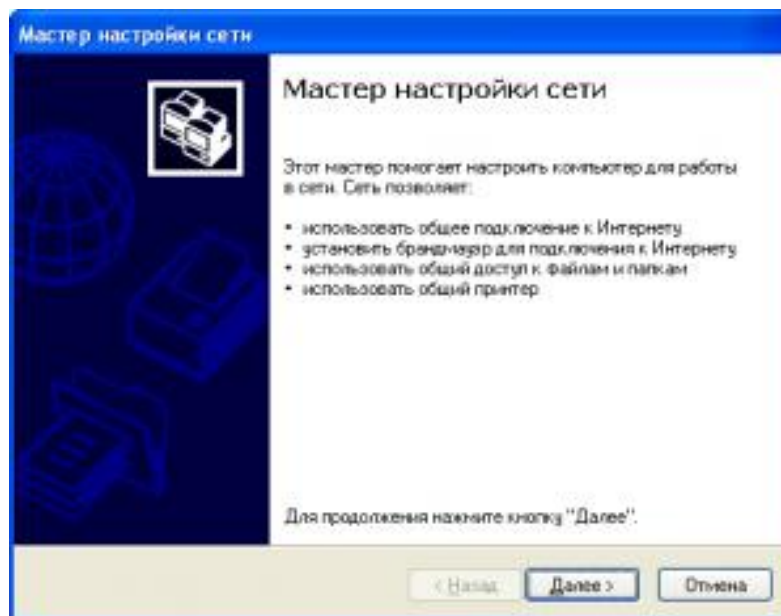


Рисунок 4.2 – Мастер настройки сети

На следующей странице просмотрите требования и, убедившись, что все соответствует, щелкните **Далее**.

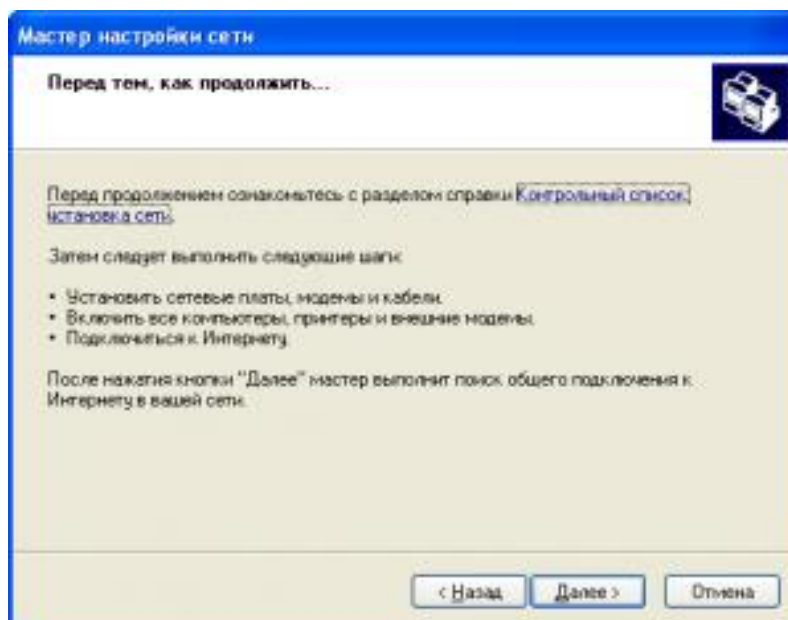


Рисунок 4.3 – Первый шаг мастера

На странице **Выберите метод подключения** щелкните **Другое** и затем щелкните **Далее**.

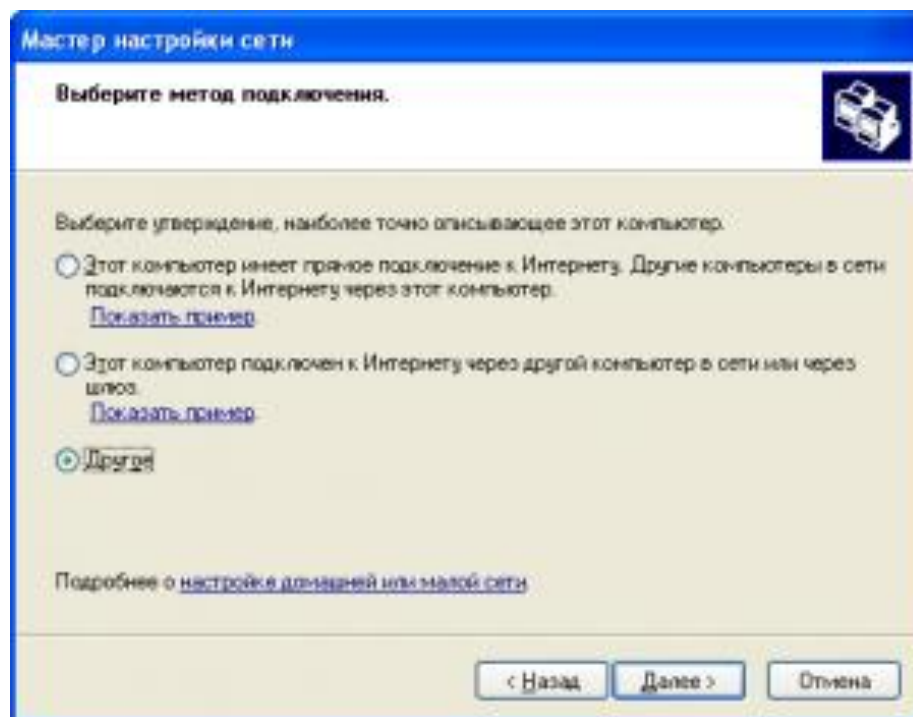


Рисунок 4.4 – Выбор метода подключения

На странице **Другие способы подключения к Интернету** щелкните **Этот компьютер принадлежит к сети, не имеющей подключения к Интернету**, затем щелкните **Далее**.

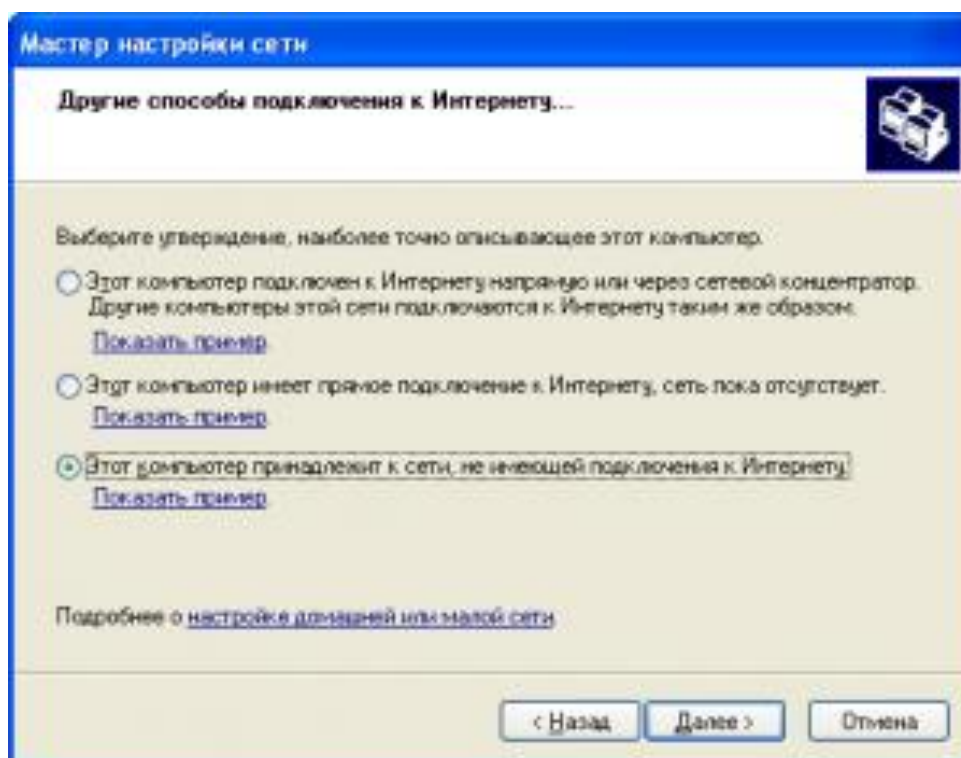


Рисунок 4.5 – Выбор метода подключения

В текстовое поле **Описание** введите workstation

В текстовое поле **Имя компьютера** введите уникальное имя (напри-

мер: STUDENTA), называя тем самым свою рабочую станцию в сети, а затем щелкните **Далее**.

Замечание: Когда вы даете имя своему компьютеру, убедитесь, что это имя уникально в данной рабочей группе. Именуйте компьютеры последовательно, например, StudentB, StudentC, StudentD и так далее.

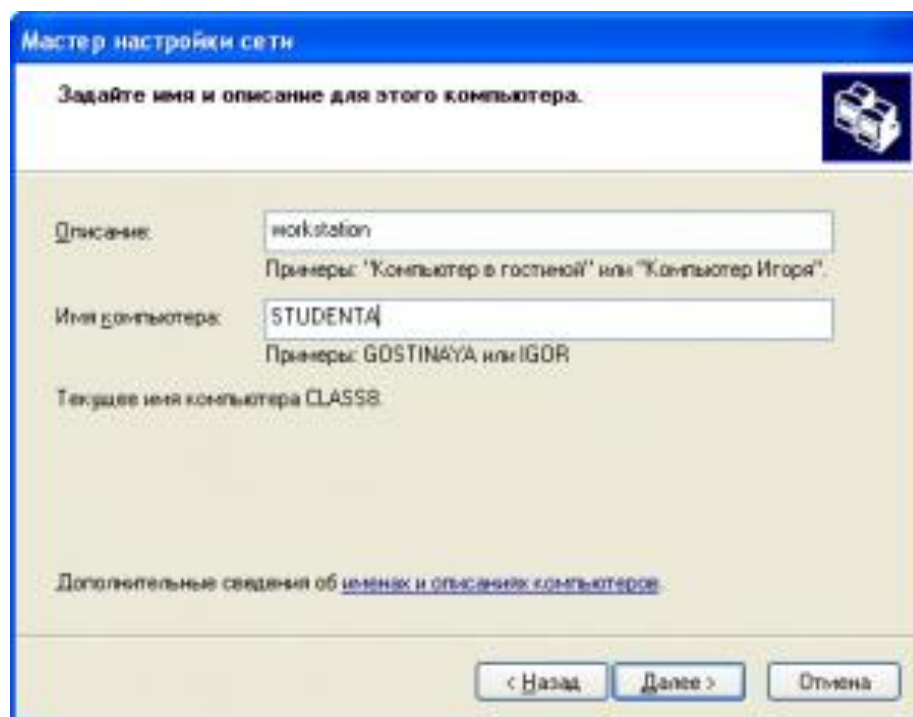


Рисунок 4.6 – Задание имя компьютера

На странице **Задайте имя для вашей сети** смените стандартное имя **Рабочей группы** например mynetwork.

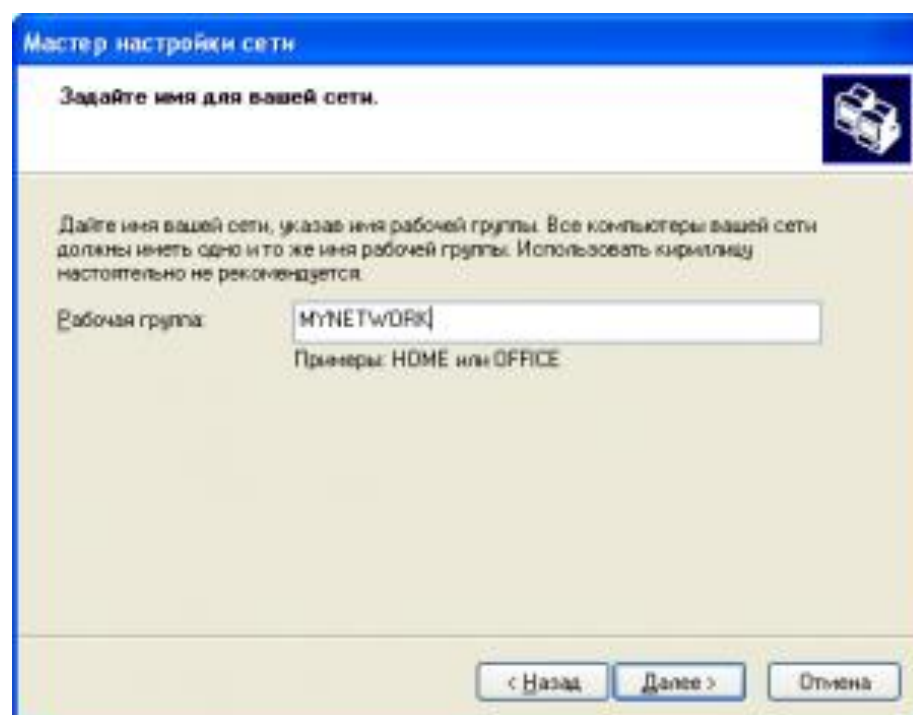


Рисунок 4.7 – Задание имени сети

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

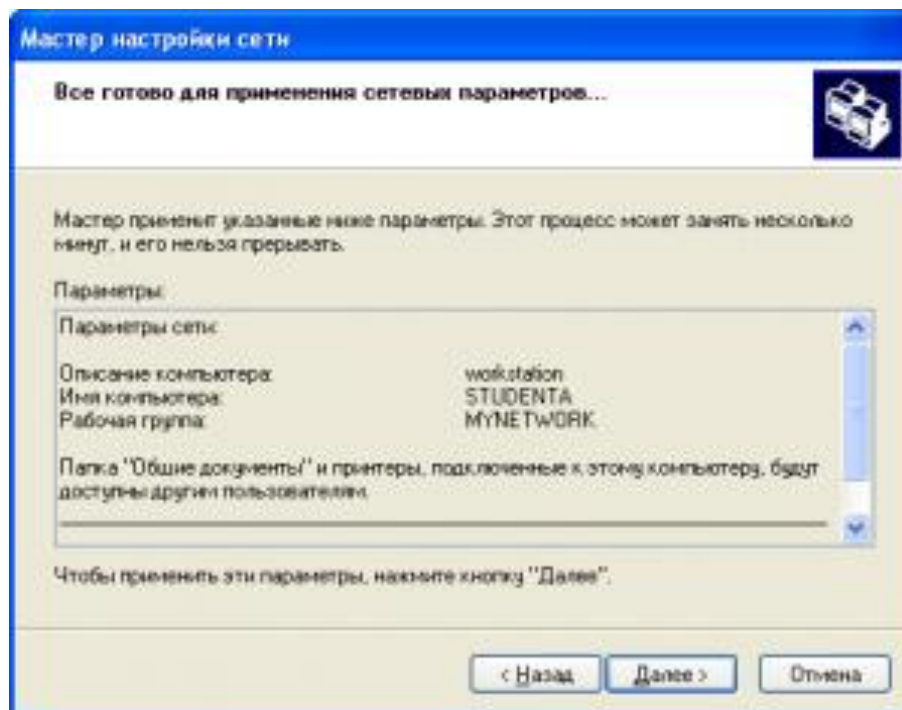


Рисунок 4.8 – Проверка заданных параметров

На следующей странице щелкните **Просто завершить работу мастера**, а затем щелкните **Далее**.

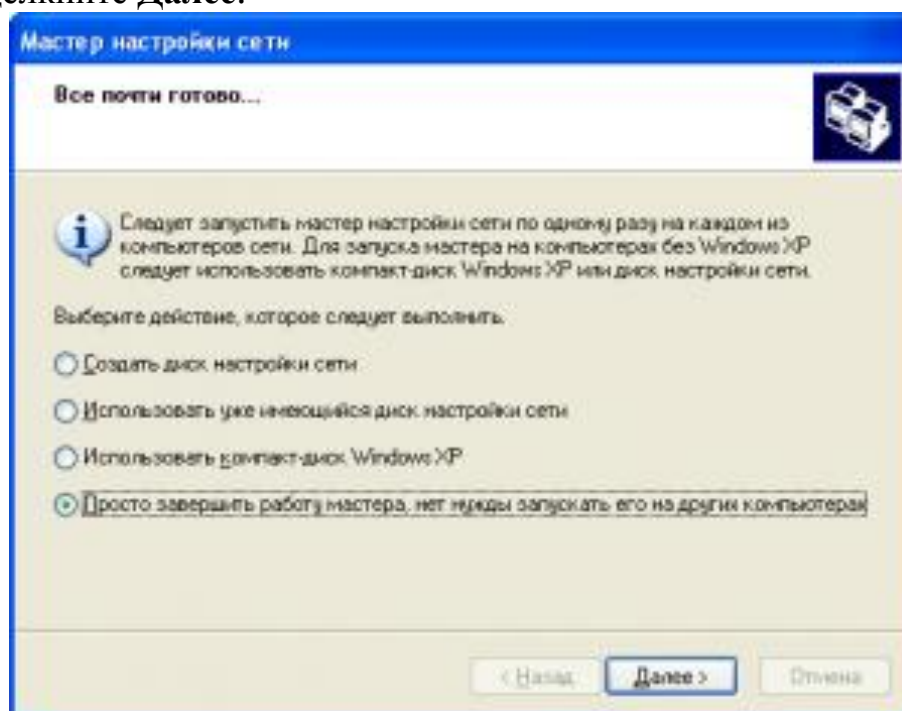


Рисунок 4.8 – Проверка заданных параметров

На странице **Завершение работы мастера настройки сети** щелкните **Готово**.

Если вам будет предложено перезагрузить ваш компьютер, то щелкните **Да**.

Начните работу на своем компьютере.

Пусть учащиеся запустят «**Мастер настройки сети**» (шаги с 3 по 13) на остальных компьютерах в каждой сети, чтобы подключить их к рабочей группе **MUNETWORK**

Для проверки работы одноранговой сети необходимо создать папку для совместного использования на каждом компьютере.

Щелкните **Пуск**, отметьте **Все программы**, щелкните **Стандартные**, и затем щелкните **Проводник**.

На левой панели щелкните **Мои документы**.

В открывшемся окне щелкните **Файл**, затем отметьте **Создать**, и щелкните **Папка**.

Введите Имя папки, которое состоит из вашего имени и слова **Папка** (например: Папка Миши), и нажмите **Enter**.

В окне **Мои документы** щелкните правой кнопкой мыши по только что созданной папке и выберите пункт меню **Общий доступ и безопасность**.

Во вкладке **Доступ** щелкните **Открыть общий доступ к этой папке** и нажмите

В правой половине открывшегося окна дважды щелкните по только что созданной папке.

В открывшемся окне щелкните **Файл**, отметьте **Создать** и щелкните **Текстовый документ**.

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

Дождитесь, пока остальные учащиеся создадут файлы в директории для совместного использования.

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

Щелкните **Пуск**, отметьте **Все программы**, щелкните **Стандартные**, а затем щелкните на **Проводник**.

На левой панели щелкните **Сетевое окружение**, а затем щелкните **Отобразить компьютеры рабочей группы**.

Замечание: теперь вы можете увидеть список компьютеров рабочей группы сети **MUNETWORK**.

На правой панели дважды щелкните по какому-либо компьютеру (не своему) для того, чтобы найти файлы, созданные другими студентами для совместного пользования.

На правой панели дважды щелкните по одной из созданных папок для получения доступа к файлам, созданным другими студентами

На правой панели дважды щелкните по имени файла, чтобы открыть

его. Итак, вы получили удаленный доступ к файлам на другом компьютере.

Содержание отчета

1. Тема работы.
2. Цель работы.
3. Скриншоты основных этапов создания сети.

5 ОСНОВЫ IP - АДРЕСАЦИИ

Цель работы

Научится решать следующие задачи:

1. Идентифицировать 5 различных классов IP-адресов.
2. Описывать характеристики и использование классов IP-адресов.
3. Определять класс IP-адреса исходя из его значения.
4. Определять, какая часть IP-адреса идентифицирует сеть (network ID) и какая – хост (host ID).
5. Определять допустимые и недопустимые IP- адреса хостов, исходя из правил адресации.
6. Определять диапазон адресов и маску подсети по умолчанию для каждого класса адресов.

Ход работы

Задание 1. Изучить теоретические основы IP-адресации

1. Сколько октетов в IP - адресе?
2. Сколько битов в октете?
3. Сколько бит в маске подсети?
4. В каких диапазонах десятичных и двоичных значений может быть значение первого октета IP-адресов класса «В»?

Десятичные: от **128** до **191**

Двоичные: от **1000 0000** до **1011 1111**

5. Какие октеты представляют сетевую часть IP-адреса класса «С»
6. Какие октеты представляют часть адреса хоста в IP-адресе класса «А»?
7. Какой из приведенных ниже адресов является примером широковещательного адреса для сети класса В?

147.1.1.1
147.255.255.255
147.13.0.0
147.14.255.255

Заполните таблицу:

Таблица 5.1 – характеристики классов IP адресации.

Класс адреса	Старшие биты первого октета	Диапазон дес. значений первого октета	Network / Host ID (N=Network, H=Host)	Маска подсети по умолч.	Кол-во сетей	Количество хостов (используемых адресов) в сети
A	0	1-126 (Значение 127 зарезервировано для организации внутренней петли устройств, которая используется при тестировании)	N.N.N.N	255.0.0.0	126	16777214
B	10	128-191	N.N.N.N	255.255.0.0	64	65534
C	110	192-223	N.N.N.N	255.255.255.0	32	254
D	1110	224-239	N.N.N.N		Используется для мультикастинга.	
E	11110	240-255	N.N.N.N		Зарезервирован для экспериментальных целей.	

Задание 2. Определение частей IP- адресов.

Заполнить таблицу об идентификации различных классов IP-адресов.

Таблица 5.2 – Идентификация различных классов IP-адресов

IP- адреса хостов	Класс адреса	Адрес сети	Адреса хостов	Широковещательный (broadcast) адрес	Маска подсети по умолчанию
216.14.55.137					
123.1.1.15					
150.127.221.244					
194.125.35.199					
175.12.239.244					

Разбить каждую сеть на две подсети, вычислить диапазон каждой, адрес подсети, подкаст.

Дан IP- адрес 142.226.0.15

Чему равен двоичный эквивалент второго октета?

Какому классу принадлежит этот адрес?

Чему равен адрес сети, в которой находится хост с этим адресом?
Является ли этот адрес хоста допустимым в классической схеме адресации?

Задание 3

Найти адрес сети, минимальный IP, максимальный IP и число хостов по IP-адресу и маске сети:

IP-адрес: 192.168.215.89 Маска: 255.255.255.0 /24

Задание 4

Что произойдет с данными из 1 задачи, если маску сети изменить на 255.255.255.128

Задание 5

Найти маску сети, минимальный IP, максимальный IP по IP-адресу и адресу сети: IP-адрес: 124.165.101.45 Сеть: 124.128.0.0

Задание 6

Найти минимальный IP, максимальный IP по адресу сети и маске:

Маска: 255.255.192.0 Сеть: 92.151.0.0

Задание 7

Найти адрес сети, минимальный IP, максимальный IP и число хостов по IP-адресу и маске сети: IP-адрес: 85.45.5.33 Маска: 255.252.0.0

Содержание отчета

1. Идентификация 5 различных классов IP-адресов – таблица 5.1.
2. Описание характеристики и использование классов IP-адресов - таблица 6.2.
3. Определение класса IP-адреса исходя из его значения.
4. Определение допустимых и недопустимых IP- адресов хостов, исходя из правил адресации.
5. Определение диапазона адресов и масок подсети по умолчанию для каждого класса адресов.
6. Решения задач.

6 ИЗУЧЕНИЕ СЕТЕВОГО УРОВНЯ МОДЕЛИ OSI НА ПРИМЕРЕ ПРОТОКОЛА IP

Цель работы

Изучить правила адресации сетевого уровня, научиться распределять адреса между участниками сети передачи данных и организовывать маршрутизацию между сегментами сети

Теоретические сведения

Сетевой уровень модели OSI

Сетевой уровень отвечает за возможность доставки пакетов по сети передачи данных – совокупности сегментов сети, объединенных в единую сеть любой сложности посредством узлов связи, в которой имеется возможность достижения из любой точки сети в любую другую.

В связи с необходимостью перенаправлять пакеты из одного сегмента сети в другой, сетевые адреса должны удовлетворять следующим требованиям:

- Адреса должны быть уникальны. В сети не может быть нескольких участников с одинаковыми адресами во избежание неоднозначности.
- Сетевой адрес должен содержать информацию о том, как достичь получателя по сети.

Это приводит к структурности адреса – адрес разбивается на части, позволяющие определить местоположение участника внутри сети.

Структура может быть сложной многоуровневой, например адрес содержит информацию о стране, области, населенном пункте, предприятии, здании, отделе и т.д. или простой, содержащей номер сети и номер компьютера в сети.

По сложной структуре легче построить маршрут прохождения пакета, но адрес оказывается сложным и перегруженным часто ненужной информацией. Примером такой адресации может служить доменная адресация в Интернет, по адресу `asu.bru.mogilev.by` нетрудно понять, где находится данный участник сети и как до него добраться.

Простая структура позволяет значительно сократить размер адреса и сохраняет возможность работы в сети любой структуры, но для этого могут потребоваться сложные и, часто, не столь очевидные алгоритмы, как в предыдущем случае.

Протокол IP (Internet Protocol)

Архитектуру сетевого уровня удобно рассматривать на примере сетевого протокола IP – самого распространенного в настоящее время, основного протокола сети Интернет. Термин «стек протоколов TCP/IP» означает «набор протоколов, связанных с IP и TCP(протоколом транспортного уровня)».

Архитектура протоколов TCP/IP предназначена для объединенной сети, состоящей из соединенных друг с другом шлюзами отдельных разнородных

пакетных подсетей, к которым подключаются разнородные машины.

Каждая из подсетей работает в соответствии со своими специфическими требованиями и имеет свою природу средств связи. Однако предполагается, что каждая подсеть может принять пакет информации (данные с соответствующим сетевым заголовком) и доставить его по указанному адресу в этой конкретной подсети.

Не требуется, чтобы подсеть гарантировала обязательную доставку пакетов и имела надежный сквозной протокол.

Таким образом, две машины, подключенные к одной подсети, могут обмениваться пакетами.

Когда необходимо передать пакет между машинами, подключенными к разным подсетям, то машина-отправитель посылает пакет в соответствующий шлюз (шлюз подключен к подсети также как обычный узел). Оттуда пакет направляется по определенному маршруту через систему шлюзов и подсетей, пока не достигнет шлюза, подключенного к той же подсети, что и машина-получатель: там пакет направляется к получателю.

Таким образом, адрес получателя должен содержать в себе:

- номер (адрес) подсети;
- номер (адрес) участника (хоста) внутри подсети.

IP адреса представляют собой 32-х разрядные двоичные числа. Для удобства их записывают в виде четырех десятичных чисел, разделенных точками. Каждое число является десятичным эквивалентом соответствующего байта адреса (для удобства будем записывать точки и в двоичном изображении).

192.168.200.47 является десятичным эквивалентом двоичного адреса
11000000.10101000.11001000.00101111

Иногда применяют десятичное значение IP-адреса. Его легко вычислить

$$192 \cdot 256 + 168 \cdot 256 + 200 \cdot 256 + 47 = 3232286767$$

или с помощью метода Горнера :

$$(((192 \cdot 256) + 168) \cdot 256 + 200) \cdot 256 + 47 = 3232286767$$

Таблица 6.1 - Перевод некоторых чисел из двоичной системы счисления в десятичную и обратно.

Двоичное	Десятичное
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252

11111110	254
11111111	255

Количество разрядов адреса подсети может быть различным и определяется маской сети.

Маска сети также является 32-х разрядным двоичным числом. Разряды маски имеют следующий смысл:

1. если разряд маски равен 1, то соответствующий разряд адреса является разрядом адреса подсети,
2. если разряд маски равен 0, то разрядом хоста внутри подсети.

Все единичные разряды маски (если они есть) находятся в старшей (левой) части маски, а нулевые (если они есть) – в правой (младшей).

Исходя из вышесказанного, маску часто записывают в виде числа единиц в ней содержащихся.

255.255.248.0 (11111111.11111111.11111000.00000000) –

является правильной маской подсети (/21), а

255.255.250.0 (11111111.11111111.11111010.00000000) –

является неправильной, недопустимой.

Нетрудно увидеть, что максимальный размер подсети может быть только степенью двойки (двойку надо возвести в степень, равную количеству нулей в маске).

При передаче пакетов используются правила маршрутизации, главное из которых звучит так: «Пакеты участникам своей подсети доставляются напрямую, а остальным – по другим правилам маршрутизации».

Таким образом, требуется определить, является ли получатель членом нашей подсети или нет.

Определение диапазона адресов подсети.

Определение диапазона адресов подсети можно произвести из определения понятия маски:

1. те разряды, которые относятся к адресу подсети, у всех хостов подсети должны быть одинаковы;
2. адреса хостов в подсети могут быть любыми.

То есть, если наш адрес 192.168.200.47 и маска равна /20, то диапазон можно посчитать:

11000000.10101000.11001000.00101111 – адрес

11111111.11111111.11110000.00000000 – маска

11000000.10101000.1100XXXX.XXXXXXXX – диапазон адресов

где 0,1 – определенные значения разрядов,

X – любое значение,

Что приводит к диапазону адресов:

от

11000000.10101000.11000000.00000000 (192.168.192.0)

до

11000000.10101000.11001111.11111111 (192.168.207.255)

Следует учитывать, что некоторые адреса являются запрещенными или служебными и их нельзя использовать для адресов хостов или подсетей. Это адреса, содержащие:

- 0 в первом или последнем байте,
- 255 в любом байте (это широковещательные адреса),
- 127 в первом байте (внутренняя петля – этот адрес имеется в каждом хосте и служит для связывания компонентов сетевого уровня).

Поэтому доступный диапазон адресов будет несколько меньше.

Диапазон адресов:

- 10.X.X.X – для больших локальных сетей;
- 172.16.X.X – для больших локальных сетей, но применяется реже,
- 192.168.X.X – для маленьких (небольших) локальных сетей,

не может быть использован в сети Internet, т.к. отданы для использования в сетях непосредственно не подключенных к глобальной сети.

Команда ipconfig

Команда ipconfig отображает краткую информацию, т.е. только IP-адрес, маску подсети и стандартный шлюз для каждого подключенного адаптера, для которого выполнена привязка с TCP/IP.

2. Решить задачи.

1. Какие адреса из приведенного ниже списка являются допустимыми адресами хостов и почему:

- 0.10.10.10
- 10.0.10.10
- 10.10.0.10
- 10.10.10.10
- 127.0.127.127
- 127.0.127.0
- 255.0.200.1
- 1.255.0.0

2. Перечислите все допустимые маски, по какому принципу они получаются.

3. Определите диапазоны адресов подсетей (даны адрес хоста и маска подсети):

- 10.212.157.12/24
- 27.31.12.254/31
- 192.168.0.217/28
- 10.7.14.14/16

4. Какие из адресов

- 241.253.169.212
- 243.253.169.212
- 242.252.169.212

242.254.169.212

242.253.168.212

242.253.170.212

242.253.169.211

242.253.169.213

будут достигнуты напрямую с хоста

242.254.169.212/21.

Определите диапазон адресов в его подсети.

5. Посмотрите параметры IP на своем компьютере с помощью команды `ipconfig`. Определите диапазон адресов и размер подсети, в которой Вы находитесь. Попробуйте объяснить, почему выбраны такие сетевые параметры и какие сетевые параметры выбрали бы Вы.

Контрольные вопросы

1. Чем занимается сетевой уровень?
2. Что такое сеть передачи данных?
3. Какие требования предъявляются к сетевой адресации?
4. Можно ли использовать в качестве сетевого MAC-адрес?
5. Что такое маска подсети?
6. Какова структура IP-адреса?
7. Чем определяется размер подсети?
8. Как определить диапазон адресов в подсети?
9. Как определить размер подсети?

7 СЕТЕВЫЕ УТИЛИТЫ ОС WINDOWS

Цель работы

Изучить утилиты командной строки Windows, предназначенные для контроля и мониторинга сетей, построенных на базе стека протоколов TCP/IP.

Теоретические сведения

Сетевая операционная система Windows содержит набор утилит, полезных при диагностике сети. Основными задачами этих программ является:

- Определение работоспособности сети
- Определение параметров и характеристик сети
- В случае неправильного функционирования сети – локализация службы или сервиса, вызывающих неисправность.

Главными параметрами сетевых подключений являются их канальные и сетевые адреса и параметры, влияющие на работу сетевого уровня.

Единственным параметром канального уровня, который может быть просмотрен, являются MAC адреса сетевых адаптеров. Для их просмотра можно воспользоваться утилитой IPCONFIG, которая покажет MAC адреса для каждого адаптера, или, для последних версий Windows, с помощью ROUTE PRINT. Для изменения MAC адресов следует воспользоваться драйверами соответствующих сетевых адаптеров, если, конечно, они допускают подобную операцию.

1 IPCONFIG

Параметры IP просматривают с помощью утилиты IPCONFIG.

Использование:

```
ipconfig [/? | /all | /release [адаптер] | /renew [адаптер] |  
/flushdns | /displaydns /registerdns |  
/showclassidaдаптер |  
/setclassid адаптер [устанавливаемый_код_класса_dhcp] ]
```

Параметры:

адаптер – полное имя или имя, содержащие подстановочные знаки «*» и «?» (* – любое количество знаков, ? – один любой знак). См. примеры ключи:

/? – отобразить это справочное сообщение.

/all – отобразить полную информацию о настройке параметров.

/release – освободить IP-адрес для указанного адаптера.

/renew – обновить IP-адрес для указанного адаптера.

/flushdns – очистить кэш разрешений DNS.

/registerdns – обновить все DHCP-аренды и перерегистрировать DNS-имена

/displaydns – отобразить содержимое кэша разрешений DNS.

/showclassid – отобразить все допустимые для этого адаптера коды (IDs) DHCP-классов.

/setclassid – изменить код (ID) DHCP-класса.

По умолчанию отображается только IP-адрес, маска подсети и стандартный шлюз для каждого подключенного адаптера, для которого выполнена привязка с TCP/IP.

Для ключей /release и /renew, если не указано имя адаптера, то будет освобожден или обновлен IP-адрес, выданный для всех адаптеров, для которых существуют привязки с TCP/IP.

Для ключа /setclassid, если не указан код класса (ID), то существующий код класса будет удален.

Примеры:

ipconfig – отображает краткую информацию.

Настройка протокола IP для Windows

Подключение по локальной сети 2 – Ethernet адаптер:

DNS-суффикс этого подключения . . . :

IP-адрес автонастройки. : 169.254.236.138

Маска подсети : 255.255.0.0

Основной шлюз :

Main – PPP адаптер:

DNS-суффикс этого подключения . . . :

IP-адрес. : 82.209.222.238

Маска подсети : 255.255.255.255

Основной шлюз : 82.209.222.238

ipconfig /all – отображает полную информацию.

Настройка протокола IP для Windows

Имя компьютера. : home

Основной DNS-суффикс. :

Тип узла. : неизвестный

IP-маршрутизация включена . . . : нет

WINS-прокси включен : нет

Подключение по локальной сети 2 – Ethernet адаптер:

DNS-суффикс этого подключения . . . :

Описание. : Realtek RTL8029(AS)-based

Ethernet адаптер (Универсальный) #2

Физический адрес. : 52-54-05-E2-77-88

Dhcp включен. : да

Автонастройка включена. : да

IP–адрес автонастройки. : 169.254.236.138
Маска подсети : 255.255.0.0
Основной шлюз :

Main – PPP адаптер:

DNS–суффикс этого подключения . . . :
Описание. : WAN (PPP/SLIP) Interface
Физический адрес. : 00–53–45–00–00–00
Dhcp включен. : нет
IP–адрес. : 82.209.222.238
Маска подсети : 255.255.255.255
Основной шлюз : 82.209.222.238
DNS–серверы : 194.158.206.206
193.232.248.2
NetBIOS через TCP/IP. : отключен

ipconfig /renew– обновляет сведения для всех адаптеров.

ipconfig /renew EL* – обновляет сведения для адаптеров, начинающихся с EL

ipconfig /release *ELINK?21* – освобождает IP–адреса для всех адаптеров, имена которых удовлетворяют запросу: ELINK–21 или myELELINKi21adapter и т.п.

2 ARP

Соответствие MAC и IP адресов производится службой ARP. Для работы с этой службой имеется утилита ARP.

Служба ARP работает с таблицей ARP, состоящей из двух колонок: IP адрес и MAC адрес (физический адрес). При необходимости отправить пакет по какому–то IP адресу в таблице ARP находят соответствующий ему MAC адрес и на канальном уровне передают информацию. Если передача производится через шлюз, то в таблице ищут MAC адрес шлюза и передают пакет с IP адресом получателя и MAC адресом шлюза.

Если в таблице ARP нет нужного IP адреса, то посылается запрос – специальный пакет ARP по IP адресу получателя с широковещательным MAC адресом. Получатель, получив такой пакет, посылает ответ от своего IP адреса и своего MAC адреса. Отправитель, получив этот ответ, добавляет запись в ARP таблицу.

Таблица ARP динамическая, поэтому запись в ней «живет» некоторое время, после которого удаляется, но имеется возможность создавать в таблице и постоянные (статические) записи.

Отображение и изменение таблиц преобразования IP–адресов в физические, используемые протоколом разрешения адресов (ARP).

Использование:

ARP –s inet_addr eth_addr [if_addr]

```
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]
```

Параметры:

–a – отображает текущие ARP–записи, опрашивая текущие данные протокола. Если задан `inet_addr`, то будут отображены IP и физический адреса только для заданного компьютера. Если более одного сетевого интерфейса используют ARP, то будут отображаться записи для каждой таблицы.

–g – то же, что и ключ –a.

`inet_addr` – определяет IP–адрес.

–N `if_addr` – отображает ARP–записи для заданного в `if_addr` сетевого интерфейса.

–d – удаляет узел, задаваемый `inet_addr`. `inet_addr` может содержать символ шаблона * для удаления всех узлов.

–s – добавляет узел и связывает интернет адрес `inet_addr` с физическим адресом `eth_addr`. Физический адрес задается 6 байтами (в шестнадцатеричном виде), разделенных дефисом. Эта связь является постоянной.

`eth_addr` – определяет физический адрес.

`if_addr` – если параметр задан – он определяет интернет адрес интерфейса, чья таблица преобразования адресов должна измениться. Если не задан – будет использован первый доступный интерфейс.

Пример:

`arp -s 157.55.85.212 00-aa-00-62-c6-09` – добавляет статическую запись.

`arp -a` – выводит ARP–таблицу.

3 **Протокол ICMP**

Для мониторинга и управления сетями передачи данных разработан и используется протокол ICMP. На его базе можно:

1. Проверить доступность адресов сети
2. Определить маршрут
3. Определить время достижения пакетами узлов сети.

Решается это посылкой специальных пакетов.

Опции маршрутизации и временных меток являются весьма интересными, так как они обеспечивают способ наблюдения или управления тем, как межсетевые шлюзы маршрутизируют дейтаграммы.

Опция запись маршрута позволяет источнику создать пустой список IP–адресов и заставить каждый шлюз, обрабатывающий дейтаграмму, добавлять свой IP–адрес к этому списку. Всякий раз, когда машина обрабатывает дейтаграмму, имеющую опцию записи маршрута, она добавляет свой адрес к списку записи маршрута (в опции должно быть выделено достаточно места исходным отправителем для того, чтобы поместились все нужные элементы).

При прибытии дейтаграммы машина–получатель должна выделить и

обработать список IP–адресов.

Если получатель обрабатывает дейтаграмму обычным образом, он будет игнорировать записанный путь.

Отметим, что отправитель должен разрешить наличие опции записи маршрута, а получатель должен быть согласен обработать полученный список; сама по себе машина не получит автоматически информацию о пройденном пути автоматически, если она включит опцию записи маршрута.

Опция временных меток работает аналогично опции записи маршрута в том отношении, что опция временных меток содержит вначале пустой список, а каждый шлюз на всем протяжении пути от источника к назначению заполняет элемент в этом списке.

Каждый элемент в списке состоит из двух 32–битных частей: IP–адреса шлюза, заполнившего этот элемент, и 32–битового целого числа – временной метки.

Временные метки определяют время и дату, когда шлюз обрабатывал дейтаграмму, и выражаются в миллисекундах после полуночи по Гринвичу. Если стандартное представление времени невозможно, шлюз может использовать любое представление локального времени.

4 TRACERT

Для оценки маршрута прохождения пакетов используют утилиту TRACERT (tracert)

В отличие от PING на пробные пакеты постоянного размера отвечает каждый узел, через который этот пакет проходит. Программа измеряет и показывает время между отправкой пакета и получением ответа.

Использование:

tracert [-d] [-h максЧисло] [-j списокУзлов] [-w интервал] имя

Параметры:

–d – без разрешения в имена узлов.

–h максЧисло – максимальное число прыжков при поиске узла.

–j списокУзлов – свободный выбор маршрута по списку узлов.

–w интервал – интервал ожидания каждого ответа в миллисекундах.

Примеры:

tracert www.lycos.com

Трассировка маршрута к mia–search.mia.lycos.com [209.202.248.101]
с максимальным числом прыжков 30:

1 136 ms 149 ms 149 ms 194.158.206.83

2 136 ms 209 ms 139 ms 194.158.206.197

3 164 ms 149 ms 149 ms 193.232.249.18

4 132 ms 149 ms 219 ms 193.232.248.128

```

5 160 ms 149 ms 169 ms80.77.105.197
6 158 ms 149 ms 149 mssl-bb21-sto-8-0.sprintlink.net [80.77.96.41]
7 185 ms 159 ms 189 mssl-bb21-cop-12-0.sprintlink.net
[213.206.129.33]
8 163 ms 159 ms 189 mssl-bb20-cop-15-0.sprintlink.net [80.77.64.33]
9 270 ms 269 ms 229 mssl-bb21-msq-10-0.sprintlink.net
[144.232.19.29]
10 257 ms 249 ms 259 mssl-bb20-msq-15-0.sprintlink.net
[144.232.9.109]
11 235 ms 249 ms 249 mssl-bb25-nyc-6-0.sprintlink.net
[144.232.20.75]
12 232 ms 239 ms 252 mssl-bb21-nyc-15-0.sprintlink.net
[144.232.13.2]
13 239 ms 239 ms 299 mssl-bb23-nyc-3-0.sprintlink.net
[144.232.7.109]
14 246 ms 239 ms 339 mssl-gw31-nyc-0-0.sprintlink.net
[144.232.13.32]
15 244 ms 249 ms 259 mssl-tiws-2-0.sprintlink.net [144.232.230.2]
16 296 ms 319 ms 279 msSo7-2-0-0-grtmiabr4.red.telefonica-
wholesale.net[213.140.38.254]
17 296 ms 289 ms 299 msSo2-0-0-0-grtmiana2.red.telefonica-
wholesale.net[213.140.36.89]
18 274 ms 289 ms 299 msteusa-7-3-0-0-grtmiana2.red.telefonica-
wholesale.net[213.140.39.50]
19 271 ms 298 ms 299 ms66.119.71.166
20 283 ms 319 ms 279 msmia-search.mia.lycos.com [209.202.248.101]

```

Трассировка завершена.

TRACERT позволяет обнаружить некоторые ошибки маршрутизации в сети. Такими ошибками являются отсутствие правила маршрутизации в каком либо шлюзе, или петля маршрутов по умолчанию.

Пример отсутствия правила на узле:
tracert 10.249.0.100
Трассировка маршрута к 10.249.0.100
с максимальным числом прыжков 30:

```

1 13 ms 14 ms 14 ms10.7.11.11
2 * * *Сеть недоступна [10.7.11.11]
Трассировка завершена.

```

Пример петли маршрутизации:

```
tracert 10.250.0.100
```

Трассировка маршрута к 10.250.0.100
с максимальным числом прыжков 30:

```
1 13 ms 14 ms 14 ms 10.7.11.11
2 18 ms 17 ms 17 ms 10.7.10.11
3 19 ms 18 ms 24 ms 10.7.11.11
4 28 ms 14 ms 19 ms 10.7.10.11
5 23 ms 14 ms 22 ms 10.7.11.11
6 19 ms 16 ms 33 ms 10.7.10.11
```

...

Хорошо видно, что шлюз 10.7.11.11 посылает пакет на 10.7.10.11, а 10.7.11.11 на 10.7.10.11. Это возможно, если либо для сети, к которой принадлежит адрес 10.250.0.100 неправильно прописаны правила маршрутизации, либо неправильно прописана маршрутизация по умолчанию на одном или обоих узлах.

5 NSLOOKUP

Имеется специальная служба, сопоставляющая доменные адреса Интернет с IP адресами – DNS (domainnameservice). Для проверки ее работоспособности используют утилиту NSLOOKUP. Для работы этой утилиты должен быть определен сервер DNS в параметрах IP компьютера. С его помощью и будет производиться распознавание имен.

Использование:

```
nslookup [-подкоманда ...] [{искомый_компьютер| [-сервер]}]
```

Параметры:

–подкоманда ... – задает одну или несколько подкоманд nslookup как параметры командной строки.

искомый_компьютер – ищет данные для параметра искомый_компьютер, используя текущий, заданный по умолчанию сервер имен DNS, если никакого другого сервера не указано

–сервер – указывает, что данный сервер следует использовать в качестве сервера имен DNS. Если параметр –сервер не указан, используется сервер DNS, заданный по умолчанию.

–help|? – Выводит краткое описание подкоманд nslookup.

Пример:

```
nslookup
```

```
Default Server:mail.mogilev.by
```

```
Address:194.158.206.206
```

```
> lycos.com
```

```
Server:mail.mogilev.by
```

```
Address:194.158.206.206
```

Non-authoritative answer:

Name:lycos.com

Address:209.202.248.101

> hp.com

Server:mail.mogilev.by

Address:194.158.206.206

DNS request timed out.

timeout was 2 seconds.

Non-authoritative answer:

Name:hp.com

Addresses:192.6.234.8, 192.6.234.9, 192.6.234.10, 192.151.52.187
161.114.22.105

> bru.mogilev.by

Server:mail.mogilev.by

Address:194.158.206.206

Name:bru.mogilev.by

Address:82.209.221.110

>exit

Задания для самостоятельного выполнения

1. Используя утилиту PING определить пропускную способность сети до адресов 192.168.0.1, 192.168.0.201, 192.168.0.254, 192.168.1.1. Объясните разницу в результатах.
2. Используя утилиту TRACERT и таблицу маршрутизации (адрес server.af), постройте схему сеть филиала.
3. Передайте пакеты участникам сети напрямую и через шлюз. Объясните полученные записи в таблице ARP.
4. Определите IP адреса: www.microsoft.com, www.hp.com, www.tut.by, ftp.cdrom.ru при помощи утилиты NSLOOKUP.

Контрольные вопросы

1. Для чего используется утилита PING?
2. Как с помощью утилиты PING оценить пропускную способность сети? Объясните формулу.
3. Что такое петля маршрутизации?
4. Как выглядят правила маршрутизации, образующие петлю?
5. Зачем нужна таблица ARP?
6. Объясните разницу во времени между обращениями к одному и тому же хосту по имени и IP адресу.
- 7.

Содержание отчета

Тема, цель, описание выполнения заданий с иллюстрациями, ответы на контрольные вопросы

8 ПРОТОКОЛЫ ВЫСШИХ УРОВНЕЙ МОДЕЛИ OSI

Цель работы

Ознакомиться с принципами работы текстовых протоколов высших уровней на примере протоколов электронной почты.

Оборудование: персональный компьютер, включенный в сеть; Microsoft Windows; утилита TELNET; сервер электронной почты в сети

Теоретические сведения

Большинство протоколов высших уровней – текстовые – запросы и ответы передаются в виде текста, т.е. в запросах и ответах могут присутствовать только печатные символы.

Во многих протоколах ответы начинаются со специальной строки, состоящей из трехзначного числа и, возможно, текстового описания типа ответа. Трехзначное число разделяется на две части: 1-ый символ рассматривается как код класса сообщения; два последние – как тип сообщения данной важности.

Коды классов следующие:

1 – информационное сообщение. Обычно игнорируется программными клиентами.

2 – удачное завершение запроса. Рассматривается программами-клиентами как успех обработки запроса и обычно игнорируется.

Часто программы-серверы не различают сообщения первого и второго типа, т.е. информационное сообщение проходит по второй категории.

3 – сообщение об удачной обработке запроса, но требующее дополнительных действий клиента.

4 – ошибка со стороны клиента, т.е. клиент послал запрос, который не может обработать сервер вследствие ошибочности или недостаточности данных.

5 – ошибка со стороны сервера. Клиент послал правильный запрос, но сервер не смог его выполнить в силу каких-то причин.

Трехзначные коды ответов очень удобны для программного распознавания, нет необходимости распознавать текст ответа, который, в общем случае, может прийти на разных языках, достаточно распознать только 3 цифры.

Программа TELNET

Для работы с текстовыми протоколами воспользуемся программой TELNET, входящей в состав Windows. Эта программа предназначена для работы с протоколом TELNET, задачей которого является обмен информацией между клиентом и сервером без каких либо преобразований, т.е. организация прозрачного канала между клиентом и сервером.

Синтаксис команды TELNET следующий:

TELNET адрес_сервера [порт]

Если порт не указан, используется 23 - стандартный порт протоко-

ла TELNET.

Протокол SMTP

Для начала попробуем поработать с протоколом SMTP. Обычно он работает, используя порт 25.

Для наглядности команды пользователя выделены красным цветом, а ответы сервера – синим.

Даем команду на подключение:

```
telnet 192.168.200.1 25
```

Получаем ответ

```
220 homeVPOP3 SMTPServerReady
```

Обратите внимание на число 220 в начале строки ответа. Это нормальный ответ, сервер ответил на наш запрос на подключение.

Многие серверы, работающие по текстовым протоколам, поддерживают команду HELP. Проверим.

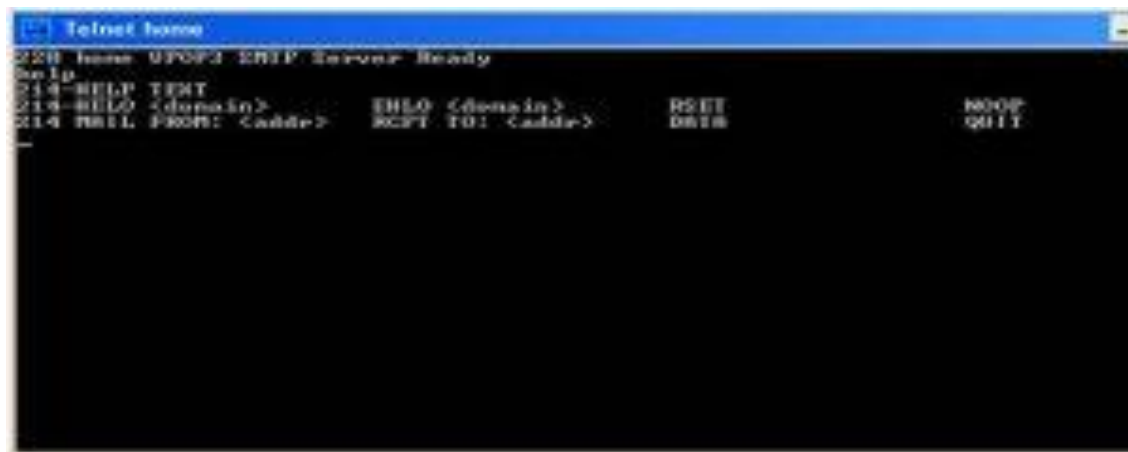


Рисунок 8.1 – Команда Help

Дадим серверу неправильный запрос

```
abrakadabra
```

```
500 Command Unrecognised
```

Как ни странно, но код ответа 5 – ошибка на стороне сервера!

Попробуем написать письмо

Поздороваемся J

```
helo home
```

```
250 home VPOP3 SMTP Server - Hello home, pleased to meet you
```

Укажем отправителя письма

```
mail from: user1
```

```
250 <user1>... Sender ok
```

Укажем получателя письма

```
rcptto: user2
```

```
250 <user2>... Recipient ok
```

Перейдем в режим ввода письма

```
data
```

```
354 Start Mail input, end with <CRLF>.<CRLF>
```

Обратите внимание на код ответа 354.

Это нормальное завершение, но требуются дополнительные данные – само письмо, которое, как видно, должно заканчиваться строкой, состоящей из одной точки «.».

А теперь само письмо. Формат письма описан стандартами. Их изучение не входит в нашу задачу, но наиболее важные служебные строки вкратце рассмотрим:

Date: Tue, 22 Nov 2005 19:55:07 +0200

Дата создания по GMT и часовой пояс

From: User user1@home.my

От кого

Reply-To: User user1@home.my

Кому отвечать

To: user2@home.my

Кому

Subject: Test

Тема письма

MIME-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

Информация почтовой программе, как закодировано письмо – с помощью этих строк почтовая программа клиент сможет реализовать шестой уровень – представить информацию пользователю в читабельном виде

Hello user2,

It's a test message.

Best regards,

User <mailto:user1@home.my>

Само письмо

.

250 OK

Письмо принято!

Теперь выходим

quit

221 home VPOP3 Server Closing Connection

Протокол SMTP (Simple Mail Transfer Protocol) используется для передачи электронной почты от клиента серверу или между серверами. Не содержит встроенных средств идентификации и преобразования.

Протокол POP3

Теперь поработаем с протоколом POP3. Обычно он работает, используя порт 110.

Даем команду на подключение:

telnet 192.168.200.1 25

Получаем ответ

+OK VPOP3 Server Ready <1.7b0.435a37>

Работает, но трехсимвольного кода ответа нет!

Попробуем help

help

-ERR Unrecognised command

Видим, что помощи нет, заодно и посмотрели, как сервер отвечает на ошибочный для него запрос.

Как мы знаем, POP3 требует аутентификации, поэтому представимся:

user user2

+OK User Accepted, PASSword required

А теперь пароль.

pass 2

+OK user2 has 1 message(s) (580 octets)

Нам есть почта! Посмотрим.

list

+OK 1 messages (580 octets)

1 580

Одно письмо 580 символов. Если бы было несколько писем, было бы несколько строк с указанием номеров и размеров писем. Точка в последней строке показывает, что это окончание ответа.

Теперь прочитаем (получим) первое письмо.

retr 1

+OK 580 octets

Received: from 192.168.200.1 by home ([192.168.200.1] running VPOP3)
with SMTP

or <user2>; Tue, 22 Nov 2005 20:31:07 +0200

Date: Tue, 22 Nov 2005 19:55:07 +0200

From: User <user1@home.my>

Reply-To: User <user1@home.my>

To: user2@home.my

Subject: Test

MIME-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

Message-Id: <VPOP31.3.0c.20051122203134.814.e.1.40132205@home>

X-Server: VPOP3 V1.3.0c - Registered to: Collega

Hello user2,

It's a test message.

Best regards,

User <mailto:user1@home.my>

Служебных полей стало больше – их добавил сервер.
Обратите внимание на последнюю строку ответа
Теперь удалим письмо с сервера, ведь оно уже прочитано:
delete 1
+OK message 1 deleted
Проверим, есть ли что еще
list
+OK 0 messages (0 octets)

Ничего нет. А можно и так, для программы это будет более удобным
list 1
-ERR Invalid Message Number
Ну, и теперь выходим
quit
+OK VPOP3 Server Closing Connection

В приведенном выше примере было отправлено письмо от пользователя «user1» пользователю «user2» и получена почта пользователя «user2» с помощью утилиты TELNET, т.е. без использования почтового клиента.

Протокол POP3 (Post Office Protocol) предназначен для получения электронной почты от сервера к клиенту. Содержит средства идентификации клиента, использует факультативные средства преобразования.

Протокол FTR

Протокол FTP (File Transfer Protocol) – протокол передачи файлов.

Он использует 20-ый порт для установления соединений и 21-ый порт для установления соединений и передачи файлов. Этот протокол содержит встроенные средства идентификации клиента. Все распознаваемые им команды состоят из 3-х или 4-х символов, являющихся сокращениями или аббревиатурами выполняемых действий.

```

220 LINUX FTP server (Version 5.60) ready.
help
214 The following commands are recognized (* >): unimplemented).
USER      PORT      STOR      MSNM*     MNT0      NLST      MKD      CMDP      PASSZ
PASS      PASV      APPE      MRSQ*     ADOR      SITE      NMKD      XCUP      CCC
ACCI*     TYPE      MLFL*     MRCF*     DELE      SYST      SPD      STGO      SIZE
SMMT*     STRU      MAIL*     ALLO      CWD      STAT      NSMD      AUTH      NDIR
REIN*     MODE      MSMD*     REST      XCMD      HELP      PWD      ABAT
QUIT      REIR      MSOM*     RMFR      LIST      MOOP      XPWD      FOOT
214 Direct comments to ftp-hugs@LINUX.

```

Риунок8.2 - Протокол НТТР

Протокол HTTP (Hyper Text Transfer Protocol) – протокол передачи гипертекста, т.е. данных разного представления (текст, изображения, видео, звук). Обычно этот протокол работает на 80-ом порту. Он содержит средства идентификации и перекодирования передаваемой информации.

Как видим работа с текстовыми протоколами не представляет особых трудностей. Правда некоторые протоколы содержат большое число команд и чтобы узнать их формат требуется использовать их стандарт и описания RFC.

Задание для самостоятельного выполнения

Во всех заданиях адрес сервера: 10.203.0.120.

Где необходимо требуется пояснить трехсимвольные коды ответов, например, при первом появлении такого кода.

В пятом и шестом заданиях, после аутентификации (если она необходима) рекомендуется в первую очередь вызвать помощь командой help и посмотреть информацию о других командах, поддерживаемых данным протоколом.

Получить у преподавателя адрес сервера электронной почты, имена и пароли пользователей. Отправить и получить почту без использования почтового клиента (для аутентификации использовать имя пользователя типа: user№, тогда паролем будет №, в качестве номера № использовать номер Вашей подгруппы).

Поработать с POP3 без аутентификации. Сделать соответствующие выводы.

Определить, является ли протокол FTP текстово-ориентированным и поддерживает ли он трехсимвольные коды ответов. Подтвердить и объяснить полученные результаты.

Подключиться к HTTP серверу и определить, является ли протокол HTTP текстово-ориентированным и поддерживает ли он трехсимвольные коды ответов. Подтвердить и объяснить полученные результаты.

Получить у преподавателя адрес и порт неизвестного для вас протокола и сервера. Получите список его команд, объясните, что делает каждая команда. Попробовать некоторые из них и проанализировать результаты. (использовать 1000-ый порт, при аутентификации имя пользователя и пароль: admin).

Поработайте с FTP-сервером с помощью TELNET и программы FTP. Объясните и подтвердите на конкретном примере разницу между ними (при аутентификации имя пользователя: anonymous и пароль: а). Для запуска программы FTP в командной строке вызвать ftp>open (узел) 10.203.0.120)

Контрольные вопросы

1. Почему протоколы называются протоколами высших уровней?
2. Почему прием и передача электронной почты производятся по разным протоколам?
3. Почему POP3 требует обязательной аутентификации, а SMTP нет?

4. Как определить окончание письма?
5. Почему для проверки наличия писем удобнее использовать list1 по сравнению с list без параметра?
6. Для чего предназначен данный вам сервер?
7. Является ли его протокол текст-ориентированным?
8. Поддерживает ли он трехсимвольные коды ответов?
9. Почему для работы со стандартными протоколами используют специальные программы?

9 НАСТРОЙКА БЕСПРОВОДНОЙ СЕТИ

Цель работы

Научиться настраивать Wi-Fi роутер в различных режимах.

Теоретические сведения

Пример 1. Легкая (полуавтоматическая) настройка беспроводного маршрутизатора TL-WR1043ND

Мы подключим к WI-FI маршрутизатор TP-LINK, точнее – модель TL-WR1043ND (Рисунок 9.1-9.3). Это современное устройство, у которого максимальная скорость беспроводного соединения: 300 Мбит/сек, а скорость портов 1000 Мбит/сек.



Рисунок 9.1 - Wi-Fi-точка доступа (роутер) TL-WR1043ND



Рисунок 9.2 - Передняя панель беспроводного маршрутизатора TL-WR1043ND

Светодиодные индикаторы и кнопка-индикатор QSS (быстрая настройка параметров безопасности):

PWR – питание. Индикатор выкл- питание отключено, вкл- питание включено.

SYS – система. Вкл. - загрузка исходных параметров или системная ошибка. Мигает - устройство работает в нормальном режиме. Выкл. - системная ошибка.

WLAN – беспроводная сеть. Выкл. - функция беспроводной передачи данных отключена. Мигает - функция беспроводной передачи данных включена.

WAN (Интернет), LAN (Локальная сеть) 1-4. Выкл. - у порта нет подключенных устройств. Вкл. - к порту подключено устройство, но оно неактивно. Мигает - к порту подключено устройство, и оно активно.

QSS - быстрая настройка параметров безопасности. Медленно мигает - беспроводное устройство производит подключение к сети через функцию QSS. Этот процесс занимает примерно две минуты. Вкл. - беспроводное устройство было успешно подключено к сети посредством функции QSS. Быстро мигает - не удалось подключить беспроводное устройство к сети посредством функции QSS.

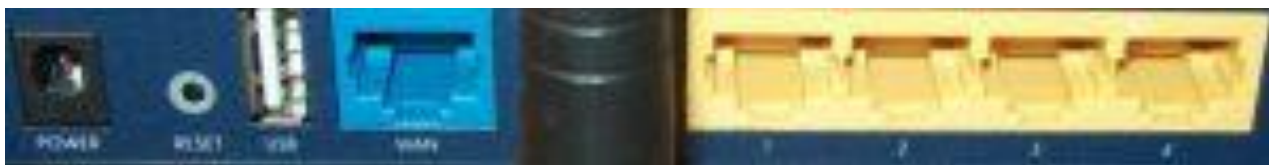


Рисунок 9.3 - Задняя панель беспроводного маршрутизатора TL-WR1043ND

На задней панели расположены следующие элементы:

POWER - разъем для подключения питания от адаптера питания, входящего в комплект поставки беспроводного маршрутизатора TL-WR1043ND

RESET – кнопка сброса конфигурации роутера для его возврата к заводским настройкам. При помощи иголки нажмите и удерживайте кнопку Reset 5 секунд, затем подождите, пока маршрутизатор выполнит перезагрузку.

USB - разъем для подключения устройства хранения данных или, например, принтера.

WAN синяя розетка RJ-45 для подключения DSL/кабельного модема или сети Интернет (порт для подключения Сети от провайдера).

Антенна Wi-Fi черного цвета служит для беспроводного получения и передачи данных.

1,2,3,4 (LAN) – розетки RJ-45 желтого цвета для подключения маршрутизатора к компьютерам локальной сети.

Итак, наш беспроводный роутер подключен к электросети, от него идет витая пара на стационарный ПК (патчкорд входит в комплект поставки), а Wi-Fi мы будем использовать, чтобы подключить ноутбук. Настройку роутера можно производить как на стационарном ПК (десктопе), так и со стороны ноутбука. Или там, или там нужно выполнить команду Панель Управления – Центр управления сетями и общим доступом – Настройка нового подключения или сети-Создание и настройка новой сети (рисунок 9.4).

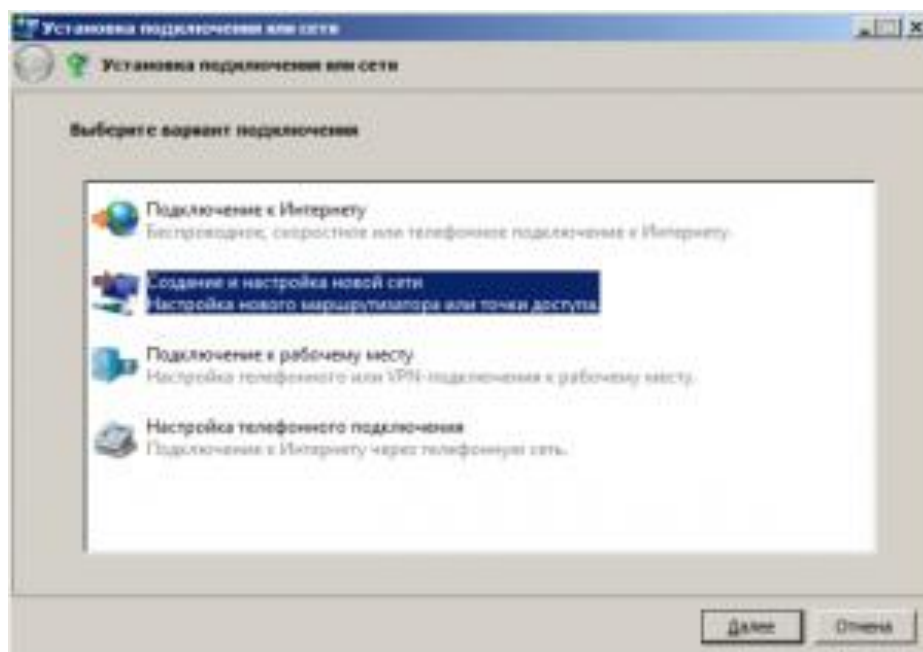


Рисунок 9.4 - Окно Установка подключения или сети

Нажимаем на кнопку Далее, видим наше беспроводное устройство (рисунок 9.5).

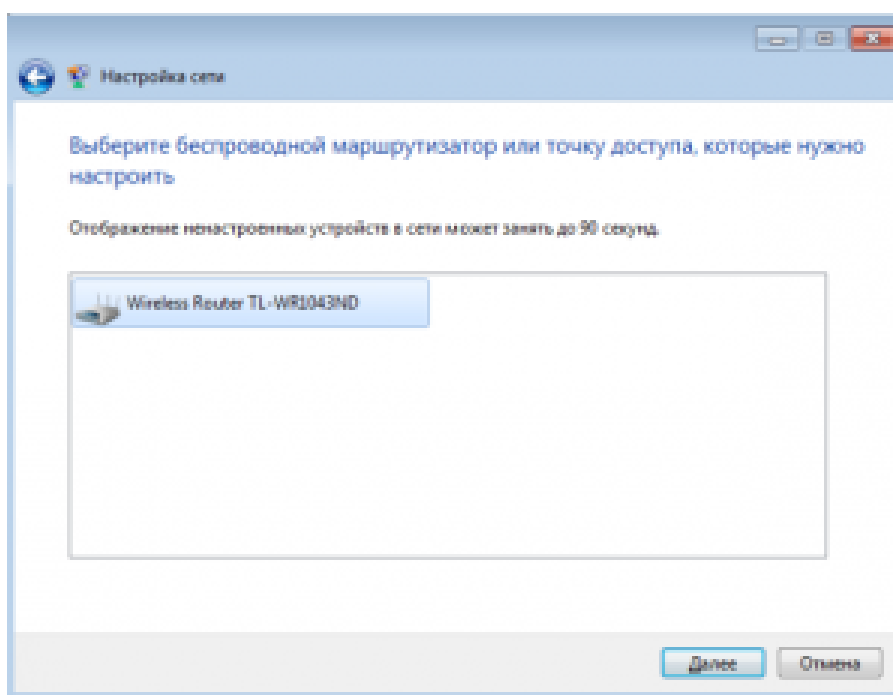


Рисунок 9.5 - Обнаружение точки доступа прошло нормально

Следующим этапом необходимо ввести PIN-код с этикетки на маршрутизаторе (рисунок 9.6 и рисунок 9.7).



Рисунок 9.6 - На этикетке маршрутизатора читаем PIN-код

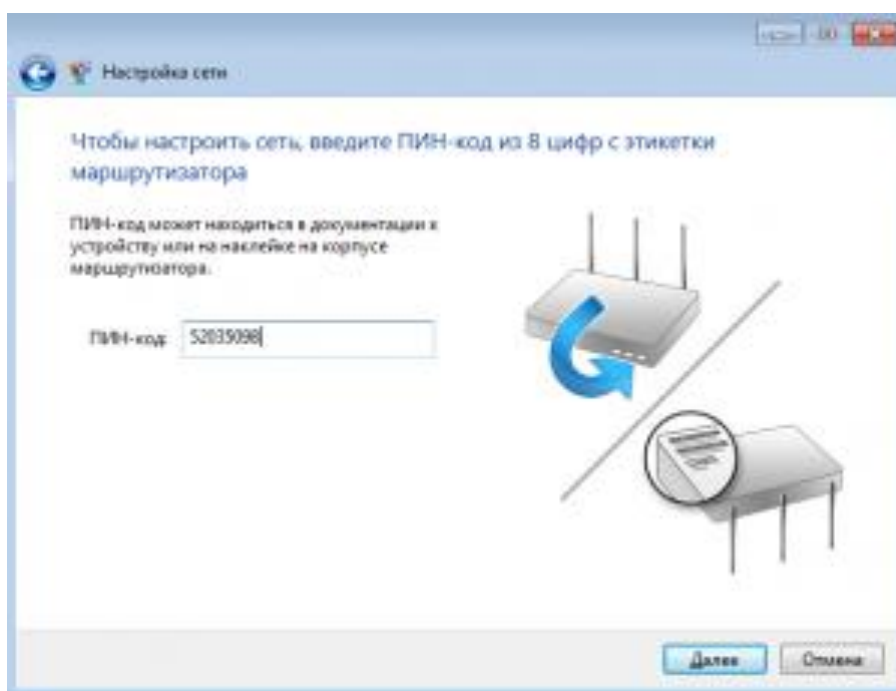


Рисунок 9.7 - Вводим PIN-код в окно Настройка сети

После нажатия на кнопку Далее следует согласиться с рекомендуемыми настройками точки доступа или задать свои (имя беспроводной сети, пароль для доступа к сети, уровень безопасности и тип шифрования) – рисунок 9.8.

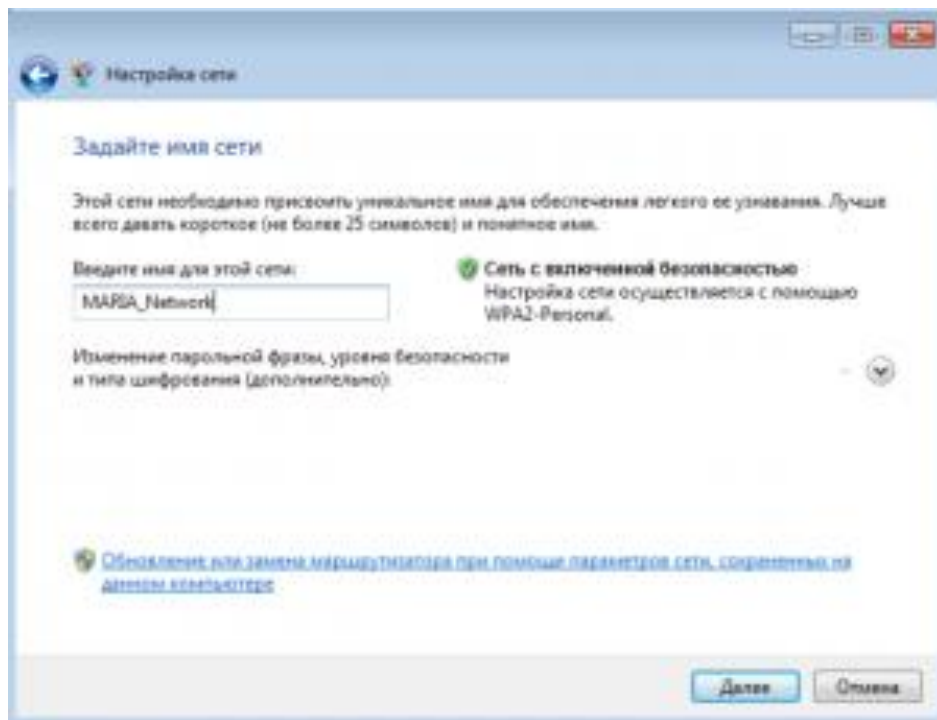


Рисунок 9.8 - Вводим имя сети (его придумываем сами)

После нажатия кнопки Далее произойдет настройка точки доступа (беспроводного маршрутизатора), генерация ключа безопасности и подключение нашего ноутбука к беспроводной сети (рисунок 9.9 и рисунок 9.10).

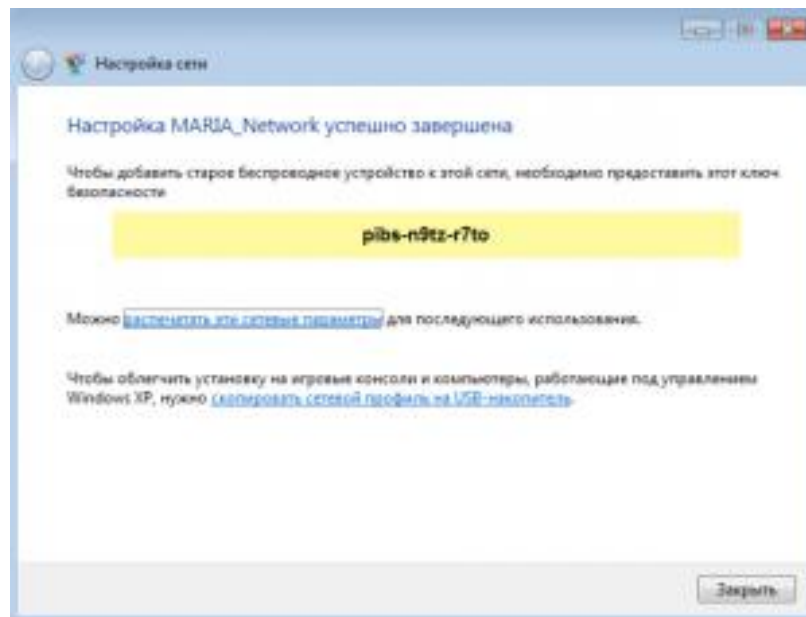


Рисунок 9.9 - Создание ключа безопасности

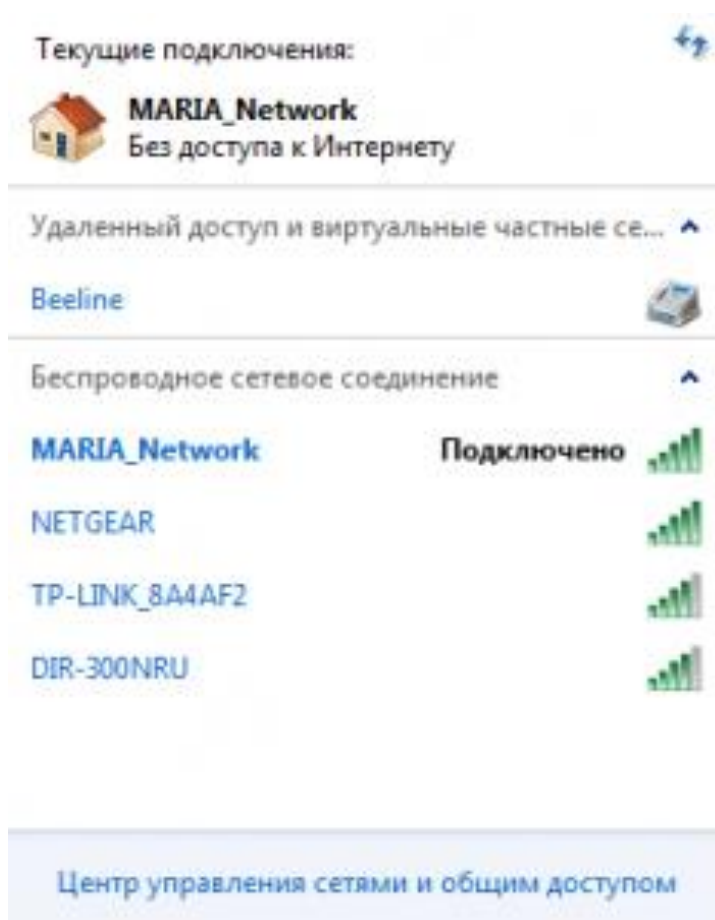


Рисунок 9.10 - Беспроводное соединение подключено

Примечание

Модель TL-WR1043ND имеет кнопку быстрой настройки защиты (QSS) для автоматической передачи ключа шифрования клиентскому устройству с такой же функцией. Поэтому, при подключении к нашей беспроводной сети нового компьютера под управлением Windows 7 (их может быть до 20 шт.), можно не вводить ключ безопасности, а просто нажать на эту кнопку на маршрутизаторе. Подключение к беспроводной сети произойдет автоматически (рисунок 9.11).

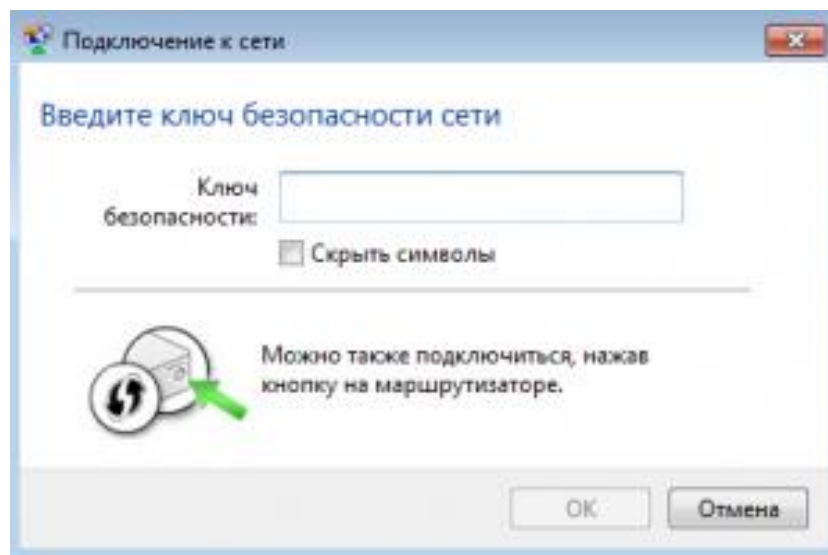


Рисунок 9.11 - Окно ввода ключа безопасности

Пример 2. Настройка на работу в Интернет Wi-Fi роутера Net Gear JWNR2000 в ручном режиме

В этой работе мы изучим, как можно с помощью Wi-Fi роутера подключить к Интернет два ПК: стационарный и ноутбук. Порты и индикаторы роутера приведены на рисунок 9.12.

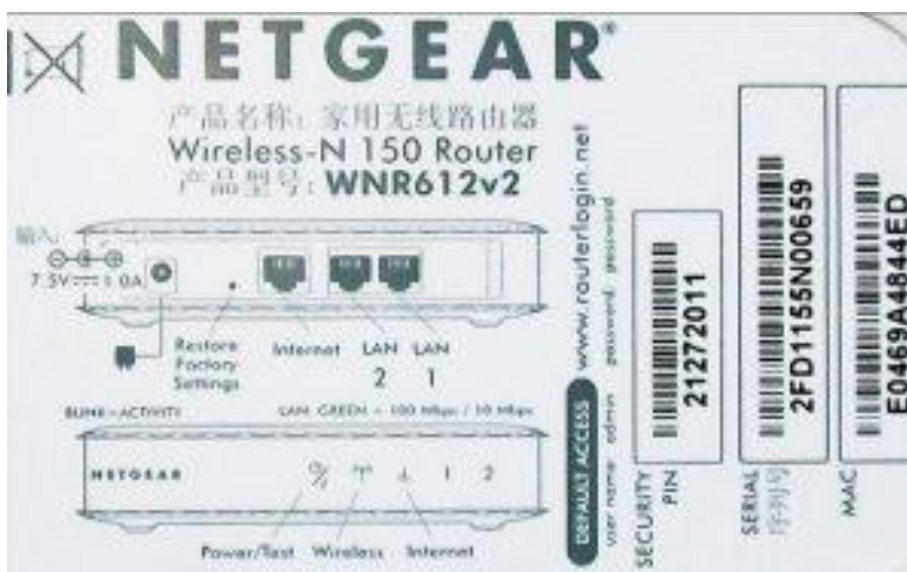


Рисунок 9.12 - Обозначение портов и индикаторов роутера Net Gear JWNR2000

Характеристики этой модели маршрутизатора для выделенной линии таковы:

Частота- 2,4 Гц

Режимы- Infrastructure, WDS-Bridge

Кнопки -Reset, WPS

Примечание

Кнопка WPS нужна для упрощение процесса настройки беспроводной

сети. Нажатие WPS автоматически обозначает имя сети и задает шифрование, для защиты от несанкционированного доступа в сеть, при этом нет необходимости вручную задавать все параметры.

Индикаторы - LAN, Power, WLAN, WPS

Порты Fast Ethernet - 4 порта 10/100 Мбит/сек

Порты WAN - 1 порт RJ-45

Управление - Веб-интерфейс, GUI, SNMP

Firewall - фильтрация по MAC-адресу, фильтрация пакетов, защита от DoS-атак

Поддержка схем обеспечения безопасности беспроводной передачи WPA2-PSK; WPA-PSK; TKIP; AES; WEP-кодирование с 64- или 128-битным ключом

Защищенные VPN-протоколы - PPTP, PPPoE

Получение IP-адреса -Static IP, Dynamic IP

QoS- Поддерживается

Поддержка WMM (Wi-Fi Multimedia) - Есть

DMZ - Поддерживается

NAT - Поддерживается

DHCP-сервер - Есть

Максимальная скорость беспроводной передачи данных - 300 Мбит/сек

Стандарты беспроводной связи - IEEE 802.11n, IEEE 802.11g, IEEE 802.11b

Шаг 1 – Настройка стационарного ПК для ОС Windows XP

Подключаем роутер согласно схеме на рисунок 9.13.



Рисунок 9.13 - Схема подключения устройств беспроводной сети к точке доступа

Далее нужно настроить протокол TCP/IP как на рисунке 9.14.

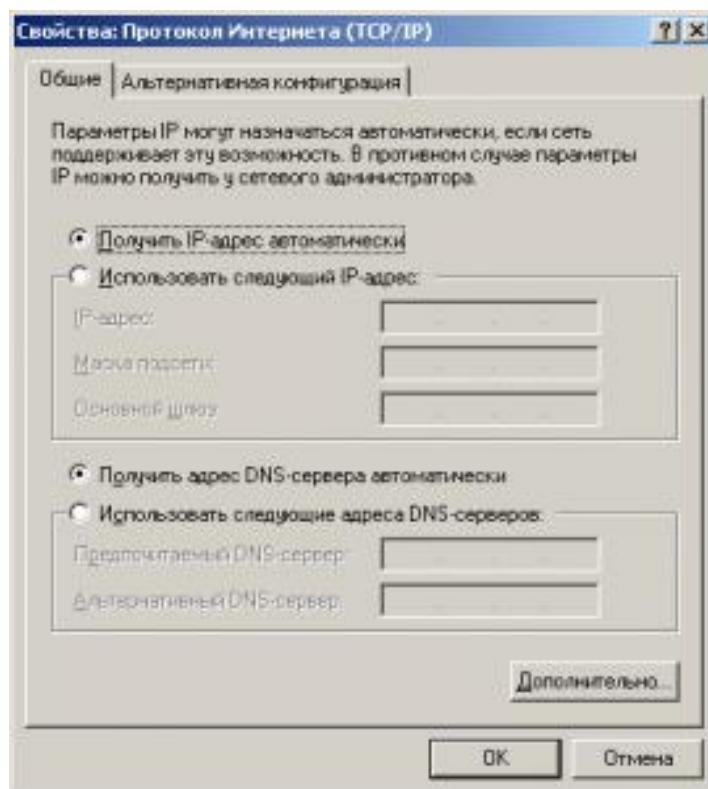


Рисунок 9.14 - Настройка протокола Интернет

Затем введите в браузере 192.168.1.1 и получите следующее окно (Рисунок 15). Вводим сюда Имя пользователя и Пароль (они написаны на этикетке роутера – см. рисунок 9.15).

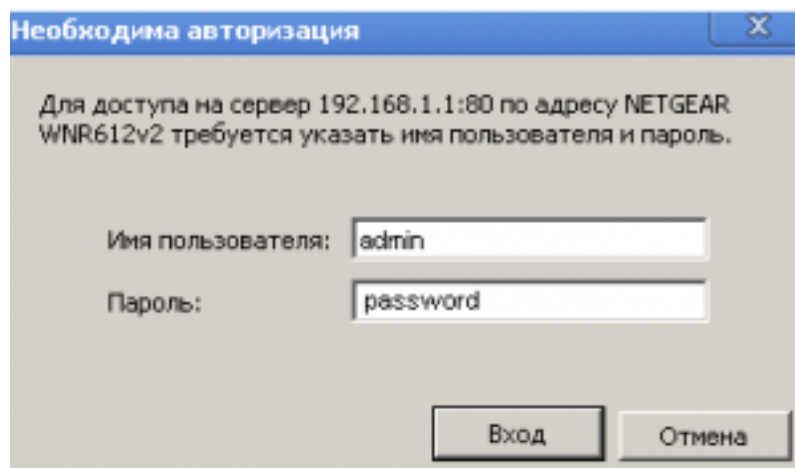


Рисунок 9.15 - Окно входа на сервер 192.168.1.1

После нажатия на кнопку Вход откроется окно Основные настройки. В программе имеется Мастер установки, но он здесь не очень хорош, поэтому лучше воспользоваться ручной настройкой роутера (рисунок 9.16).



Рисунок 9.16 - Эти данные вводите в соответствии с договором провайдера Интернет

В данное окно вводим IP-адрес, IP-маску подсети и IP-адрес шлюза из договора с провайдером. Нажимает на кнопку Применить – появляется другое окно Основные настройки (рисунок 9.17).



Рисунок 9.17 - Окно основные настройки

Здесь в соответствии с договором провайдера Интернет вводим Имя пользователя и Пароль. В этом окне же следует в списке Поставщик услуг Интернета выбрать протокол PPPoE (рисунок 9.18). Нажимаем Применить.



Рисунок 9.18 - Из протоколов доступа выбираем протокол PPPoE

После обновления параметров роутера в поле Сохранение найдите опцию Установить пароль и замените пароль по умолчанию, т.е. password на какой-либо свой, например, quthor. Далее настройте окно Параметры беспроводного соединения – рисунок 9.19.



Рисунок 9.19 - Окно Параметры беспроводного соединения

Примечание

SSID – название беспроводной сети

Фраза – пароль здесь задан 12345678, но лучше ввести что-либо более сложное.

Совет

Для замены пароля наберите 192.168.1.1., введите admin и quthor, выберите команду Параметры беспроводного соединения и введите новый пароль,

например, masha+vova=love

ШАГ 2 – Настройка Wi-Fi сети на ноутбуке для ОС Windows

Настроим работу Wi-Fi адаптера на ноутбуке, чтобы он смог получить Интернет от роутера NetGear. Выполните на ноутбуке команду Панель управления-Сеть и Интернет-Подключение к сети (рисунок 9.20).

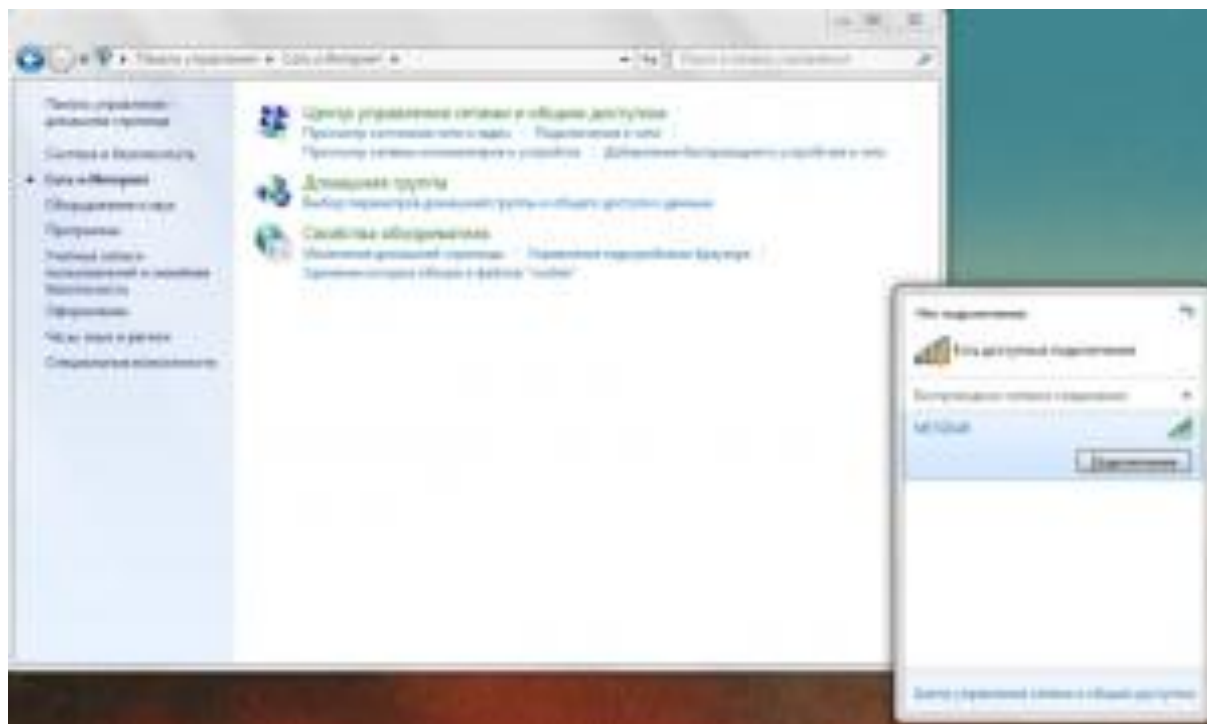


Рисунок 9.20 - Беспроводное сетевое соединение (роутер) ноутбук обнаружил

После нажатия на кнопку Подключение необходимо ввести фразу-пароль ключа безопасности (в нашем случае 12345678 или, если вы этот пароль изменили, то masha+vova=love) и Интернет на ноутбук будет подключен. Интернет запускается через любой браузер как при включенном стационарном ПК, так и без него. Лишь бы роутер был включен.

Настольная всенаправленная 8дБи антенна TL-ANT2408C

Беспроводная настольная антенна TL-ANT2408C работает на частоте 2.4-2.5ГГц с коэффициентом усиления 8дБи и позволяет существенно увеличить дальность беспроводного сигнала и повысить качество соединения. Антенна оснащена RP-SMA штекером, что обеспечивает совместимость с большинством беспроводных устройств – рисунок 9.21.



Рисунок 9.21 - Беспроводная антенна для роутера модели TL-ANT2408C

Замена стационарной антенны маршрутизатора (точки доступа) на TL-ANT2408C заметно увеличит силу и дальность беспроводного сигнала. Поскольку данная антенна является всенаправленной, то нет необходимости поворачивать ее в ту или иную сторону для получения более четкого сигнала – антенна получает и отправляет сигналы во всех направлениях.

Примечание

дБи (dBi) - это децибелл по сравнению с «i», то есть по отношению к изотропному излучателю - идеальной антенне, диаграмма направленности которой представляет собой сферу, коэффициент усиления которой равен единице и КПД которой равен 100%. дБи (dBi) характеризует коэффициент усиления антенны и ее направленные свойства по сравнению с изотропным излучателем. Строго говоря, если говорят, что данная антенна имеет коэффициент усиления, например, 8 дБ, то на самом деле имеется в виду 8 дБи.

Wi-Fi-адаптер TP-LINK TL-WN725N

Недорогой и компактный Wi-Fi-адаптер TP-LINK TL-WN725N показан на рисунок 9.22.



Рисунок 9.22 - Wi-Fi адаптер TP-LINK TL-WN725N

Характеристики:

Стандарт беспроводной связи - 802.11n, частота 2.4 ГГц

Макс. скорость беспроводного соединения - 150 Мбит/с

Интерфейс подключения - USB 2.0

Защита информации (режим шифрования данных) - WEP, WPA, WPA2, 802.1x

Мощность передатчика 20 dBm

Примечание

дБм (dBm) - это децибелл по сравнению с «м», в данном случае по отношению к милливату. Иначе говоря, это значение того, на сколько децибелл данная мощность больше (или меньше) чем 1 мВт.

Беспроводной мини сетевой USB-адаптер (USB WLAN) TL-WN823N

Беспроводной мини сетевой USB-адаптер TL-WN823N предназначен для подключения ноутбука или настольного компьютера к беспроводной сети. Скорость беспроводного соединения до 300 Мбит/с. – рисунок 9.23.



Рисунок 9.23 - Адаптер TL-WN823N с кнопкой WPS

Адаптер имеет функцию программной точки доступа. Включив этот режим, пользователи получают совместный доступ к прочим Wi-Fi устройствам (ноутбуки, смартфоны или планшетики) со своих ноутбуков или персональных компьютеров с проводным подключением. Адаптер позволяет произвести настройку безопасности одним нажатием кнопки WPS (Wi-Fi Protected Setup). Пользователи могут моментально настроить защиту сети одним нажатием на маршрутизаторе кнопки WPS, после чего автоматически устанавливается соединение, защищенное режимом шифрования WPA2, который считается более надежным по сравнению с шифрованием WEP. Это не только быстрее обычной процедуры настройки безопасности, но и более удобно, так как пользователям даже не придется запоминать пароль.

USB-адаптер Wi-Fi TP-Link TL-WN822N

Модель TP-Link TL-WN822N хорошо справляется с поиском слабого сигнала Wi-Fi, так как имеет две мощных всенаправленных антенны с коэффициентом усиления 3 дБи (это больше, чем у стандартного ноутбука). Адаптер имеет кнопку QSS для быстрой настройки защищенного беспроводного соединения, а также светодиодный индикатор активности. Функция QSS (Quick Secure Setup) необходима для быстрой настройки защищенного беспроводного соединения. Эта функция является аналогом технологии WPS (Wi-Fi Protected Setup), только называется по-другому. При включенном беспроводном модуле на маршрутизаторе устройства тут же обнаруживают друг друга и запрашивают у пользователя разрешение на соединение. Вы нажимаете кнопки QSS на маршрутизаторе и USB-адаптере и тем самым настраиваете защищенное с использованием алгоритмов шифрования WPA2 соединение. Пользователю останется лишь задать желаемый пароль (Рисунок 24).



Рисунок 9.24 - USB-адаптер Wi-Fi TP-Link TL-WN822N

Характеристики адаптера:

Стандарты - IEEE 802.11b/g/n (300 Мбит/с)

Порты - 1 x Mini-USB

Частотный диапазон, ГГц - 2,4–2,4835

Антенны - 2 x внешняя складная всенаправленная, 3 дБи

Безопасность - WEP, WPA/WPA2, WPA-PSK/WPA2-PSK

Режимы работы - Ad-Hoc/в инфраструктуре

Дополнительные функции - поддержка Sony PSP, QSS

Пример 3. Настройка WI-FI адаптера TP-LINK

Вставляем адаптер в USB порт ПК и устанавливаем драйвер адаптера (рисунок 9.25).

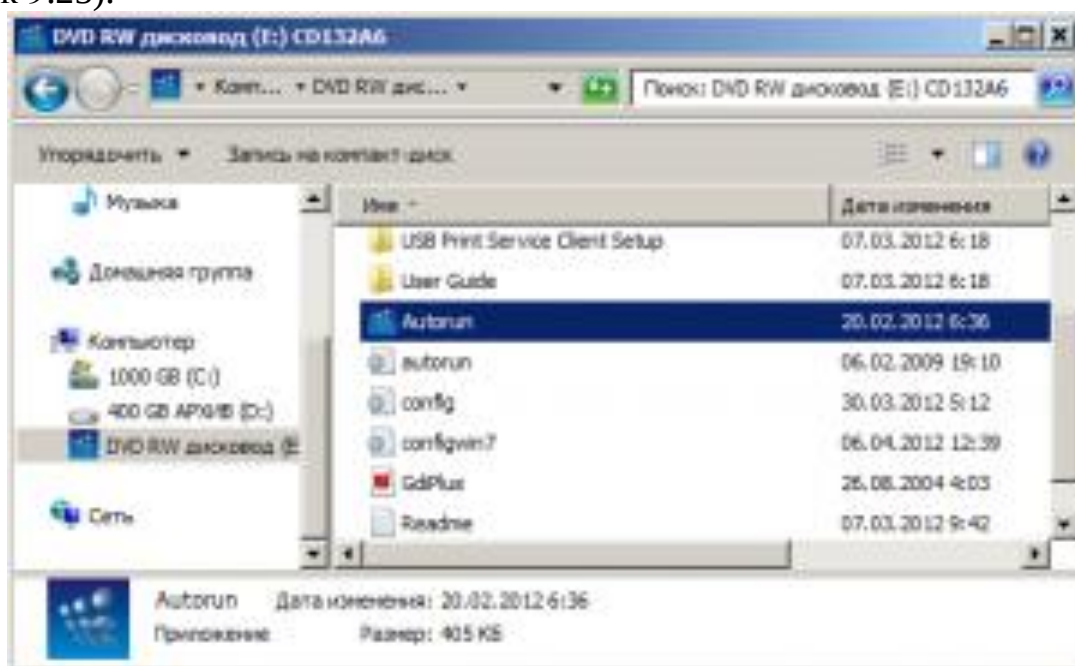


Рисунок 9.25 - Начинаем установку драйвера WI-FI адаптера

Указываем модель адаптера (рисунок 9.26) и начинаем его настройку (рисунок 9.27).



Рисунок 9.26 - Выбираем модель адаптера

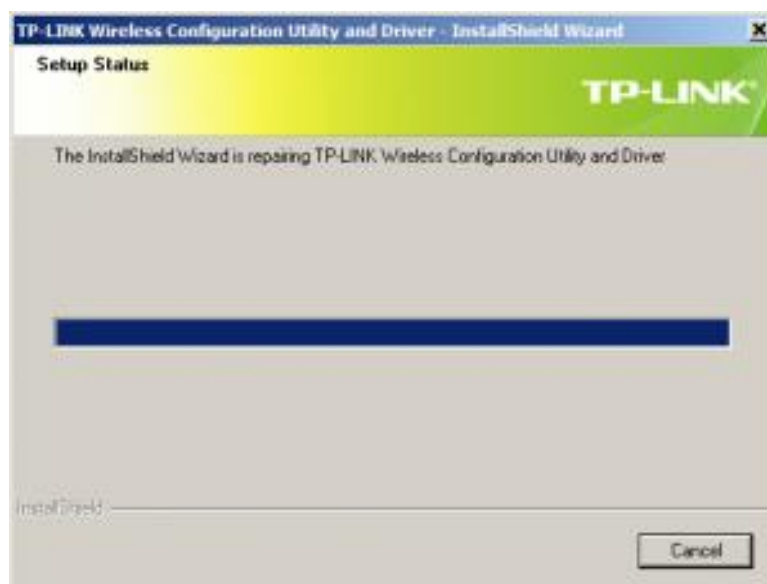


Рисунок 9.27 - Мастер начинает установку драйвера адаптера

После установки адаптер обнаружит ближайшие беспроводные сети, в том числе и наш роутер TP-Link (рисунок 9.28).



Рисунок 9.28 - Беспроводная сеть с точкой доступа TP-LINK обнаружена

Для подключения к сети мы должны или нажать на роутере кнопку WPS (рисунок 9.29) или ввести, написанный на роутере PIN-код, у нас это число 52035098 – рисунок 9.30 и рисунок 9.31.



Рисунок 9.29 - Предложение о настройке безопасности сети путем нажатия на кнопку WPS



Рисунок 9.30 - Этикетка роутера с его PIN кодом



Рисунок 9.31 - Окно ввода PIN кода

Результат – беспроводная сеть настроена (рисунок 9.32).



Рисунок 9.32 - ПК к сети Интернет подключен

В работе мы на практике рассмотрели работу с конкретными моделями беспроводных устройств, а именно: настройку беспроводного маршрутизатора TL-WR1043ND и Wi-Fi роутера Net Gear JWNR2000. Мы изучили настройку Wi-Fi сети на ноутбуке для ОС Windows. Познакомились с характеристиками настольной всенаправленной 8дБи антенны TL-ANT2408C, Wi-Fi-адаптера TP-LINK TL-WN725N, беспроводного мини сетевого USB-адаптер (USB WLAN) TL-WN823N и USB-адаптером Wi-Fi TP-Link TL-WN822N.

Задание для самостоятельного выполнения

Настроить WiFi роутер в режимах: радио удлинителя, точки доступа и туннеля.

Контрольные вопросы

1. Какие режимы работы WiFi роутера Вы знаете?
2. В чем отличие стандартов WiFi?
3. Какие технологии беспроводного доступа Вам известны?

10 УСТАНОВКА DNS СЕРВЕРА

Цель работы

Научиться настраивать DNS сервер.

Теоретические сведения

Выбор для сервера роли DNS сервера

DNS (Domain Name System - система доменных имён) - компьютерная система для получения IP-адреса по имени хоста и обратно.

Назначим нашему серверу роль DNS сервера (рисунок 10.1).

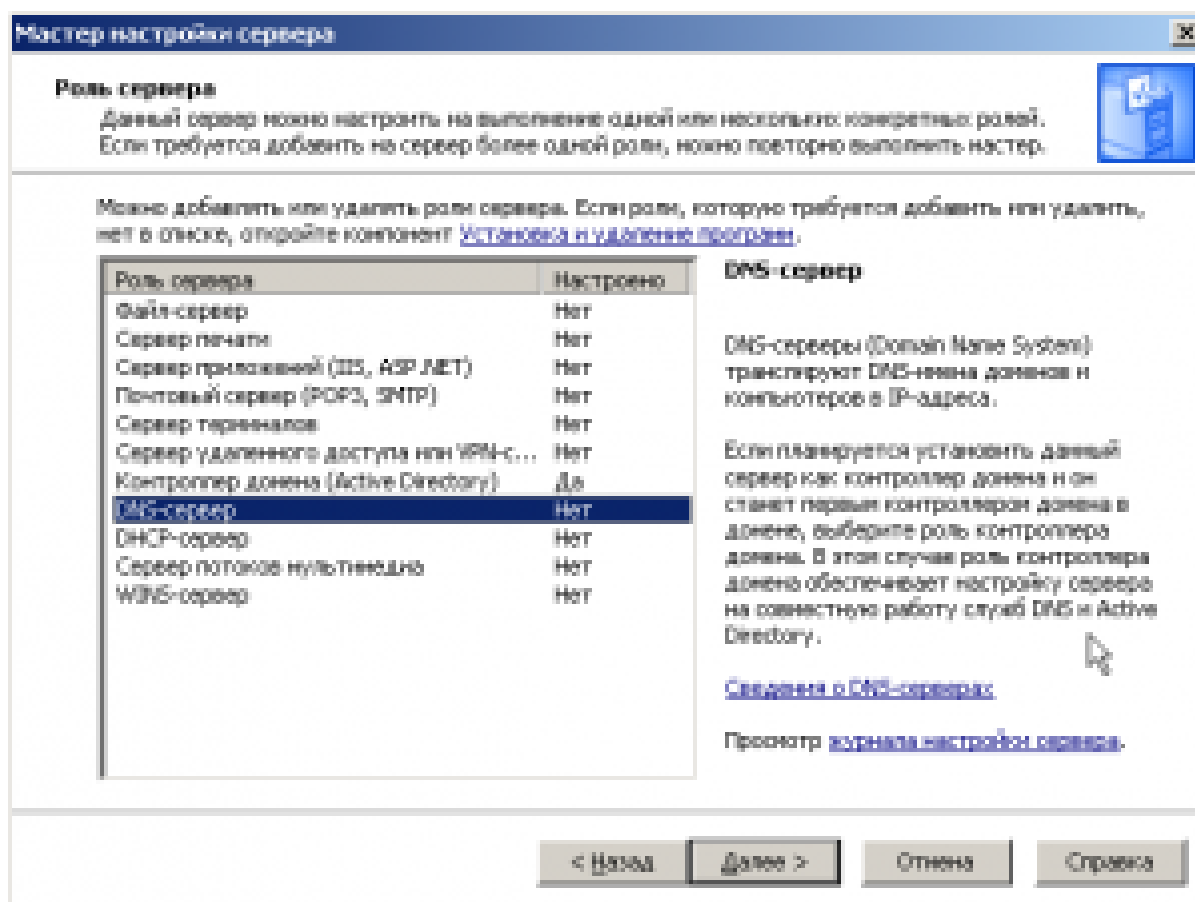


Рисунок 10.1 - Мастер настройки сервера-DNS сервер

Далее появиться предложение изменить динамический IP адрес на статический (рисунок 10.2).

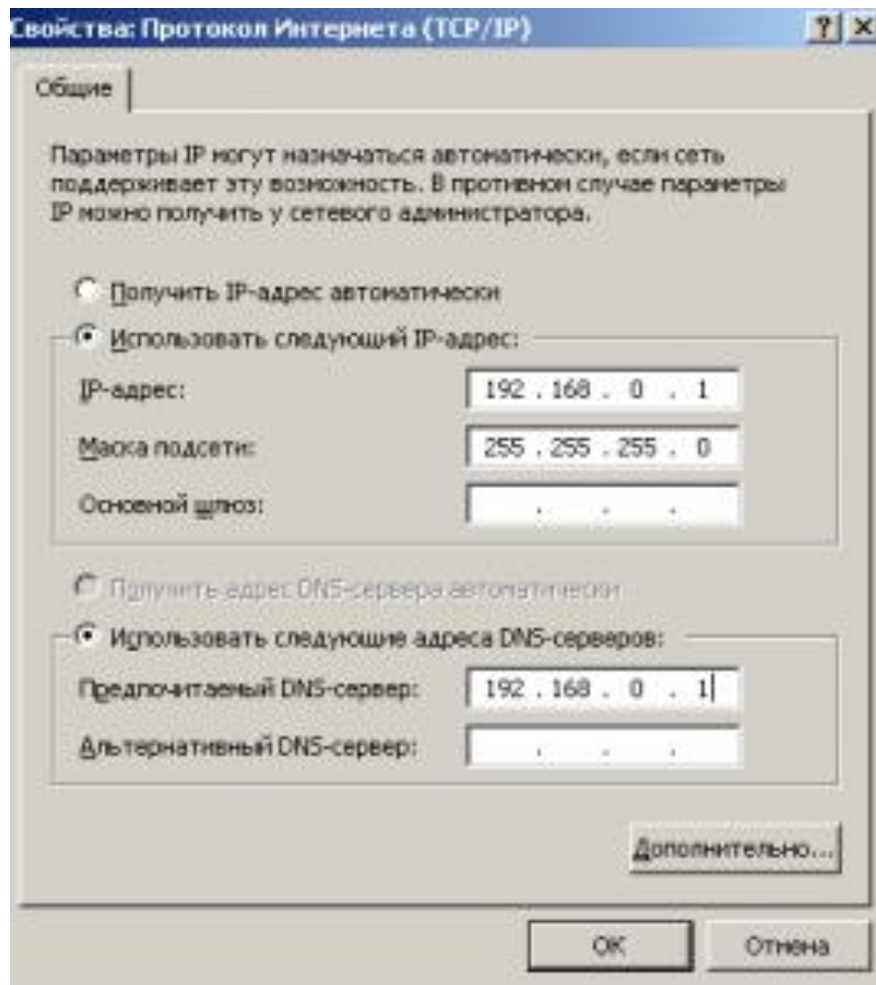


Рисунок 10.2 - Задаем серверу статический IP адрес

Далее появится Мастер настройки DNS сервера (рисунок 10.3).

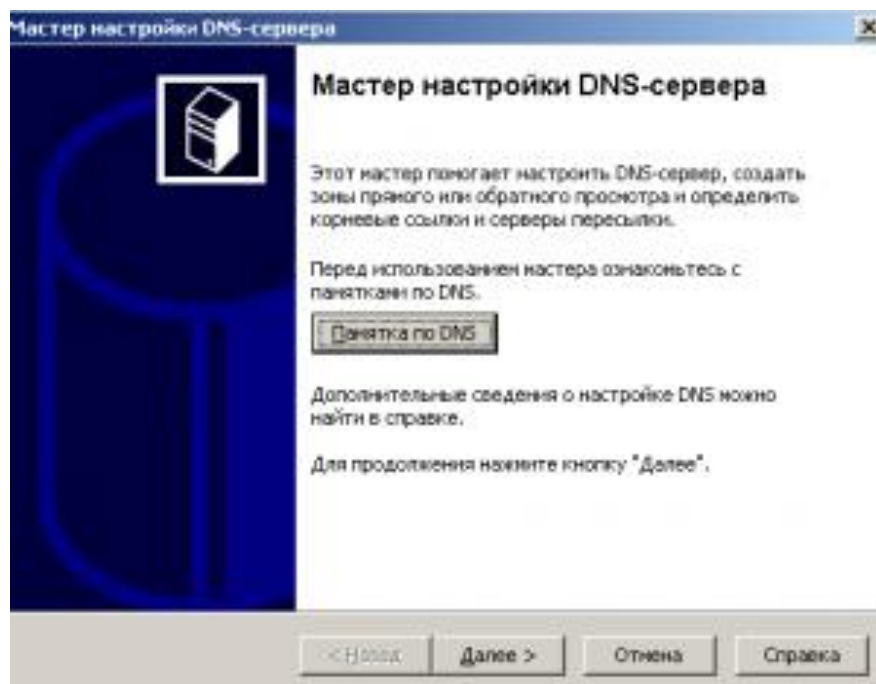


Рисунок 10.3 - Окно Мастер настройки DNS сервера

Поскольку сеть у нас небольшая, то установим верхний переключатель (рисунок 10.4).

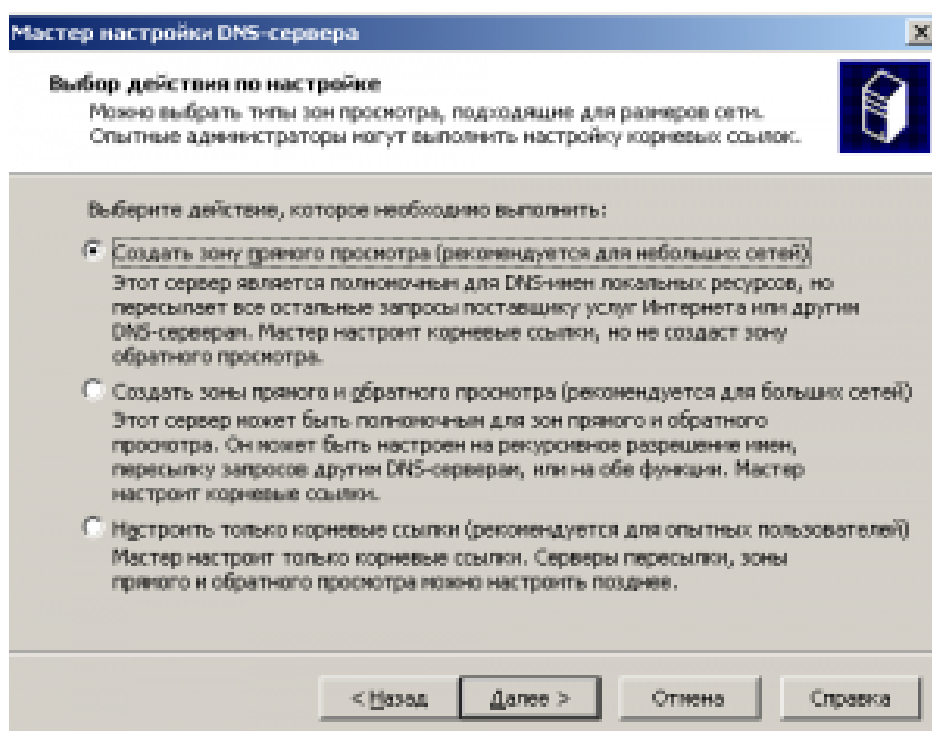


Рисунок 10.4 - Создание зоны прямого просмотра

Зону прямого просмотра назовем так же, как и домен – domain.110. Далее исходим из того, что у нас только один DNS сервер, больше пересылать запросы некому (рисунок 10.5).

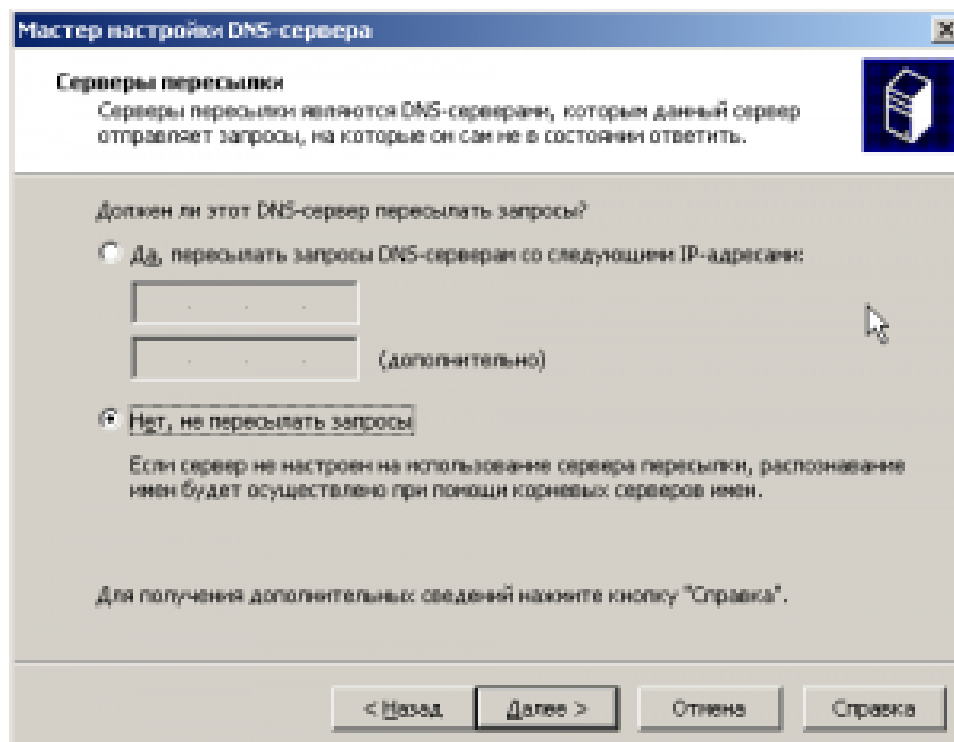


Рисунок 10.5 - Активируем нижний переключатель

Настройка сервера завершена (рисунок 10.6).

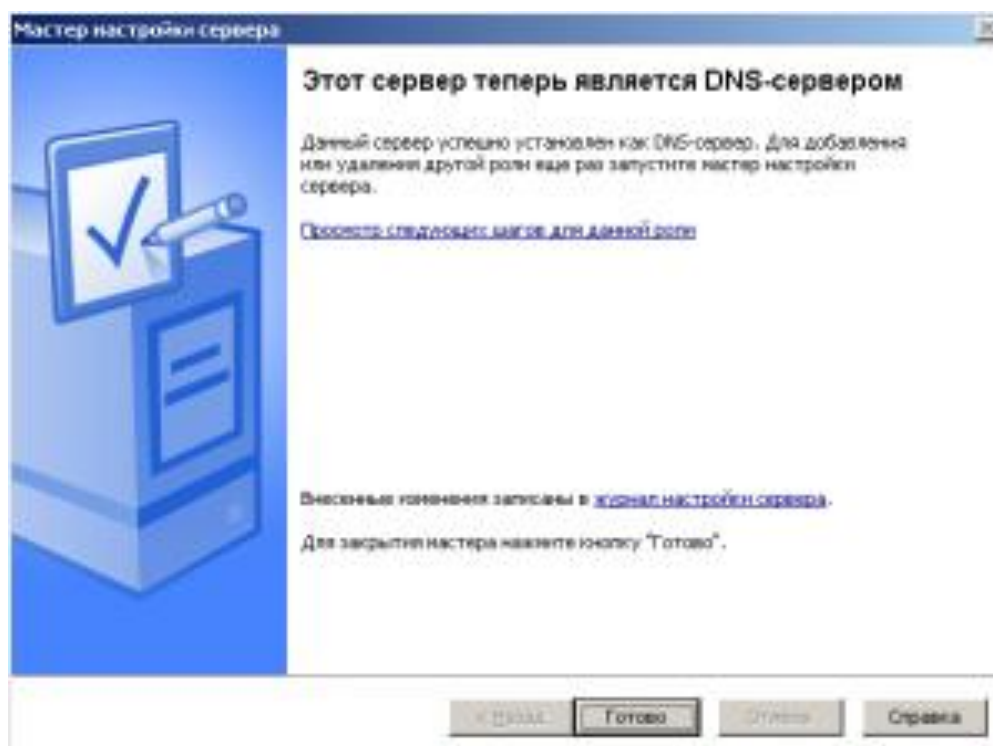


Рисунок 10.6 - Сервер получил роль DNS сервера

Выполнив команду, Пуск-Все программы-Администрирование мы увидим, что появилась новая оснастка (рисунок 10.7).

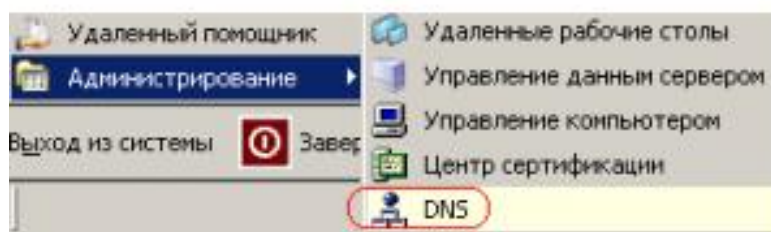


Рисунок 10.7 - На рисунке новая оснастка отмечена красным

Откроем ее (рисунок 10.8). Здесь в зоне прямого просмотра вы можете увидеть соответствие имени сервера sgv-2003 его IP адресу 192.168.0.1.

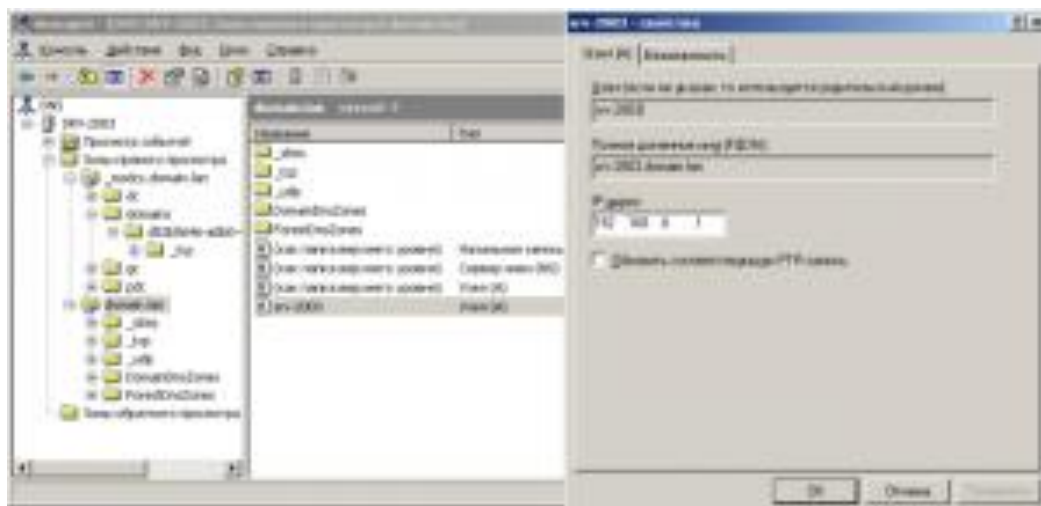


Рисунок 10.8 - На рисунке открыта зона прямого просмотра

Создание зоны обратного просмотра

Щелкните на строчку Зона обратного просмотра и выберите команду Создать новую зону (рисунок 10.9).

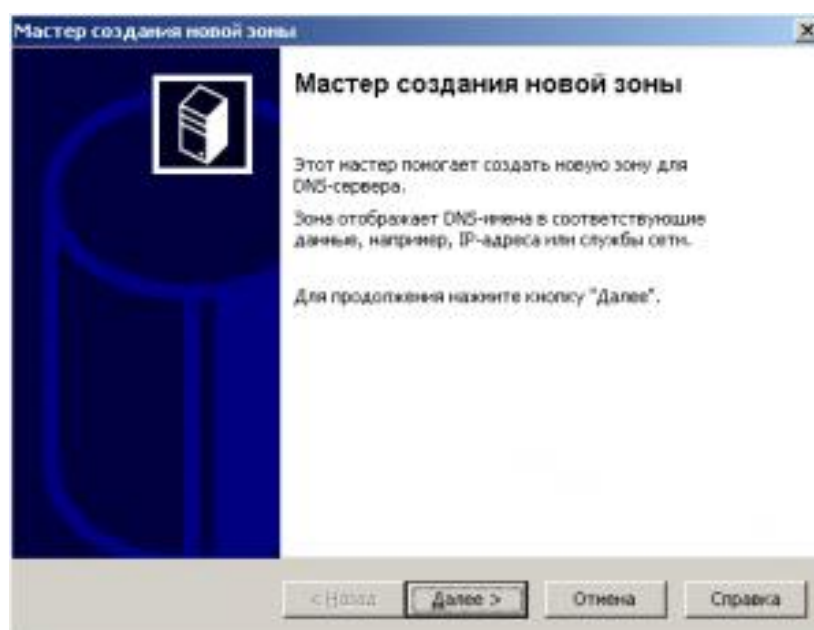


Рисунок 10.9 - Окно мастера создания новой зоны

Далее устанавливаем верхний переключатель – рисунок 10.10.

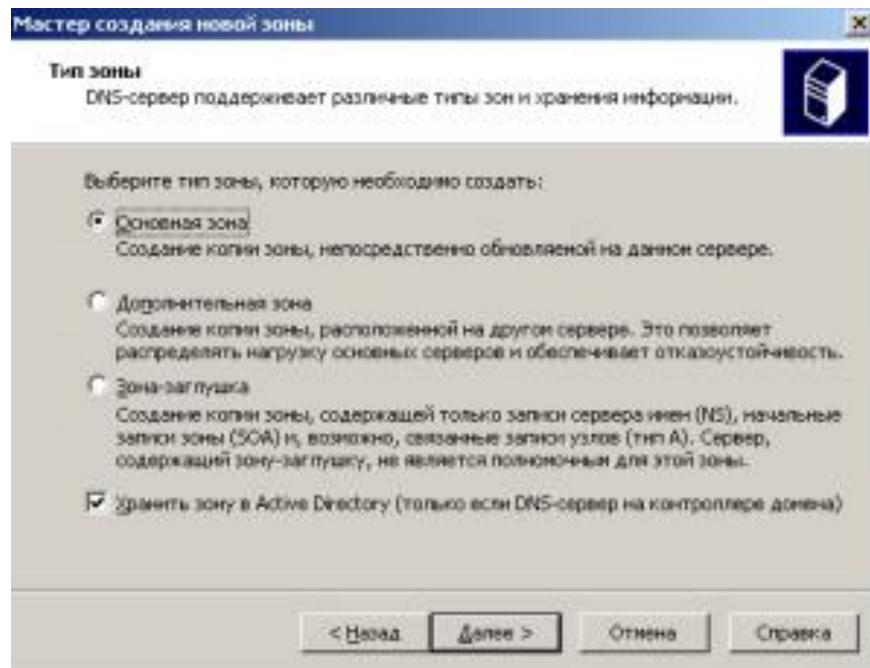


Рисунок 10.10 - Устанавливаем переключатель Основная зона

Примечание

Основная зона устанавливается на основной сервер (она - главная), Дополнительная зона необходима для резервирования и разгрузки основного сервера. Если загрузка первого DNS сервера велика (или он отключился), то часть запросов можно отправить на второй, альтернативный DNS и отказоустойчивость системы повышается (рисунок 10.11). Зона - заглушка содержит IP адрес сервера, который может обслужить запрос.

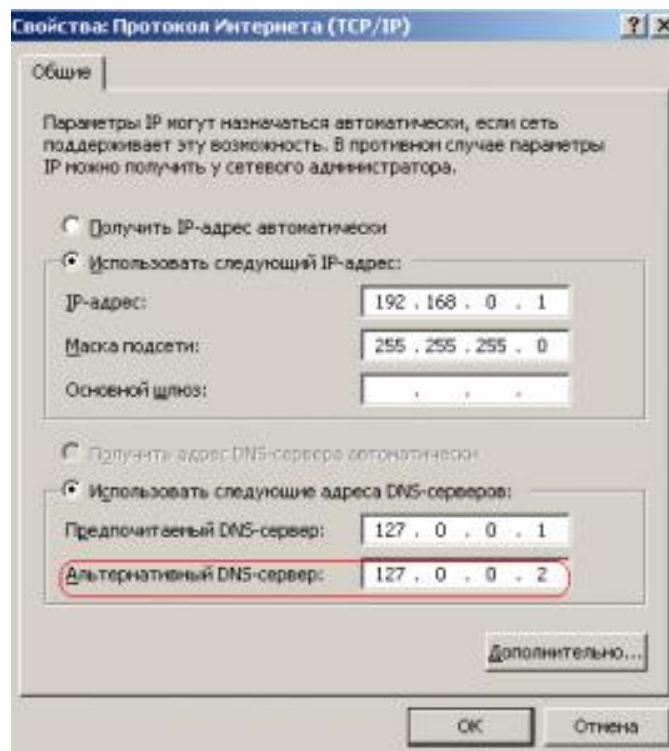


Рисунок 10.11 - Пример использования альтернативного DNS сервера

Наша сеть 192.168.0.1 относится к классу сетей C, поэтому значение 192.168.0 мы менять не можем - это и есть код сети (ID) –рисунок 10.12.

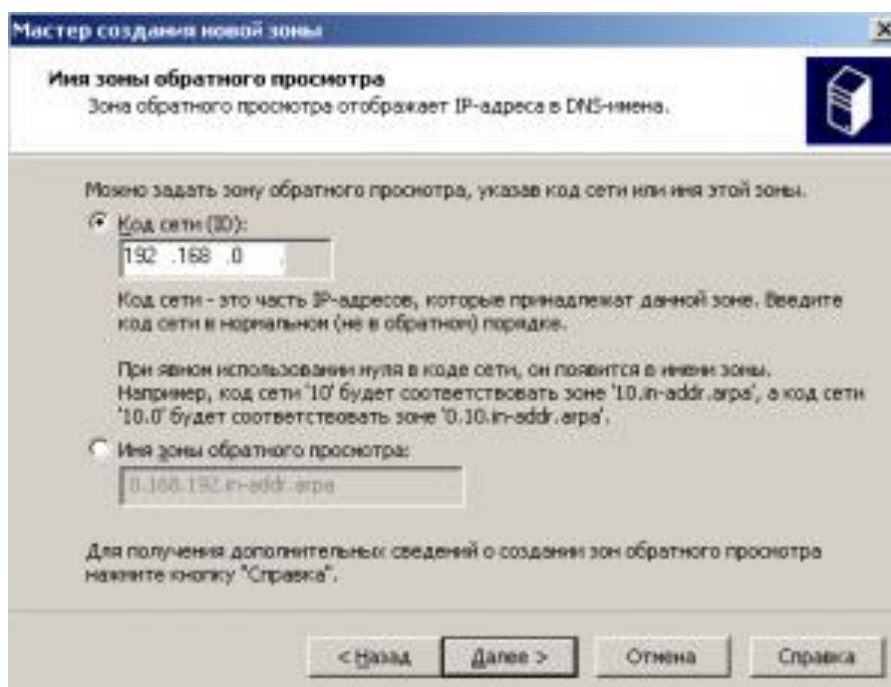


Рисунок 10.12 - Задаем код сети

Зона обратного просмотра создана. После подключения первого ПК здесь появится соответствие IP адреса ПК его имени.

Записи ресурсов DNS

Вся DNS состоит из этих RR записей, по которым пользователь может искать ресурсы в сети. Запустим консоль управления DNS и зайдем в зону прямого просмотра (рисунок 10.13).

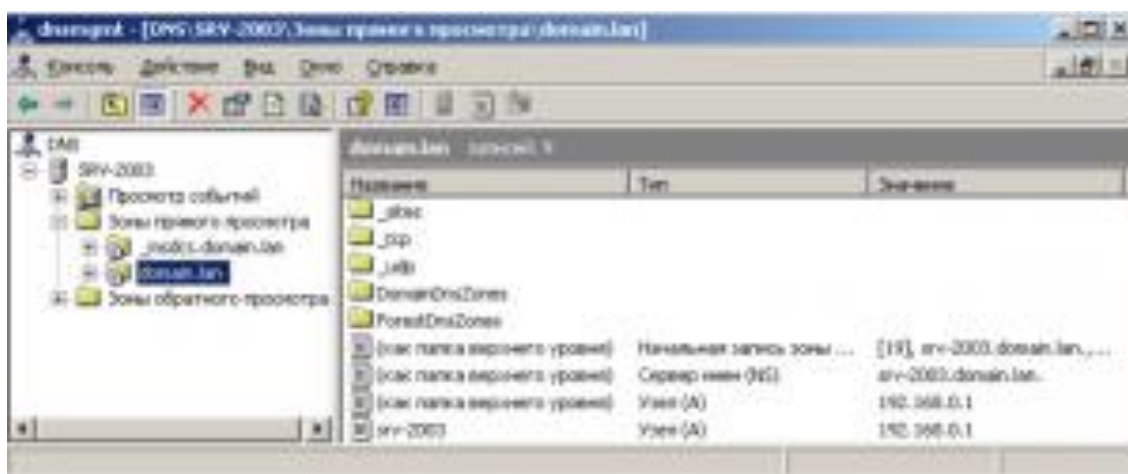


Рисунок 10.13 - Зоны прямого просмотра

Выполним двойной щелчок на строчке Начальная запись зоны (рисунок 10.14). В данном окне наиболее интересный параметр Срок жизни (TTL). Предположим, что компьютер с именем ПК-1 и IP адресом

192.168.0.1 хочет соединиться с именем ПК-2 и IP адресом 192.168.0.2. Он выдает запрос на DNS сервер и тот сообщает, что с компьютер с именем ПК-2 имеет IP адрес 192.168.0.2. Эта запись кэшируется (помещается в память) на Срок жизни (TTL). Подобный подход к запросам снижает нагрузку на DNS сервер.

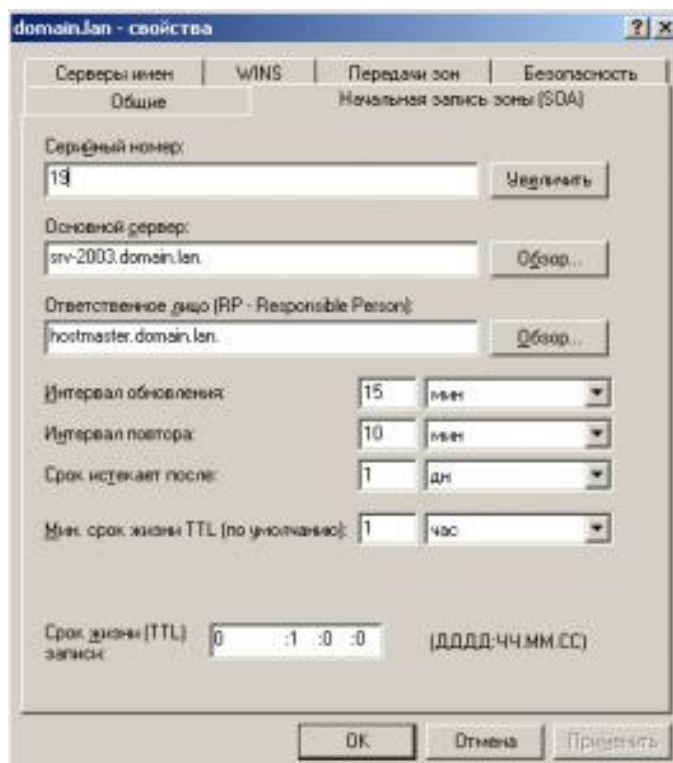


Рисунок 10.14 - Вкладка Начальная запись зоны

Теперь выполним двойной щелчок на строчке Сервер имен (рисунок 10.15). У нас DNS сервер один, поэтому запись здесь одна. Но, здесь записей может быть столько, сколько имеется DNS серверов.

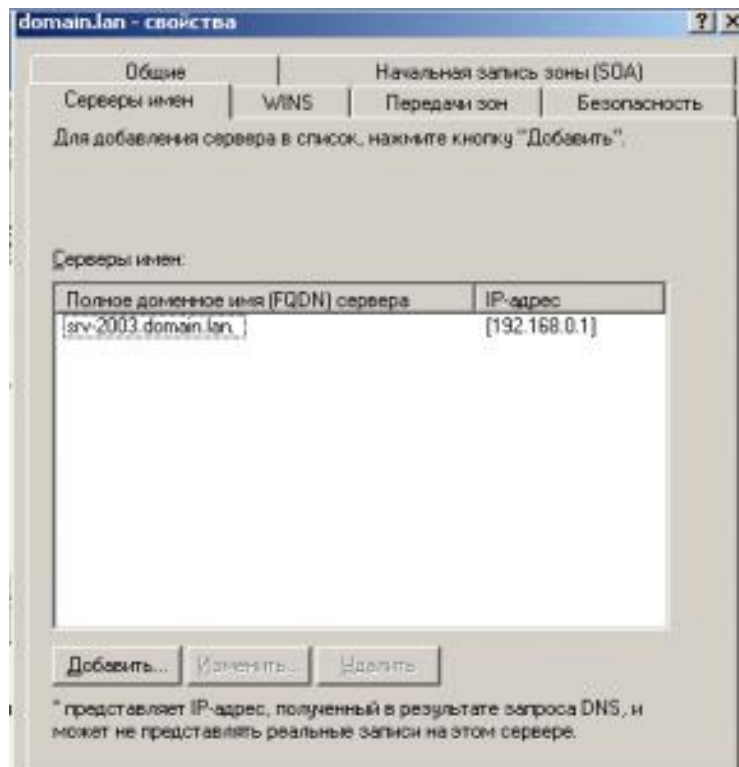


Рисунок 10.15 - Вкладка Серверы имен

Выполним двойной щелчок на строчке Узел А (рисунок 16). Эта запись устанавливает прямое соответствие между именем ПК и его IP адресом.

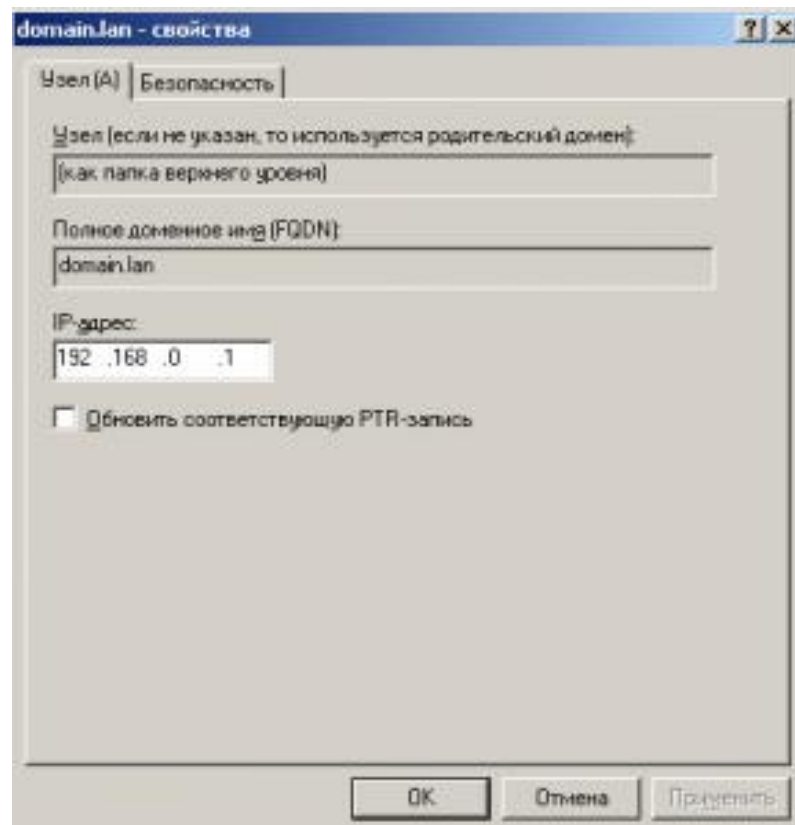


Рисунок 10.16 - Вкладка Узел А

Теперь изучим записи зоны обратного просмотра. После перезагрузки ПК здесь будет три записи (рисунок 10.17).

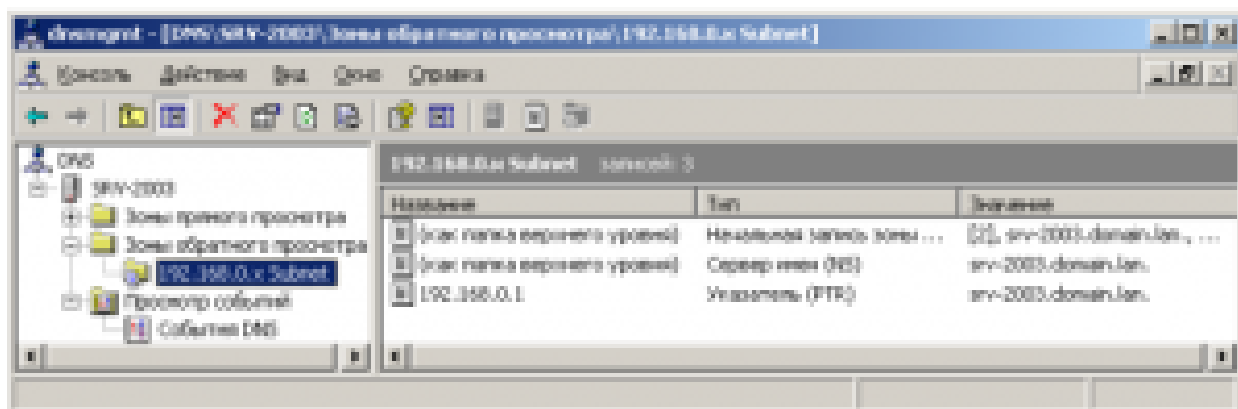


Рисунок 10.17 - Записи зоны обратного просмотра

Двойным щелчком мыши зайдем в Указатель (PTR) – рисунок 10.18. Как видим, именно здесь задается обратное соответствие IP адреса и имени ПК.

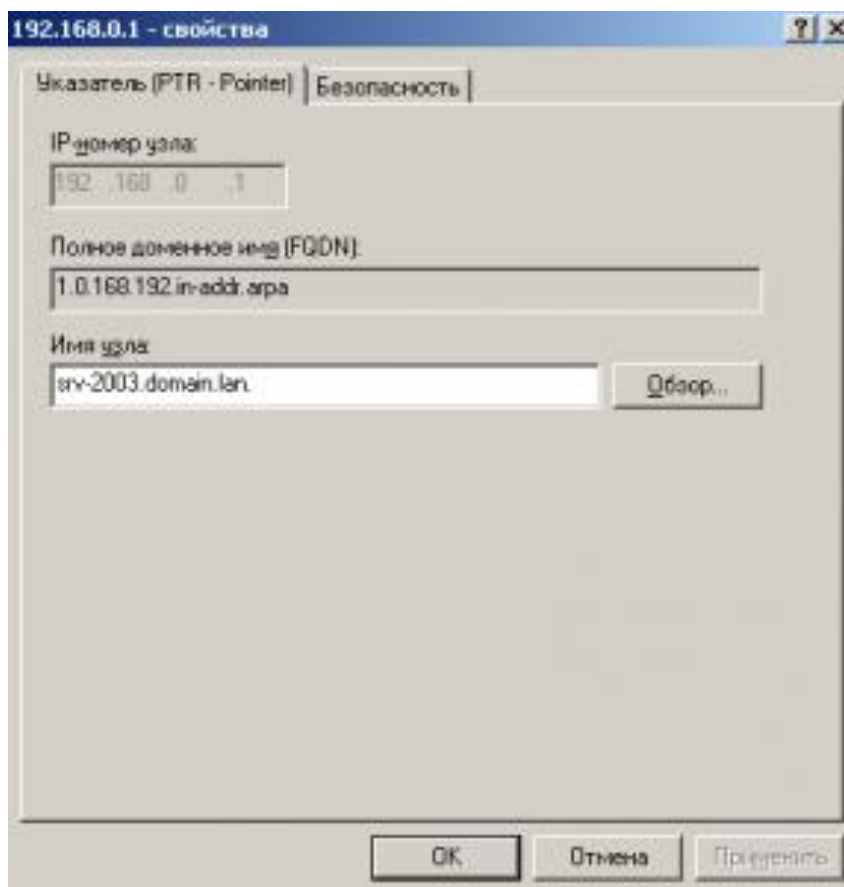


Рисунок 10.18 - Вкладка Указатель (PTR)

Проверка работы зон прямого и обратного просмотра

Далее вызовем командную строку и пропингуем наш сервер (рисунок 19). Видим, что зона прямого просмотра работает нормально и имени SRV-

2003 ставится в соответствие IP адрес 192.168.0.1.

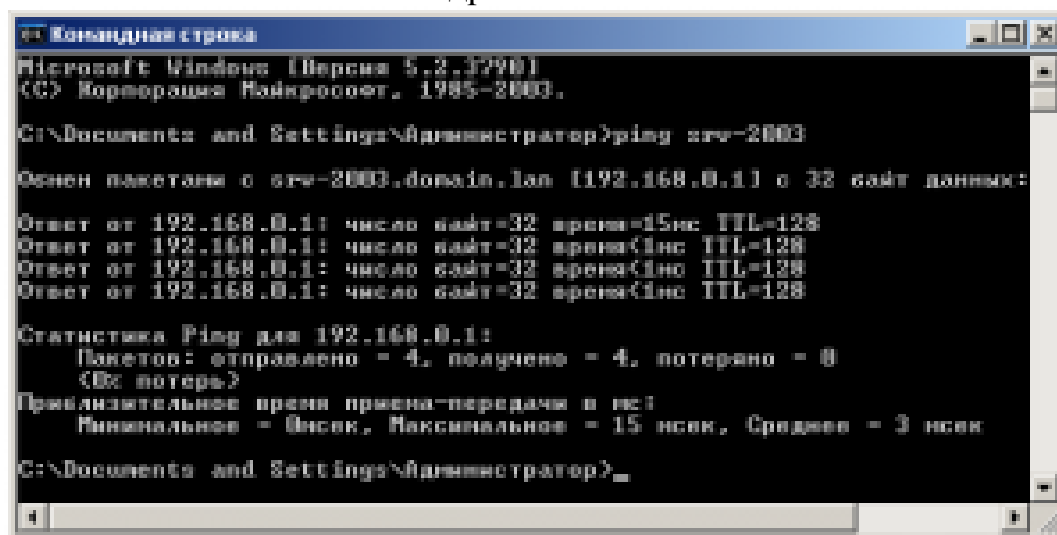


Рисунок 10.19 - Окно Командная строка

Если пропинговать не имя, а IP адрес и использовать ключ «-а», то увидим, что зона обратного просмотра также работает хорошо (рисунок 20). Обмен данными идет нормально.

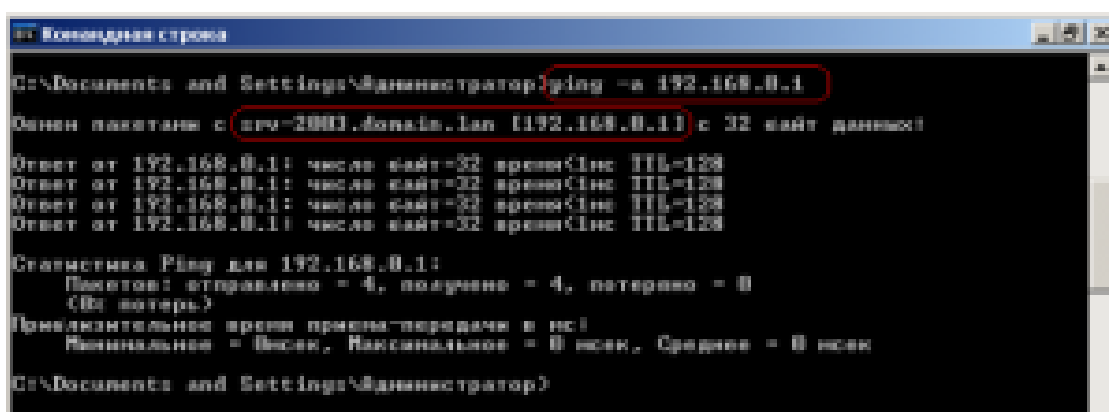


Рисунок 10.20 - Зона обратного просмотра работает хорошо

В этой работе мы произвели выбор для сервера роли DNS сервера, создали зоны прямого и обратного просмотра, а также проверили корректность работы этих зон.

Задание для самостоятельного выполнения

Настроить DNS роутер.

Контрольные вопросы

1. Каковы функции DNS сервера?

11 СОЗДАНИЕ ПОЛЬЗОВАТЕЛЕЙ ДОМЕНА

Цель работы

Научиться настраивать домен и создавать пользователей этого домена.

Теоретические сведения

Ресурсы в локальной сети

Давайте на сервере, на диске C:\ создадим две папки: **MUSIC** (только чтение), **VIDEO** (полный доступ) и затем откроем эти ресурсы для доступа пользователям (рисунок 11.1).

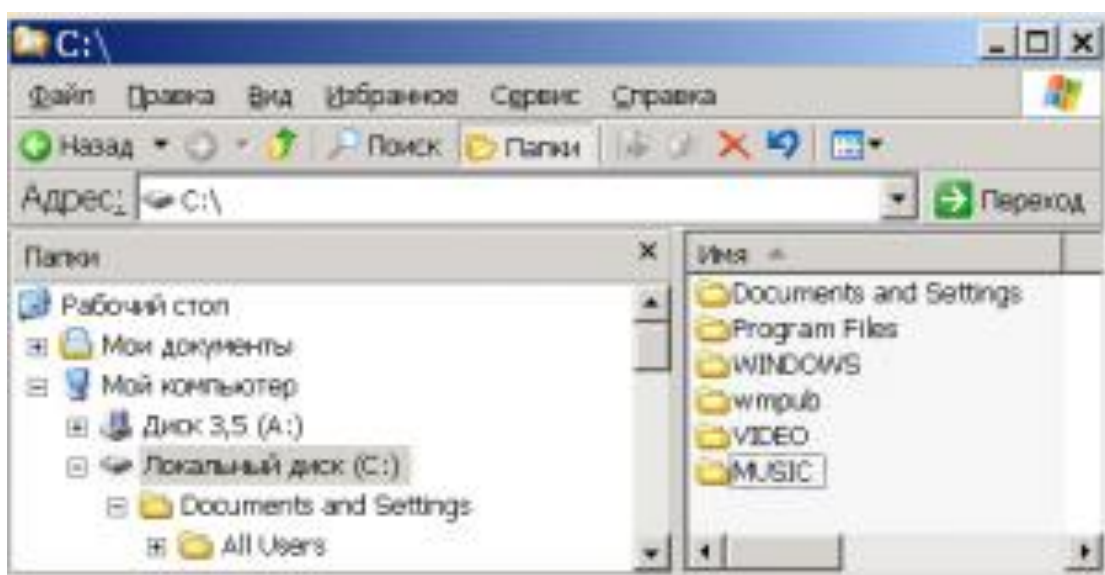


Рисунок 11.1 - На диске C:\ созданы две папки

Для назначения папкам требуемых атрибутов щелкнем на ней правой кнопкой мыши и выберем команду **Общий доступ и безопасность**. В данном окне установим переключатель **Открыть общий доступ** (рисунок 11.2).

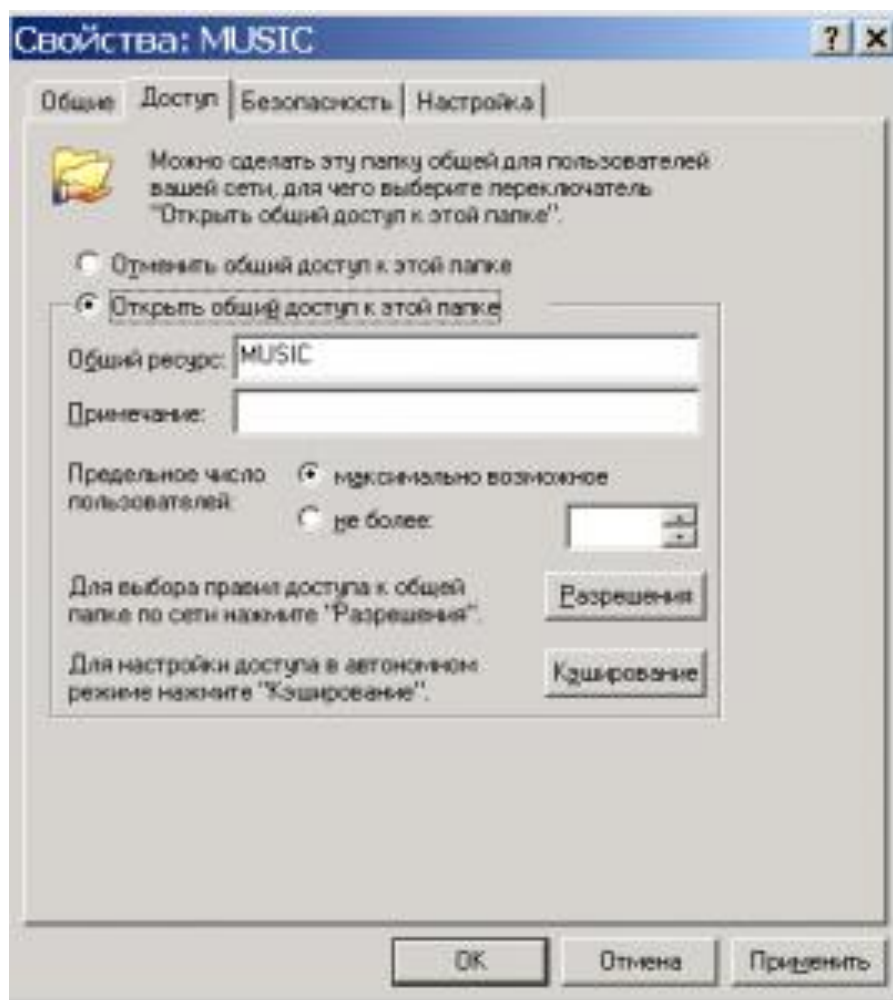


Рисунок 11.2 - Окно свойств папки Music

На вкладке **Разрешения** вы можете осуществить поиск пользователей домена и добавить их в пользователи папки MUSIC (рисунок 11.2). Для этого нужно выполнить команды **Добавить-Дополнительно-Поиск** и указать нужного пользователя. Строку **Все** пользователи, стоящую по умолчанию, следует удалить.

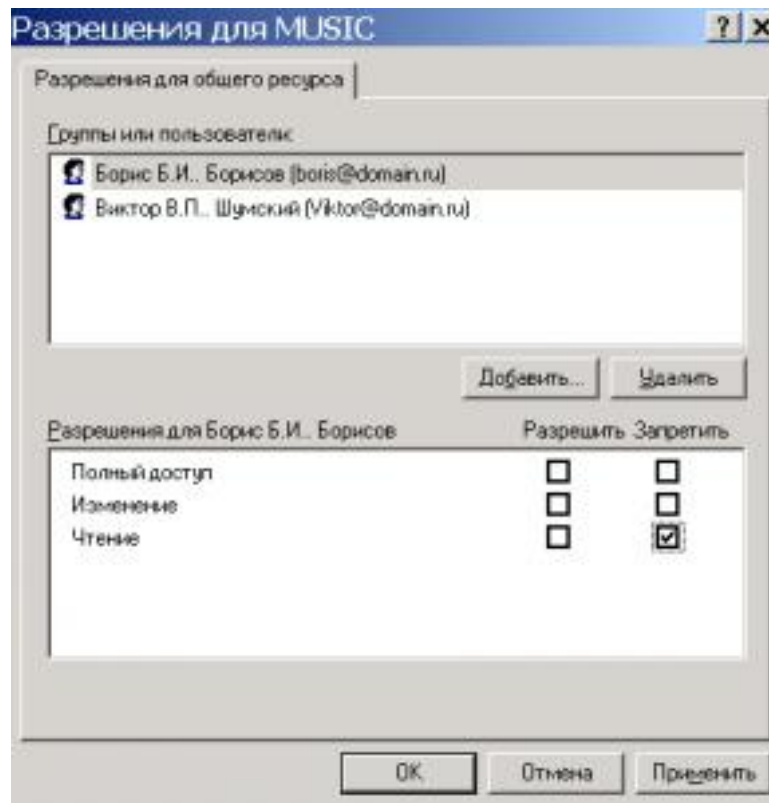


Рисунок 11.3 - Добавлены два пользователя с правом чтения папки MUSIC

Таким же образом устанавливается доступ для других папок (рисунок 11.3).

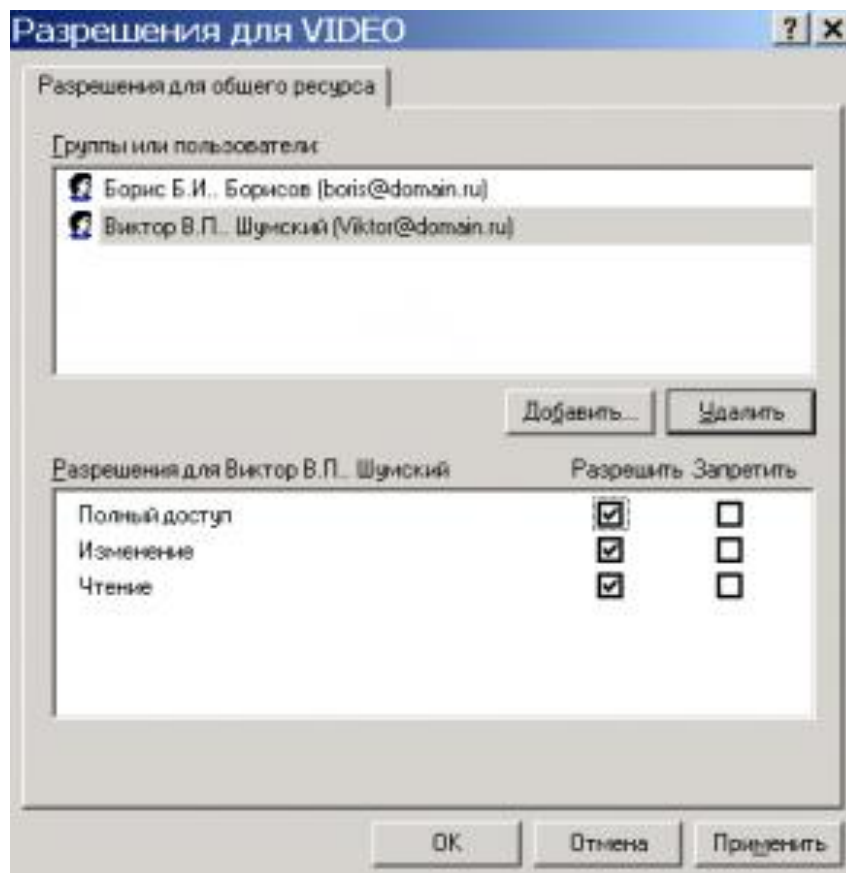


Рисунок 11.4 - К папке VIDEO пользователи имеют полный доступ

Перезагрузим и посмотрим, как эти ресурсы будут выглядеть со стороны клиента, для этого войдем в домен под именем пользователя Борисов (рисунки 11.5).

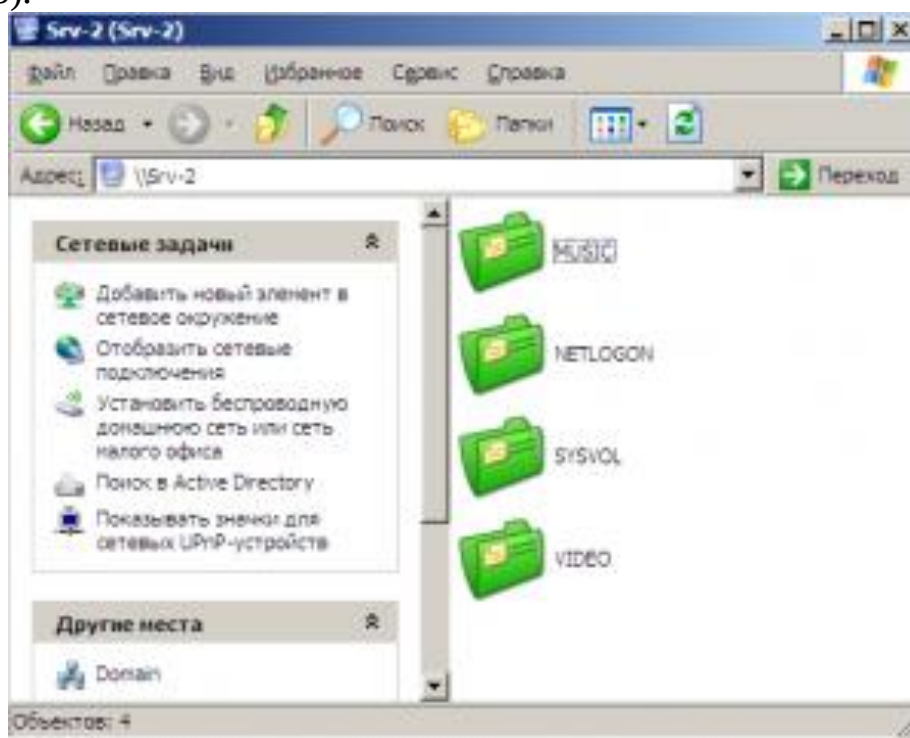


Рисунок 11.5 - Вид папок на сервере в сетевом окружении

Как вариант на клиенте можно выполнить команду **Пуск-Выполнить** и **\\Srv-2003**. Мы увидим, что со стороны клиента сетевые ресурсы сервера открыты и он может ими пользоваться согласно назначенным ему разрешениям. Пользователи, не входящие в домен, папки также увидят, но пользоваться ими не смогут (Для компьютеров, не входящих в домен папки закрыты).

В работе мы научились производить практические действия с консолью, создавать в домене подразделения, а в них-объекты. Научились организовывать доступ к ресурсам в локальной сети.

Задание для самостоятельного выполнения

Настроить домен сети, создать пользователей и добавлять ресурсы сети с разграниченным доступом.

Контрольные вопросы

1. В чем достоинства использования домена?

12 СОЗДАНИЕ ПОЛЬЗОВАТЕЛЕЙ СЕРВЕРОМ

Цель работы

Научиться создавать пользователей домена и настраивать политику безопасности.

Теоретические сведения

По умолчанию есть жесткие требования к паролям, но это неудобно и их можно изменить командой: Пуск-Панель управления-Администрирование-Политика безопасности домена. Затем Параметры безопасности-Политика безопасности-Политика паролей (рисунок 12.1).

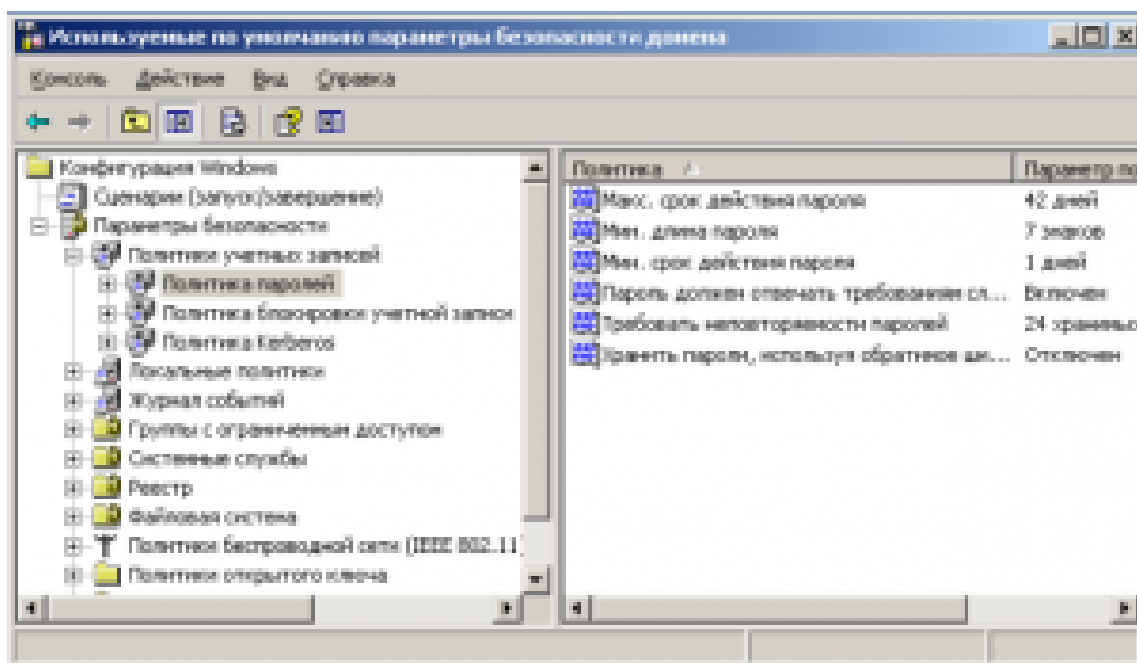


Рисунок 12.1 - Используемые по умолчанию параметры безопасности домена

Примечание

Политика паролей по умолчанию требует ввода больших и маленьких букв, также знаков и цифр. Поэтому учебный пароль может быть, например, такой 123456-Q.

Убираем переключатель того, что через 42 дня пароль нужно изменить (рисунок 12.2). Но, помним о том, что это снижает безопасность системы.

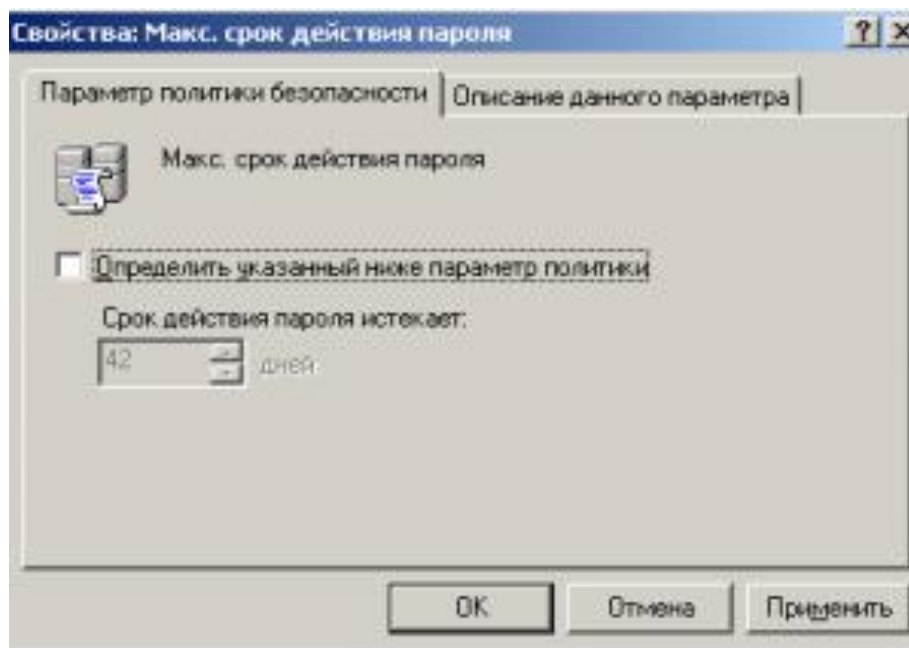


Рисунок 12.2 - Убираем этот флажок

По своему усмотрению поставим минимальную длину пароля в 6 знаков (рисунок 12.3).

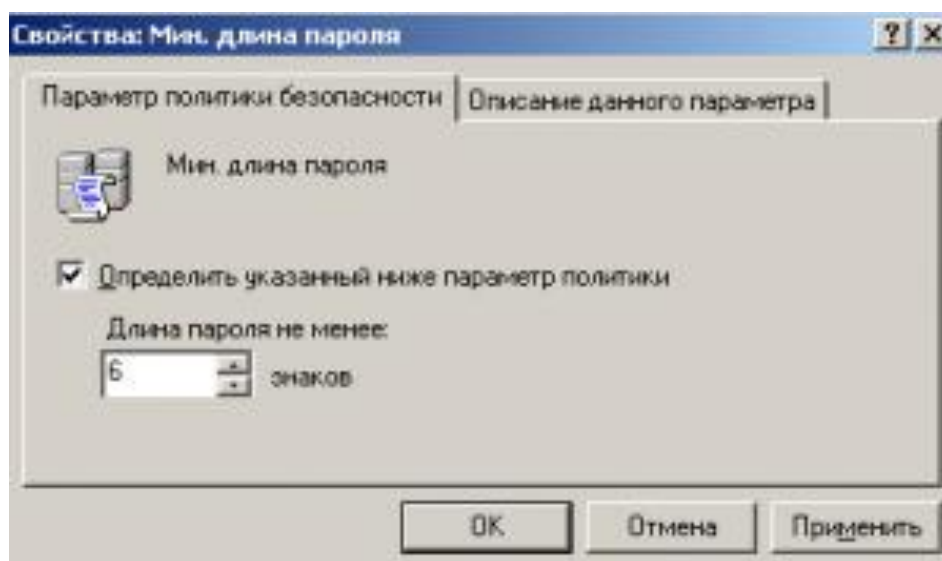


Рисунок 12.3 - Совсем отключать этот флажок не будем

Флажок требований сложности пароля (в учебных целях) отключим – рисунок 12.4.

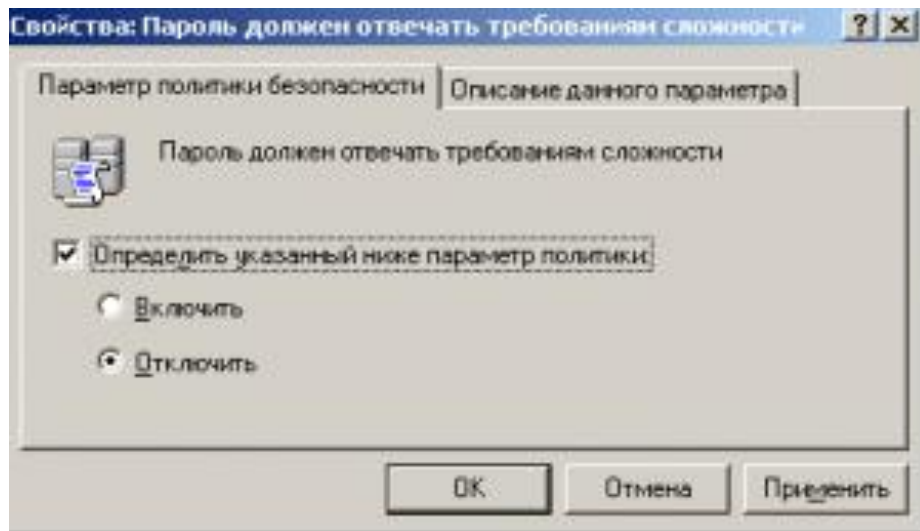


Рисунок 12.4 - Переключатель требований сложности пароля отключим

Примечание

Сложность пароля - мера эффективности, с которой пароль способен противостоять его угадыванию или методу полного перебора. В своей обычной форме сложность пароля является оценкой того, как много попыток в среднем потребуется взломщику, без прямого доступа к паролю, для его угадывания. Подробнее смотрите на сайте <http://windows.microsoft.com/ru-RU/windows7/Change-password-policy-settings>.

Политику неповторяемости паролей также отключим, так как пользователям это неудобно (рисунок 12.5).

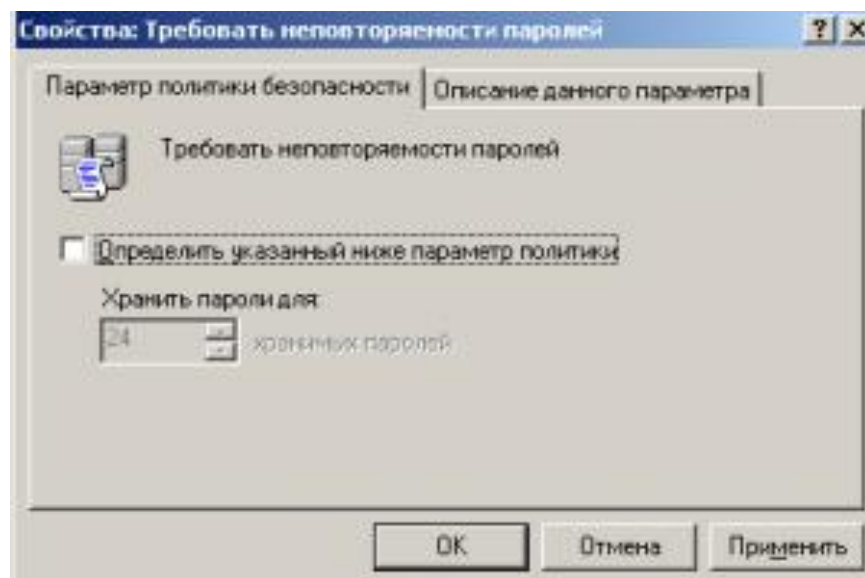


Рисунок 12.5 - Отключаем и этот флажок

Чтобы эти изменения были приняты, перезагружаем сервер.

Создаем пользователя

Для создания пользователя с доступом к домену SRV-2003.LAN выполните команду Пуск-Все программы-Администрирование-Службы компо-

нентов и в AD откройте Users (рисунки 12.6).

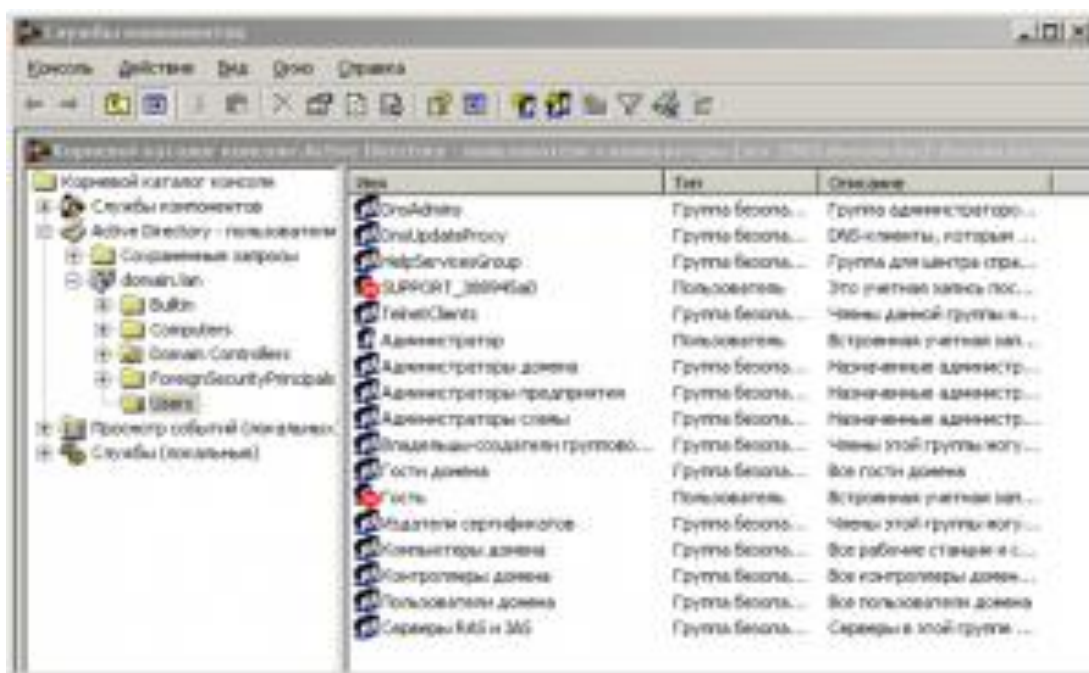


Рисунок 12.6 - Окно Службы компонентов

Для создания пользователя, который сможет использовать ресурсы нашей сети, щелкните правой кнопкой на папку Users и выберите команду Создать-Пользователь (рисунок 12.7). Графы заполним именами ваших друзей.



Рисунок 12.7 - Окно Пользователь

Далее необходимо задать пароль (рисунок 12.8). Флажки здесь вы можете поставить на ваше усмотрение.

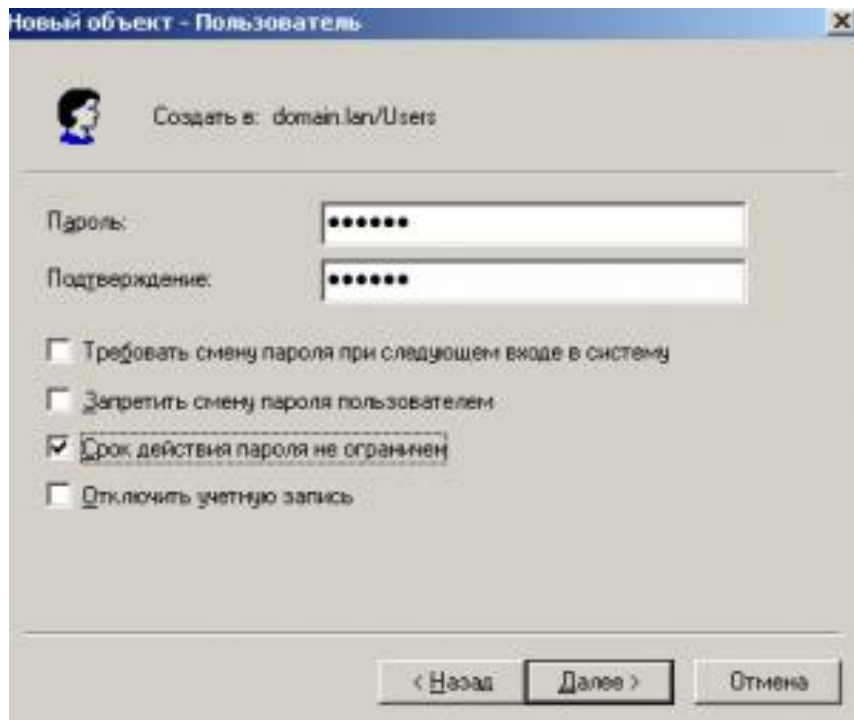


Рисунок 12.8 - Окно задания пароля пользователя

Пользователь создан (рисунок 12. 9).

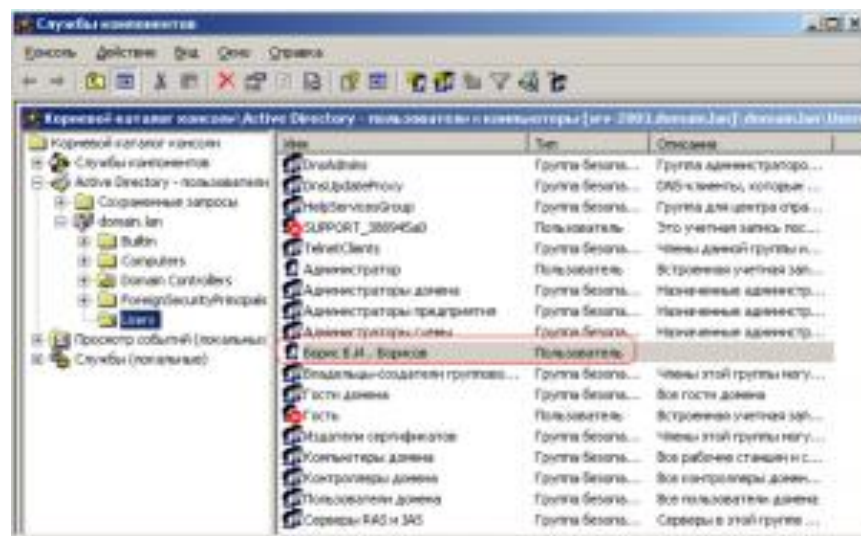


Рисунок 12.9 - Появился новый пользователь Борисов Б.И

Как работает учетная запись этого пользователя, мы сможем увидеть после того, как создадим в домене клиентский ПК.

Подключение клиента к домену

На виртуальной машине запускаем клиента (Windows XP) и сервер (Windows 2003 Server). Чтобы ПК могли связаться друг с другом, нужно выполнить некоторые предварительные настройки. Настраиваем брандмауэр, т.е. в исключения добавляем общий доступ к файлам и принтерам (рисунок 12.10).

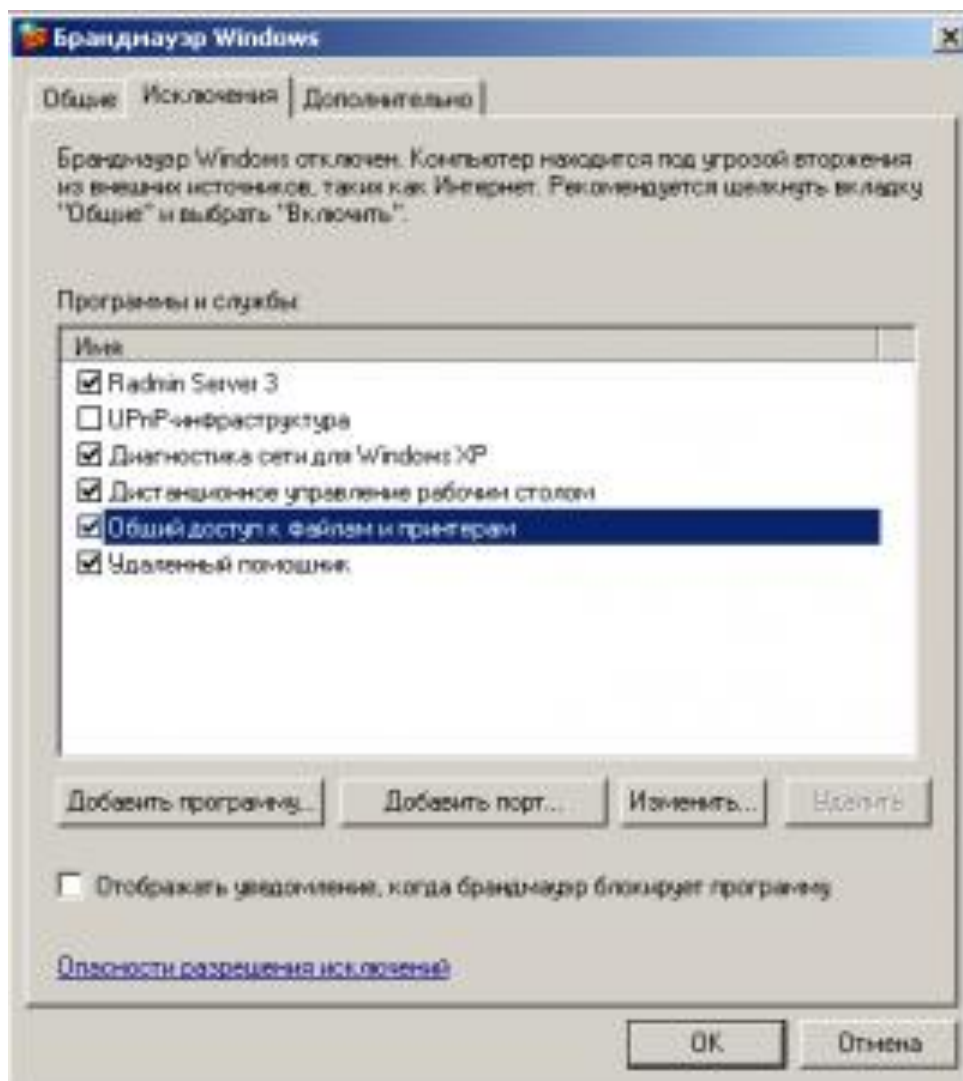


Рисунок 12.10 - Настраиваем вкладку Исключения

Дата и время на клиенте и сервере должны быть одинаковы. При этом лучше убрать флажок об автоматическом переходе на летнее время и обратно (рисунок 12.11).

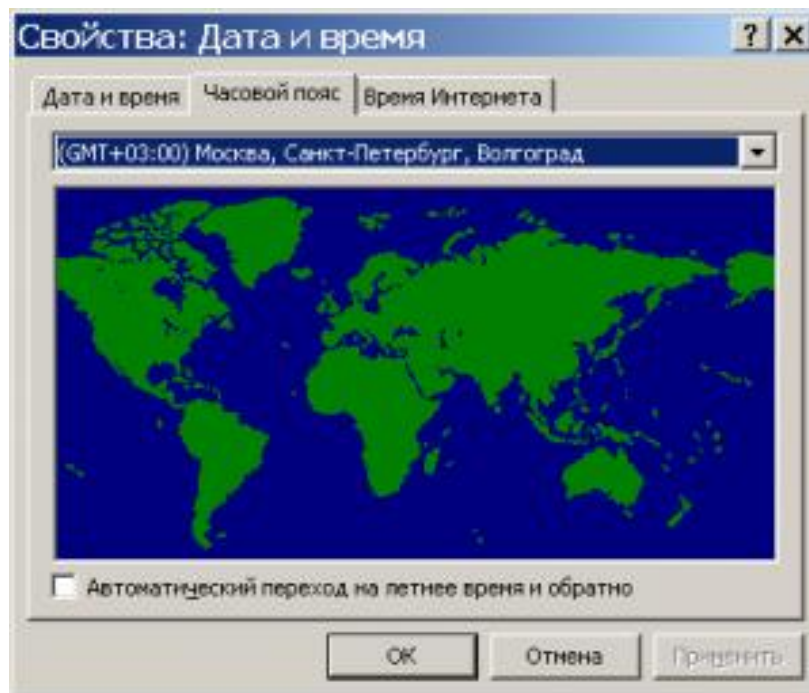


Рисунок 12.11 - Убираем флажок

В сетевых подключениях найдем и вручную (пока не настроен DHCP) настроим сетевые параметры клиента (рисунок 12.12).

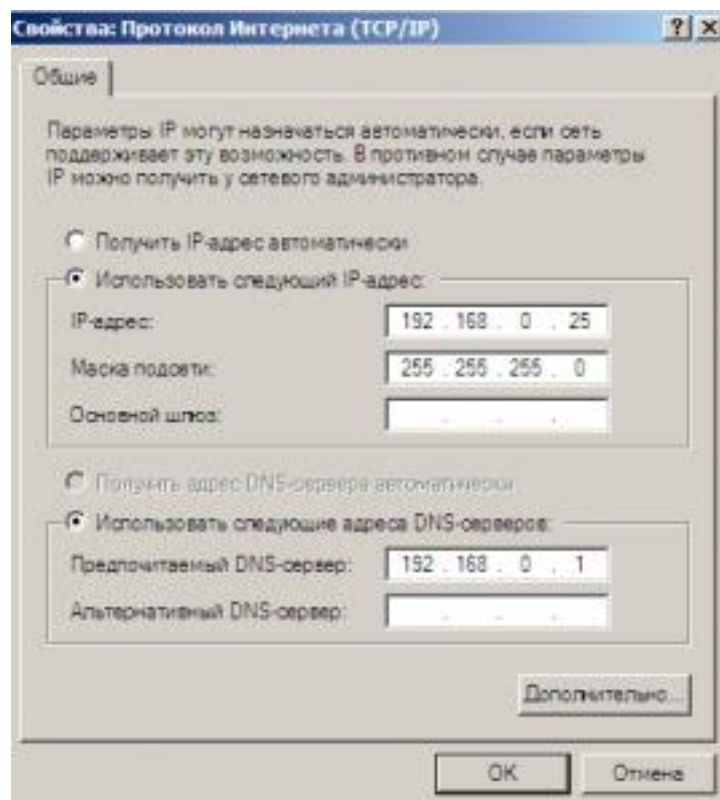


Рисунок 12.12 - Настраиваем протокол TCP/IP

Первый способ подключения ПК к домену – указать его вместо рабочей группы в окне Изменение имени компьютера (рисунок 12.13).

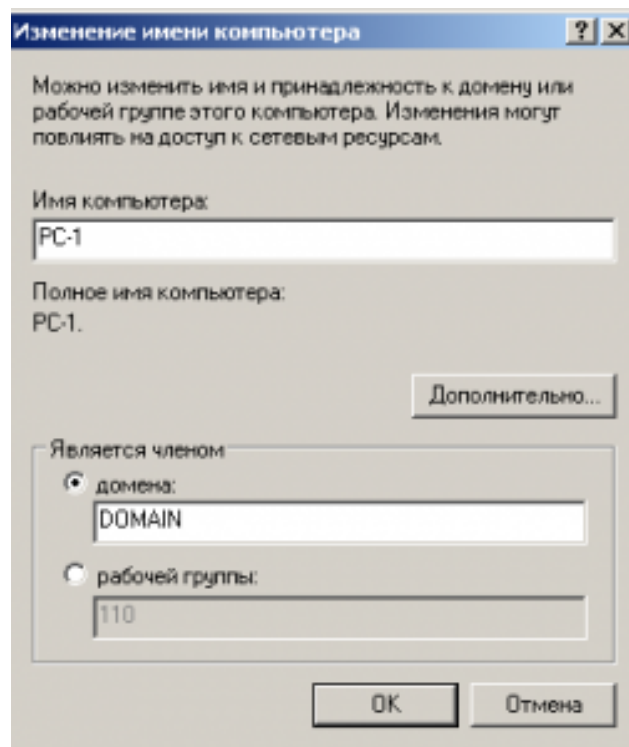


Рисунок 12.13 - Ввод имени нашего домена

После нажатия ОК введите имя и пароль (рисунок 12.14).

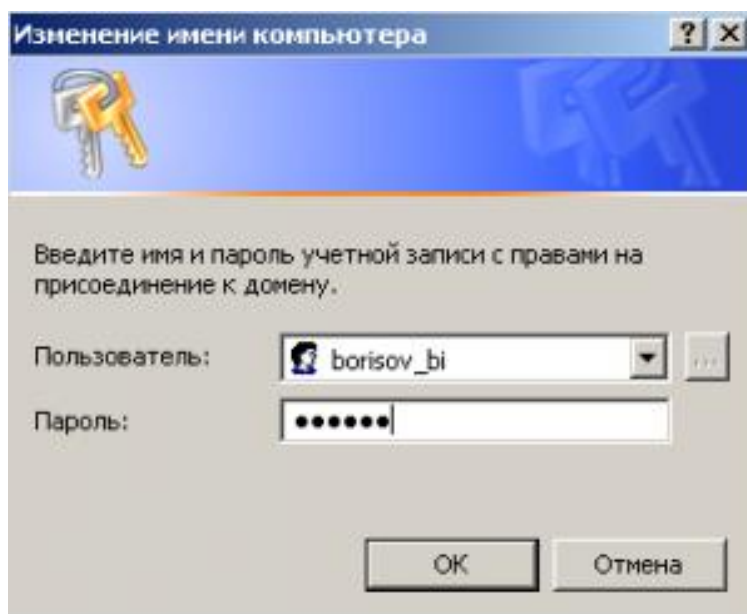


Рисунок 12.14 - Окно Изменение имени компьютера

Теперь, после перезагрузки клиента, пользователь может входить в домен (рисунок 12.15).



Рисунок 12.15 - Окно входа клиента в домен

Не путайте название вашего сервера SRV-2003 с названием домена DOMAIN. Уточнить название домена можно из сетевого окружения или при входе в систему, или – в окне Свойства системы на сервере (рисунок 12.16).

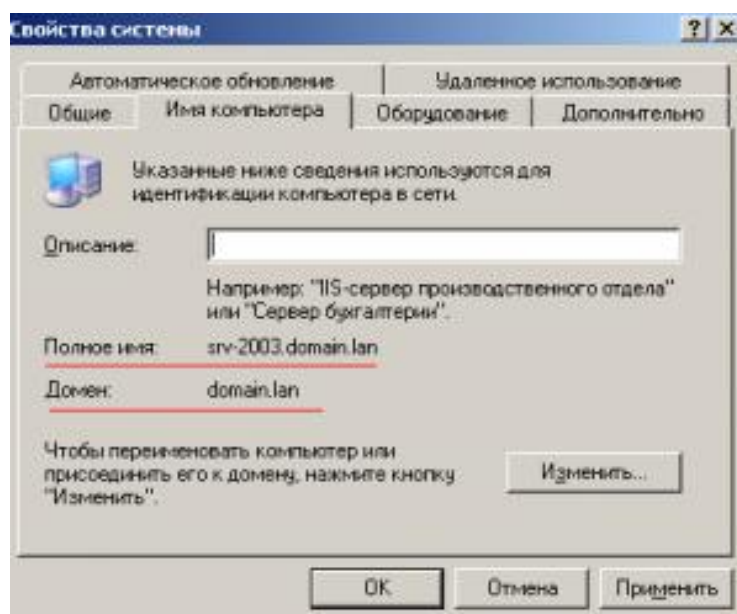


Рисунок 12.16 - Окно Свойства системы на сервере

Второй вариант создания входа в домен - нажать на кнопку Идентификация на клиенте и запустить мастера подключения ПК в домен (рисунок 12.17) и (рисунок 12.18).

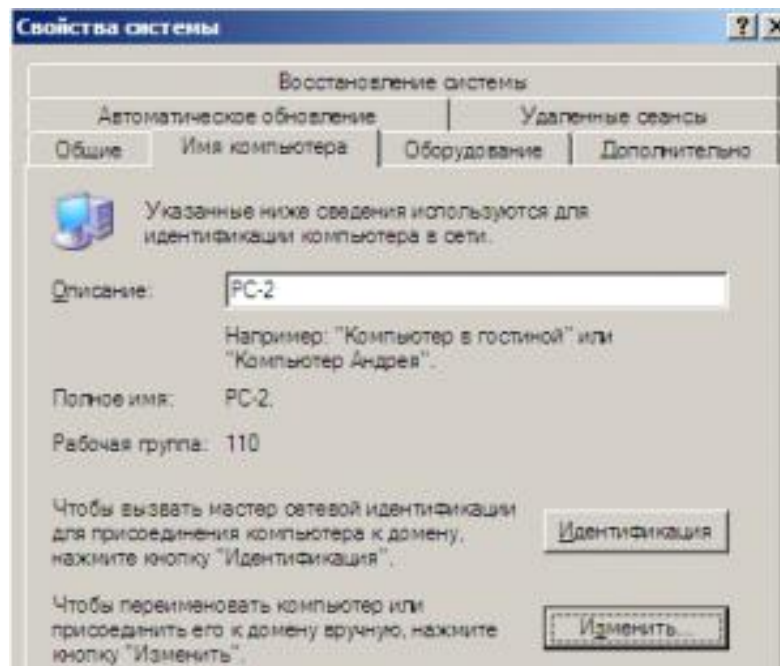


Рисунок 12.17 - Окно Свойства системы на клиенте

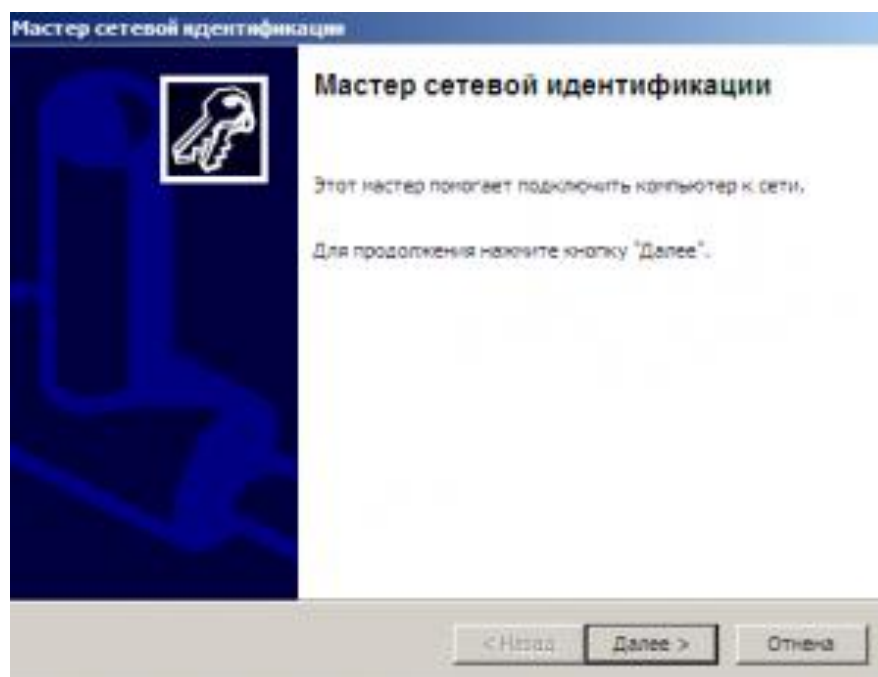


Рисунок 12.18 - Окно Мастер сетевой идентификации

Далее мы рассмотрим только окна с настройками, отличными от умолчаний (рисунок 12.19).

Мастер сетевой идентификации

Сведения об учетной записи пользователя и домене
Учетная запись пользователя определяет доступ к сетевым файлам и ресурсам.

Введите свое имя пользователя и пароль. Если вы их не знаете, то обратитесь к сетевому администратору.

Пользователь: borisov_bi

Пароль: *****

Домен: DOMAIN

< Назад Далее > Отмена

Рисунок 12.19 - Заполняем учетные данные пользователя в домене

Теперь указываем имя ПК и название домена (рисунок 12.20).

Мастер сетевой идентификации

Домен компьютера
Ваш компьютер должен принадлежать к домену.

В домене DOMAIN учетную запись для вашего компьютера найти не удалось. Введите имя компьютера и домен, к которому он принадлежит (этот домен может отличаться от домена, к которому принадлежит учетная запись пользователя).

Имя компьютера: PC-2

Домен компьютера: DOMAIN

< Назад Далее > Отмена

Рисунок 12.20 - Задаем имя ПК и название домена

Далее заполняем данные учетной записи пользователя (рисунок 12.21) или администратора сервера (рисунок 12.22).

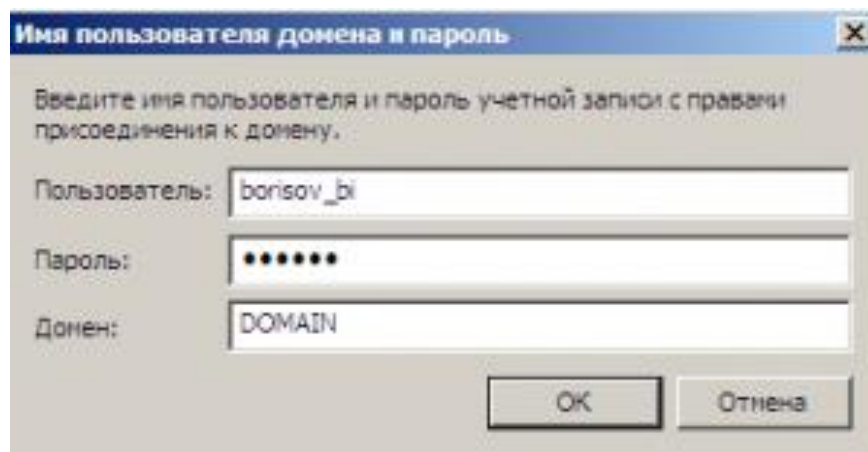


Рисунок 12.21 - Вводим учетные данные пользователя

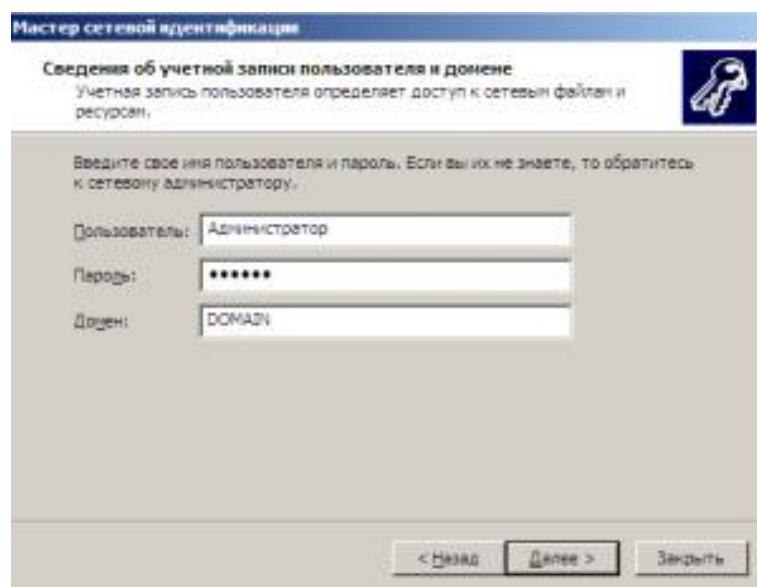


Рисунок 12.22 - Вводим учетные записи администратора сервера

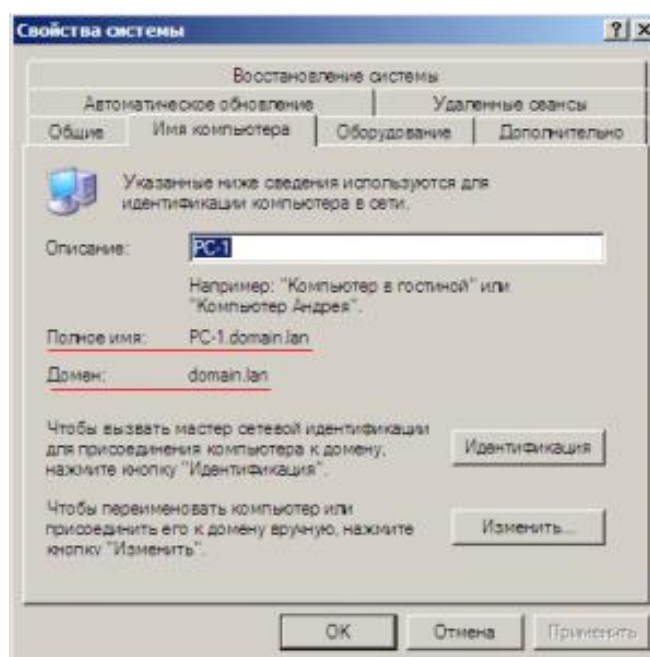


Рисунок 12.23 - Окно Свойства системы

Теперь мы можем или входить в клиентский ПК, или в домен (рисунок 12.24) и (рисунок 12.25).

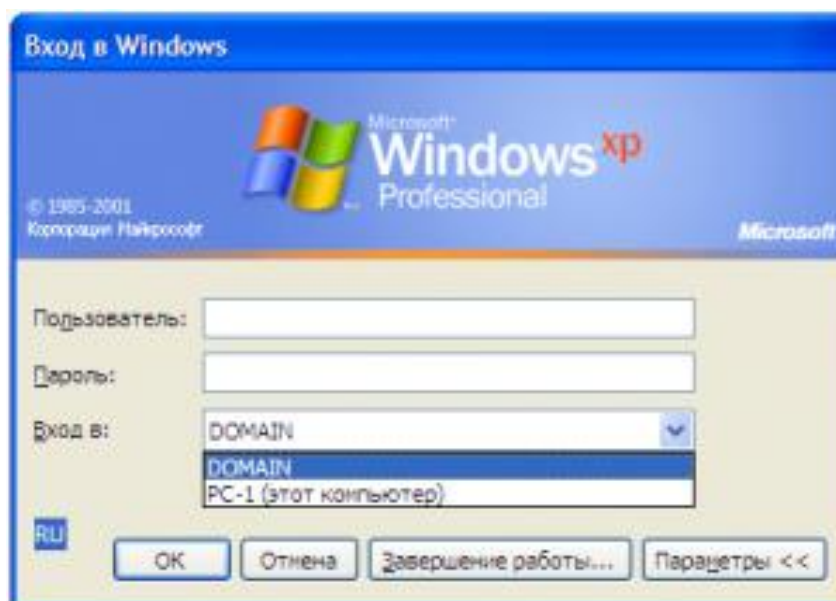


Рисунок 12.24 - Окно выбора вариантов входа в Windows



Рисунок 12.25 - Два варианта входа в ОС (Эти данные берутся из AD)

Обзор сетевого окружения

Если нажать на значок Вся сеть, то мы увидим рабочую группу и домен (рисунок 12.26).

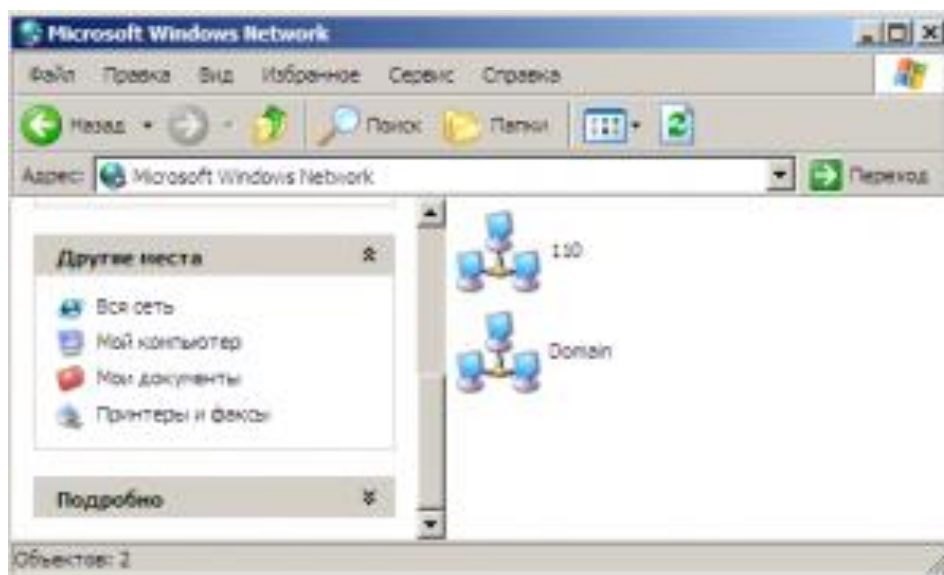


Рисунок 12.26 - Рабочая группа 110, домен – Domain

Если войти в домен, то увидим там сервер и два клиентских ПК (рисунок 12.27). При желании можно создать общие папки и другие ресурсы, это мы уже проходили и умеем.



Рисунок 12.27 - Сервер Srv-2003, клиенты PC-1 и PC-2

Таким образом, мы можем теперь войти с клиентского ПК на сервер и наоборот – с сервера на клиентский ПК. Наши ПК видят друг друга и могут общаться в сети.

Войдите в клиент как Администратор и в командной строке наберите netconfigserver, чтобы посмотреть конфигурацию клиента (рисунок 12.28).

```

C:\windows\system32\cmd.exe
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\Администратор>net config server
Настройка сервера
Комментарий для сервера          \\\FC-1
                                   FC-1
Версия программы                  Windows 2002
Включен сервер на
    Netbios_Smb <ON>
    NetBI_Tcpip_149358D3E-3C22-41A6-AB07-1ECCF87740EA <ON>296545ff>

Скрытый сервер                     No
Максимальное число пользователей 10
Максимальное число открытых файлов в сеансе 16384
Время холостого хода сеанса (мин) 15
Команда выполнена успешно.

C:\Documents and Settings\Администратор>

```

Рисунок 12.28 - Смотрим конфигурацию ПК

Если имеется запись Скрытый сервер No, то ПК отображается в сетевом окружении, если имеется строчка Скрытый сервер Yes, то ПК не отображается в сетевом окружении. Чтобы ПК был скрыт в сети и не отображался в сетевом окружении, здесь набирается команда netconfigserver /hidden:yes (рисунок 12.29).

```

C:\Documents and Settings\Администратор>net config server /hidden:yes
Команда выполнена успешно.

Скрытый сервер                      Yes

```

Рисунок 12.29 - Теперь ПК не отображается в сетевом окружении

Команда скрывает ПК из сетевого окружения не сразу – надо подождать (Потребуется перезагрузка ПК).

Чтобы на клиенте можно было устанавливать ПО входить в него нужно под записью Администратор, или Борисова Б.А. включить в группу администраторов.

Вопрос. Как вы думаете, зачем нужна команда, показанная ниже: Теперь ПК не отображался в сетевом окружении.

В работе мы изучили, как можно менять требования к паролям пользователей и создали первого простого пользователя доменом (не администратора). Далее мы произвели подключение клиента к домену и произвели обзор сетевого окружения.

Задание для самостоятельного выполнения

Создать пользователей домена и настроить политику безопасности.

Контрольные вопросы

2. Что такое политика безопасности?

13 КОНТРОЛЬНАЯ РАБОТА

Содержание отчета по контрольной работе: фамилия, имя, вариант

1. задание
2. вычисления и результаты
3. расчетные таблицы
4. выводы

Задание 1

Указать запрещенные для конечных узлов IP-адреса и объяснить причину.

Задание 2

Указать к какому классу принадлежит IP-адрес и чему равен № сети и № узла.

Задание 3

Для IP-адреса указана маска. Определить № сети и № узла.

Задание 4

Разбить заданную сеть на 4 равных подсети и указать в каждой подсети количество узлов и отведенные им адреса.

Задание 5

Разбить сеть на три подсети наиболее экономичным способом. Количество ПК в каждой подсети: N1, N2, N3. Указать для каждой подсети распределение адресного пространства, а также резерв адресов.

Варианты контрольной работы

Вариант 1	Вариант 2	Вариант 3	Вариант 4
1. Указать запрещенные для конечных узлов IP-адреса и объяснить причину: 127.0.0.0 129.68.7.1 156.9.0.255 255.255.0.8 251.6.54.2	1. Указать запрещенные для конечных узлов IP-адреса и объяснить причину: 0.0.0.19 129.68.255.255 334.6.0.1 255.5.0.8 230.6.54.2	1. Указать запрещенные для конечных узлов IP-адреса и объяснить причину: 225.0.0.19 129.68.255.255 127.26.0.81 255.255.0.98 192.16.154.92	1. Указать запрещенные для конечных узлов IP-адреса и объяснить причину: 165.0.50.255 149.58.0.0 0.26.0.81 101.255.0.98 127.16.154.92
2. К какому классу принадлежит IP-адрес и чему равен № сети и № узла: 57.9.32.4 173.84.0.6 203.7.85.9 243.8.79.6	2. К какому классу принадлежит IP-адрес и чему равен № сети и № узла: 230.9.32.4 78.84.0.6 135.7.85.9 199.8.79.6	2. К какому классу принадлежит IP-адрес и чему равен № сети и № узла: 165.19.232.4 197.154.40.26 35.77.185.49 229.38.79.86	2. К какому классу принадлежит IP-адрес и чему равен № сети и № узла: 235.49.52.44 97.59.240.76 201.77.83.46 129.28.94.6
3. Для IP-адреса указана маска. Определить № сети и № узла: A=152.285.98.54 M=255.255.224.0	3. Для IP-адреса указана маска. Определить № сети и № узла: A=147.271.65.204	3. Для IP-адреса указана маска. Определить № сети и № узла: A=168.91.102.164	3. Для IP-адреса указана маска. Определить № сети и № узла: A=176.121.95.76 M=255.255.248.0

4. Разбить сеть 172.17.0.0 на 4 равных подсети и указать в каждой подсети количество узлов и отведенные им адреса. 5. Разбить сеть 192.168.17.0 на три подсети наиболее экономичным способом. Количество ПК в каждой подсети: N1 = 20, N2 = 15, N3 = 50. Указать для каждой подсети распределение адресного пространства, а также резерв адресов.	M= 255.255.240.0 4. Разбить сеть 146.87.0.0 на 4 равных подсети и указать в каждой подсети количество узлов и отведенные им адреса. 5. Разбить сеть 192.168.255.0 на три подсети наиболее экономичным способом. Количество ПК в каждой подсети: N1 = 50, N2 = 28, N3 = 4. Указать для каждой подсети распределение адресного пространства, а также резерв адресов.	M= 255.255.248.0 4. Разбить сеть 183.237.0.0 на 4 равных подсети и указать в каждой подсети количество узлов и отведенные им адреса. 5. Разбить сеть 192.168.95.0 на три подсети наиболее экономичным способом. Количество ПК в каждой подсети: N1 = 90, N2 = 60, N3 = 10. Указать для каждой подсети распределение адресного пространства, а также резерв адресов.	4. Разбить сеть 156.98.0.0 на 4 равных подсети и указать в каждой подсети количество узлов и отведенные им адреса. 5. Разбить сеть 192.168.150.0 на три подсети наиболее экономичным способом. Количество ПК в каждой подсети: N1 = 80, N2 = 20, N3 = 32. Указать для каждой подсети распределение адресного пространства, а также резерв адресов.
---	---	--	--

Примеры выполнения задания

Пример выполнения задания 1

Указать запрещенные для конечных узлов IP-адреса и объяснить причину.

127.255.20.7
 192.60.31.255
 0.167.35.71
 145.73.0.0
 160.255.01.98

Решение:

Для конечного узла запрещены адреса, не удовлетворяющие ограничениям:

A = 127.255.20.7 - этот адрес используется для тестирования;

A = 192.60.31.255 - адрес класса C. № узла не может быть равным 11111111₂ (255₁₀);

A = 0.167.35.71 - № сети не может быть равным 0;

A = 145.73.0.0 - адрес класса B. № узла не может быть равным 0.

A = 160.255.01.98 - разрешенный для конечных узлов адрес, т.к. удовлетворяет этим ограничениям.

Пример выполнения задания 2

К какому классу принадлежит IP-адрес и чему равен № сети и № узла?

148.35.0.41
 63.41.2.17
 201.13.10.19
 225.80.37.9

Решение:

Класс IP-адреса определяется по значению первого байта IP-адреса (см. таблицу 1). Количество байт, отведенных под номер сети и номер узла, зависят от класса IP-адреса (см. рис 1).

A = 148.35.0.41 принадлежит классу B, т.к. $128 < 148 < 191$.

В классе B под № сети и № узла отведено по 2 байта, поэтому

№ сети = 148.35.0.0, а № узла = 0.0.0.41;

A = 63.41.2.17 принадлежит классу A, т.к. $1 < 63 < 126$.

В классе A под № сети отведен 1 байт, а под № узла отведено 3 байта, поэтому

№ сети = 63.0.0.0, а № узла = 0.41.2.17;

A = 201.13.10.19 принадлежит классу C, т.к. $192 < 201 < 223$.

В классе C под № сети отведено 3 байта, а под № узла отведен 1 байт, поэтому

№ сети = 201.13.10.0, а № узла = 0.0.0.19;

A = 225.80.37.9 принадлежит классу D, т.к. $224 < 225 < 239$.

Он не содержит № сети и № узла, т.к. является групповым адресом.

Пример выполнения задания 3

Для IP-адреса указана маска. Определить № сети и № узла.

A = 129.44.78.200

M = 255.255.192.0

Решение:

Т.к. двоичная запись маски содержит единицы в тех разрядах, которые соответствуют номеру сети в IP-адресе, то необходимо перевести маску и IP-адрес в двоичный код. Разряды IP-адреса, соответствующие непрерывной последовательности двоичных единиц в маске зададут № сети, а остальные разряды IP-адреса (соответствующие непрерывной последовательности двоичных нулей) - номер узла.

Для простоты ограничимся переводом в двоичный код только третьих байтов IP-адреса и маски (78 и 192 соответственно), поскольку $255_{10} = 11111111_2$, а $0_{10} = 00000000_2$. Получим $78_{10} = 01001110_2$, а $192_{10} = 11000000_2$, тогда:

A = 129. 44. 0 1 0 0 1 1 1 0.200

M = 255.255.1 1 00 0000.0

№ сети	№ узла
--------	--------

Отсюда,

№ сети = 129.44.01000000.0 = 129.44.64.0

№ узла = 0.0.00001110.200 = 0.0.14.200

Пример выполнения задания 4

Разбить заданную сеть 157.168.0.0 на 4 равных подсети и указать в каждой подсети количество узлов и отведенные им адреса:

Решение:

Адрес сети A = 157.168. 0.0 принадлежит классу B. Количество узлов

данной сети равно $2^m - 2 = 2^{16} - 2$. Маска этого класса 255.255.0.0.

Для разбиения сети на 4 равных подсети надо выбрать маску постоянной длины $M = 255.255.192.0$ (см. таблицу 2), т.к. $n = 2$. Поскольку для выбранной маски (255.255.192.0) $m = 14$, то количество узлов каждой подсети будет равно $2^m - 2 = 2^{14} - 2$. Запрещенными для узлов каждой подсети будут адреса из всех 0_2 и из всех 1_2 .

Подсеть 1		
Адрес подсети и маска	Диапазон адресов	Запрещенные адреса
$A_1 = 157.168. 0.0$ $M = 255.255.192.0$	157.168. 0.0- 157.168. 63.255	157.168. 0.0 157.168. 63.255

Подсеть 2		
Адрес подсети	Диапазон адресов	Запрещенные адреса
$A_2 = 157.168.64.0$ $M = 255.255.192.0$	157.168. 64.0-157.168. 127.255	157.168.64.0 157.168. 127.255

Подсеть 3		
Адрес подсети	Диапазон адресов	Запрещенные адреса
$A_3 = 157.168.128.0$ $M = 255.255.192.0$	157.168. 128.0- 157.191.255	157.168.128.0 157.168. 191.255

Подсеть 4		
Адрес подсети	Диапазон адресов	Запрещенные адреса
$A_4 = 157.168.192.0$ $M = 255.255.192.0$	157.168. 192.0-157.255.255	157.168.192.0 157.168. 255.255

Пример выполнения задания 5

Разбить сеть 192.168.10.0 на три подсети наиболее экономичным способом. Количество ПК в каждой подсети: $N_1 = 2$, $N_2 = 16$, $N_3 = 100$. Указать для каждой подсети распределение адресного пространства, а также резерв адресов.

Решение:

Адрес сети $A = 192.168.10.0$ принадлежит классу C. Маска этого класса 255.255. 255.0. Количество узлов данной сети равно $2^m - 2 = 2^8 - 2 = 254$. Для разбиения сети на 3 подсети наиболее экономичным способом (неиспользуемых адресов должно быть, как можно меньше) необходимо применять маски переменной длины. При этом для каждой подсети надо выбрать

наиболее подходящую по количеству узлов маску. Рассчитаем число подсетей и число узлов для всех возможных значений маски сети класса С и составим таблицу:

Маска	Двоичное значение последнего байта маски	n	m	Число подсетей	Число узлов
255.255.255.0	00000000 ₂	24	8	1	254
255.255.255.128	10000000 ₂	25	7	2	126
255.255.255.192	11000000 ₂	26	6	4	62
255.255.255.224	11100000 ₂	27	5	8	30
255.255.255.240	11110000 ₂	28	4	16	14
255.255.255.248	11111000 ₂	29	3	32	6
255.255.255.252	11111100 ₂	30	2	64	2

Из последнего столбца таблицы видно, что для сети с 2 ПК наиболее подходит маска 255.255.255.252, для сети с 16 ПК наиболее подходит маска 255.255.255.224, для сети со 100 ПК наиболее подходит маска 255.255.255.128.

Теперь выполним разбиение сети 192.168.10.0 на 3 подсети с количеством узлов 100,16,2.

Подсеть 1, 100 ПК

$A_1 = 192.168.0.0$

$M_1 = 255.255.255.128$ (126 узлов)

Диапазон адресов = 192.168.10.0 ÷ 192.168.10.127 (128 адресов)

Запрещенные адреса = 192.168.10.0 и 192.168.10.127

Адреса для 100 ПК = 192.168.10.1 ÷ 192.168.10.100

Свободные адреса = 192.168.10.101 ÷ 192.168.10.126 (26 адресов)

Подсеть 2, 16 ПК

$A_1 = 192.168.10.128$

$M_1 = 255.255.255.224$ (30 узлов)

Диапазон адресов = 192.168.10.128 ÷ 192.168.10.159 (32 адреса)

Запрещенные адреса = 192.168.10.128 и 192.168.10.159

Адреса для 100 ПК = 192.168.10.129 ÷ 192.168.10.144

Свободные адреса = 192.168.10.145 ÷ 192.168.10.158 (14 адресов)

Подсеть 3, 2 ПК

$A_1 = 192.168.10.160$

$M_1 = 255.255.255.252$ (2 узла)

Диапазон адресов = 192.168.10.160 ÷ 192.168.10.163 (4 адреса)

Запрещенные адреса = 192.168.10.160 и 192.168.10.163

Адреса для 100 ПК = 192.168.10.129 ÷ 192.168.10.144

Свободные адреса отсутствуют

Свободные адреса для новых сетей = $192.168.10.164 \div 192.168.10.254$
(101 адрес)
Запрещенный адрес = 192.168.10.255

14 ИЗУЧЕНИЕ ВСТРОЕННЫХ СРЕДСТВ ДИАГНОСТИКИ В ОС - WMIC

Цель работы

Рассмотреть и изучить возможности встроенных средств управления рабочей станцией с использованием системы Windows Management Instrumentation, просмотреть базовые настройки персонального компьютера, проанализировать сетевые настройки компьютера представленныеhtml-формате.

Теоретические сведения

При выполнении заданий лабораторной работы рекомендуется ознакомиться с материалами: Встроенная помощь ОС MS Windows «Центр справки и поддержки»: поиск по ключу «wmic » , «makescab», «expand»

Встроенная помощь к программам OS MS Windows - при помощи команды: wmic /?.

Ознакомиться с теоретическими сведениями, сохранить основные в отчет.

Программа WMIC (WMI Command-line) предоставляет простой интерфейс командной строки для работы с подсистемой

WMI (Windows Management Instrumentation - Инструментарийуправления Windows). Это позволяет воспользоваться преимуществами WMI для управления компьютерами с операционными системами Microsoft Windows. WMIC взаимодействует с существующими оболочками и служебными программами, а также может быть легко расширена с помощью сценариев или других административным приложений.

WMIC 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 WMIC.

Поставщики WMI позволяют управлять различными аппаратными компонентами, подсистемами операционной системы иприкладными системами.

WMIC можно использовать со всеми схемами, внедряемыми поставщиками WMI. WMIC можно использовать с любого компьютера, на котором включена WMIC, для удаленного управления любым компьютером с WMI.

При этом наличие WMIC на удаленном управляемом компьютере не обязательно.

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).

Просмотреть параметры компьютера, используя командную строку и программу wmic:

wmic /? - Ознакомиться с командами WMIC
wmic BASEBOARD get /value | more - Управление системной платой.
wmic BIOS get /value | more - Управление базовой системой ввода-вывода (BIOS).
wmic BOOTCONFIG get /value | more - Управление конфигурацией загрузки.
wmic COMPUTERSYSTEM get /value | more - Управление компьютером.
wmic CPU get /value | more Управление ЦП

Сохранить непустые данные в отчет в виде скриншотов.

Просмотреть параметры сетевого подключения компьютера в html-формате:

```
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
```

Посмотреть параметры сетевой платы

```
wmic PATH «Win32_Environment.Name='PROCESSOR_IDENTIFIER'» GET VariableValue> Ethernet.htm
```

```
wmic nic where (NetConnectionID =»Подключениепо локальнойсети») get /format:mof>> Ethernet.htm
```

Определить индекс сетевой платы:

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

В следующей строке заменить XX на реальное значение и выполнить следующую команду:

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

В интернет найти форумы или статьи о возможностях использования WMIC, вставить их в отчет со ссылками.

Содержание отчета

1. Тема, цель, фамилия, имя
2. Теоретические сведения по «wmic » , «makescab», «expand»
3. Скриншоты работы с командной строкой по п.3,4,5,6
4. Форум или статья по п.7

15 ПРОЕКТИРОВАНИЕ ЛОКАЛЬНОЙ СЕТИ

Цель работы

Изучить основные топологии сетей и стандарты линий связи, выявить достоинства и недостатки линий связи локальных сетей, научиться проектировать локальные сети.

Теоретические сведения

Основные понятия

Компьютерная сеть – совокупность программных и аппаратных средств и среды передачи, служащая для обмена информацией между участниками.

Локальная сеть – система для непосредственного соединения многих компьютеров. При этом подразумевается, что информация передается от компьютера к компьютеру без каких-либо посредников и по единой среде передачи. Однако говорить о единой среде передачи в современной локальной сети не приходится. Например, в пределах одной сети могут использоваться как электрические кабели различных типов (витая пара, коаксиальный кабель), так и оптоволоконные кабели. Определение передачи «без посредников» также не корректно, ведь в современных локальных сетях используются репитеры, трансиверы, концентраторы, коммутаторы, маршрутизаторы, мосты, которые порой производят довольно сложную обработку передаваемой информации. Не совсем понятно, можно ли считать их посредниками или нет, можно ли считать подобную сеть локальной.

Из этого можно сделать вывод, что компьютеры, связанные локальной сетью, объединяются, в один виртуальный компьютер, ресурсы которого могут быть доступны всем пользователям, причем этот доступ не менее удобен, чем к ресурсам, входящим непосредственно в каждый отдельный компьютер.

Сформулировать отличительные признаки локальной сети можно следующим образом:

Высокая скорость передачи информации, большая пропускная способность сети. Приемлемая скорость сейчас – не менее 10 Мбит/с.

Низкий уровень ошибок передачи (или, то же самое, высококачественные каналы связи). Допустимая вероятность ошибок передачи данных должна быть порядка $10^{-8} - 10^{-12}$.

Эффективный, быстродействующий механизм управления обменом по сети.

Заранее четко ограниченное количество компьютеров, подключаемых к сети.

При таком определении понятно, что глобальные сети отличаются от локальных прежде всего тем, что они рассчитаны на неограниченное число абонентов. Кроме того, они используют (или могут использовать) не слишком качественные каналы связи и сравнительно низкую скорость передачи, а механизм управления обменом в них не может быть гарантированно

быстрым. В глобальных сетях гораздо важнее не качество связи, а сам факт ее существования.

Однако сети имеют и довольно существенные недостатки, о которых всегда следует помнить:

Сеть требует дополнительных, иногда значительных материальных затрат на покупку сетевого оборудования, программного обеспечения, на прокладку соединительных кабелей и обучение персонала.

Сеть требует приема на работу специалиста (администратора сети), который будет заниматься контролем работы сети, ее модернизацией, управлением доступом к ресурсам, устранением возможных неисправностей, защитой информации и резервным копированием. Для больших сетей может понадобиться целая бригада администраторов.

Сеть ограничивает возможности перемещения компьютеров, подключенных к ней, так как при этом может понадобиться перекладка соединительных кабелей.

Сети представляют собой прекрасную среду для распространения компьютерных вирусов, поэтому вопросам защиты от них придется уделять гораздо больше внимания, чем в случае автономного использования компьютеров. Ведь достаточно инфицировать один и все компьютеры сети будут поражены.

Сеть резко повышает опасность несанкционированного доступа к информации с целью ее кражи или уничтожения, Информационная защита требует проведения целого комплекса технических и организационных мероприятий.

Здесь же следует упомянуть о таких важнейших понятиях теории сетей, как абонент, сервер, клиент.

Абонент (узел, хост, станция) – это устройство, подключенное к сети и активно участвующее в информационном обмене. Чаще всего абонентом (узлом) сети является компьютер, но абонентом также может быть, например, сетевой принтер или другое периферийное устройство, имеющее возможность напрямую подключаться к сети. Далее в тексте книги вместо термина «абонент» для простоты будет использоваться термин «компьютер».

Сервером называется абонент (узел) сети, который предоставляет свои ресурсы другим абонентам, но сам не использует их ресурсы. Таким образом, он обслуживает сеть. Серверов в сети может быть несколько, и совсем не обязательно, что сервер – самый мощный компьютер. Выделенный (dedicated) сервер – этосервер, занимающийся только сетевыми задачами. Невыделенный сервер может помимо обслуживания сети выполнять и другие задачи. Специфический типсервера – это сетевой принтер.

Клиентом называется абонент сети, который только использует сетевые ресурсы, но сам свои ресурсы в сеть не отдает, то есть сеть его обслуживает, а он ей только пользуется. Компьютер–клиент также часто называют рабочей станцией. В принципе каждый компьютер может быть одновременно

как клиентом, так и сервером.

Под сервером и клиентом часто понимают также не сами компьютеры, а работающие на них программные приложения. В этом случае то приложение, которое только отдает ресурс в сеть, является сервером, а то приложение, которое только пользуется сетевыми ресурсами – клиентом.

Топология локальных сетей

Под топологией (компоновкой, конфигурацией, структурой) компьютерной сети обычно понимается физическое расположение компьютеров сети друг относительно друга и способ соединения их линиями связи.

Существует три базовые топологии сети:

Шина (bus) – все компьютеры параллельно подключаются к одной линии связи. Информация от каждого компьютера одновременно передается всем остальным компьютерам.

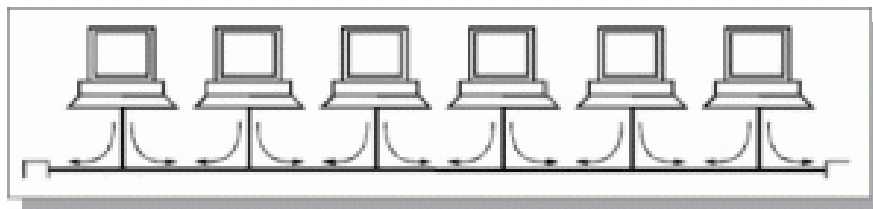


Рисунок 15.1 – Сетевая топология шина

Звезда (star) – к одному центральному компьютеру присоединяются остальные периферийные компьютеры, причем каждый из них использует отдельную линию связи. Информация от периферийного компьютера передается только центральному компьютеру, от центрального – одному или нескольким периферийным.

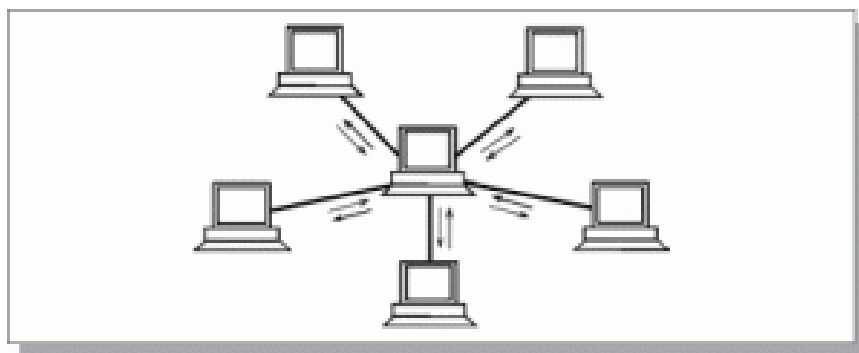


Рисунок 15.2 – Сетевая топология звезда

Кольцо (ring) – компьютеры последовательно объединены в кольцо. Передача информации в кольце всегда производится только в одном направлении. Каждый из компьютеров передает информацию только одному компьютеру, следующему в цепочке за ним, а получает информацию только от предыдущего в цепочке компьютера.

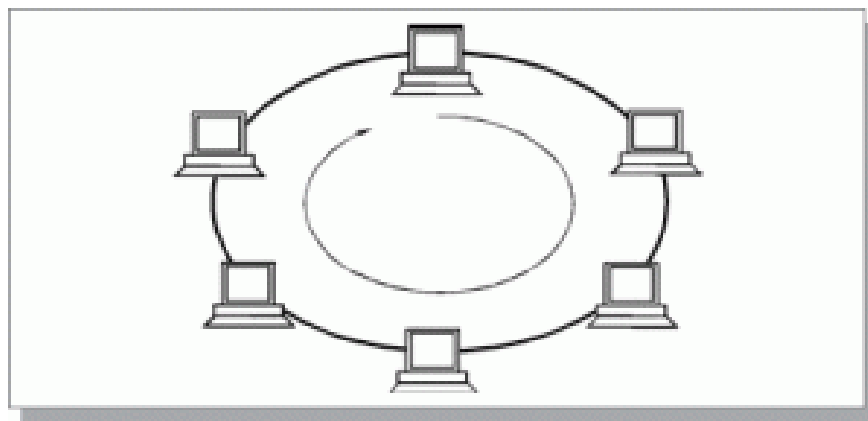


Рисунок 15.3 – Сетевая топология кольцо

На практике нередко используют и другие топологии локальных сетей, однако большинство сетей ориентировано именно на три базовые топологии.

Необходимо выделить некоторые важнейшие факторы, влияющие на физическую работоспособность сети и непосредственно связанные с понятием топология:

Исправность компьютеров (абонентов), подключенных к сети. В некоторых случаях поломка абонента может заблокировать работу всей сети. Иногда неисправность абонента не влияет на работу сети в целом, не мешает остальным абонентам обмениваться информацией.

Исправность сетевого оборудования, то есть технических средств, непосредственно подключенных к сети (адаптеры, трансиверы, разъемы и т.д.). Выход из строя сетевого оборудования одного из абонентов может сказаться на всей сети, но может нарушить обмен только с одним абонентом.

Целостность кабеля сети. При обрыве кабеля сети (например, из-за механических воздействий) может нарушиться обмен информацией во всей сети или в одной из ее частей. Для электрических кабелей столь же критично короткое замыкание в кабеле.

Ограничение длины кабеля, связанное с затуханием распространяющегося по нему сигнала. Как известно, в любой среде при распространении сигнал ослабляется (затухает). И чем большее расстояние проходит сигнал, тем больше он затухает (Рисунок 2.4). Необходимо следить, чтобы длина кабеля сети не была больше предельной длины $L_{пр}$, при превышении которой затухание становится уже неприемлемым (принимающий абонент не распознает ослабевший сигнал).

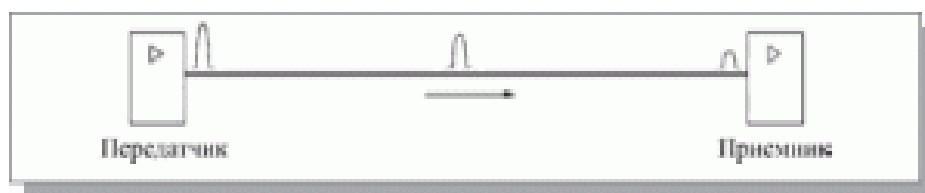


Рисунок 15.4 – Затухание сигнала при распространении по сети

Типы линий связи локальных сетей

Средой передачи информации называются те линии связи (или каналы связи), по которым производится обмен информацией между компьютерами. В подавляющем большинстве компьютерных сетей (особенно локальных) используются проводные или кабельные каналы связи, хотя существуют и беспроводные сети, которые сейчас находят все более широкое применение, особенно в портативных компьютерах.

Каждый тип кабеля имеет свои преимущества и недостатки, так что при выборе надо учитывать как особенности решаемой задачи, так и особенности конкретной сети, в том числе и используемую топологию.

Можно выделить следующие основные параметры кабелей, принципиально важные для использования в локальных сетях:

Полоса пропускания кабеля (частотный диапазон сигналов, пропускаемых кабелем) и затухание сигнала в кабеле. Два этих параметра тесно связаны между собой, так как с ростом частоты сигнала растет затухание сигнала. Надо выбирать кабель, который на заданной частоте сигнала имеет приемлемое затухание. Или же надо выбирать частоту сигнала, на которой затухание еще приемлемо. Затухание измеряется в децибелах и пропорционально длине кабеля.

Помехозащищенность кабеля и обеспечиваемая им секретность передачи информации. Эти два взаимосвязанных параметра показывают, как кабель взаимодействует с окружающей средой, то есть, как он реагирует на внешние помехи, и насколько просто прослушать информацию, передаваемую по кабелю.

Скорость распространения сигнала по кабелю или, обратный параметр – задержка сигнала на метр длины кабеля. Этот параметр имеет принципиальное значение при выборе длины сети. Типичные величины скорости распространения сигнала – от 0,6 до 0,8 от скорости распространения света в вакууме. Соответственно типичные величины задержек – от 4 до 5 нс/м.

Для электрических кабелей очень важна величина волнового сопротивления кабеля. Волновое сопротивление важно учитывать при согласовании кабеля для предотвращения отражения сигнала от концов кабеля. Волновое сопротивление зависит от формы и взаиморасположения проводников, от технологии изготовления и материала диэлектрика кабеля. Типичные значения волнового сопротивления – от 50 до 150 Ом.

Кабели на основе витых пар

Витые пары проводов используются в дешевых и сегодня, пожалуй, самых популярных кабелях. Кабель на основе витых пар представляет собой несколько пар скрученных попарно изолированных медных проводов в единой диэлектрической (пластиковой) оболочке. Он довольно гибкий и удобный для прокладки. Скручивание проводов позволяет свести к минимуму индуктивные наводки кабелей друг на друга и снизить влияние переходных процессов.

Обычно в кабель входит две или четыре витые пары.



Рисунок 15.5 – Кабель с витыми парами

Неэкранированные витые пары характеризуются слабой защищенностью от внешних электромагнитных помех, а также от подслушивания, которое может осуществляться с целью, например, промышленного шпионажа. Причем действие помех и величина излучения вовне увеличивается с ростом длины кабеля. Для устранения этих недостатков применяется экранирование кабелей.

В случае экранированной витой пары каждая из витых пар помещается в металлическую оплетку–экран для уменьшения излучений кабеля, защиты от внешних электромагнитных помех и снижения взаимного влияния пар проводов друг на друга. Для того чтобы экран защищал от помех, он должен быть обязательно заземлен. Естественно, экранированная витая пара заметно дороже, чем неэкранированная. Ее использование требует специальных экранированных разъемов. Поэтому встречается она значительно реже, чем неэкранированная витая пара.

Чаще всего витые пары используются для передачи данных в одном направлении (точка–точка), то есть в топологиях типа звезда или кольцо. Топология шина обычно ориентируется на коаксиальный кабель. Поэтому внешние терминаторы, согласующие неподключенные концы кабеля, для витых пар практически никогда не применяются.

Коаксиальные кабели

Коаксиальный кабель представляет собой электрический кабель, состоящий из центрального медного провода и металлической оплетки (экрана), разделенных между собой слоем диэлектрика (внутренней изоляции) и помещенных в общую внешнюю оболочку.



Рисунок 15.6 – Коаксиальный кабель

Коаксиальный кабель до недавнего времени был очень популярен, что связано с его высокой помехозащищенностью (благодаря металлической оплетке), более широкими, чем в случае витой пары, полосами пропускания (свыше 1ГГц), а также большими допустимыми расстояниями передачи (до

километра). К нему труднее механически подключиться для несанкционированного прослушивания сети, он дает также заметно меньше электромагнитных излучений вовне. Однако монтаж и ремонт коаксиального кабеля существенно сложнее, чем витой пары, а стоимость его выше (он дороже примерно в 1,5 – 3 раза). Сложнее и установка разъемов на концах кабеля.

Основное применение коаксиальный кабель находит в сетях с топологией типа шина. При этом на концах кабеля обязательно должны устанавливаться терминаторы для предотвращения внутренних отражений сигнала, причем один (и только один!) из терминаторов должен быть заземлен.

Реже коаксиальные кабели применяются в сетях с топологией звезда. В этом случае проблема согласования существенно упрощается, так как внешних терминаторов на свободных концах не требуется.

Существует два основных типа коаксиального кабеля:

тонкий (thin) кабель, имеющий диаметр около 0,5 см, более гибкий;

толстый (thick) кабель, диаметром около 1 см, значительно более жесткий. Он представляет собой классический вариант коаксиального кабеля, который уже почти полностью вытеснен современным тонким кабелем.

Тонкий кабель используется для передачи на меньшие расстояния, чем толстый, поскольку сигнал в нем затухает сильнее. Зато с тонким кабелем гораздо удобнее работать: его можно оперативно проложить к каждому компьютеру, а толстый требует жесткой фиксации на стене помещения. Подключение к тонкому кабелю (с помощью разъемов BNC байонетного типа) проще и не требует дополнительного оборудования. А для подключения к толстому кабелю надо использовать специальные довольно дорогие устройства, прокалывающие его оболочки и устанавливающие контакт как с центральной жилой, так и с экраном. Толстый кабель примерно вдвое дороже, чем тонкий, поэтому тонкий кабель применяется гораздо чаще.

В настоящее время считается, что коаксиальный кабель устарел, в большинстве случаев его вполне может заменить витая пара или оптоволоконный кабель. И новые стандарты на кабельные системы уже не включают его в перечень типов кабелей.

Оптоволоконные кабели

Оптоволоконный (он же волоконно–оптический) кабель – это принципиально иной тип кабеля по сравнению с рассмотренными двумя типами электрического или медного кабеля. Информация по нему передается не электрическим сигналом, а световым. Главный его элемент – это прозрачное стекловолокно, по которому свет проходит на огромные расстояния (до десятков километров) с незначительным ослаблением.



Рисунок 15.7 – Структура оптоволоконного кабеля

Структура оптоволоконного кабеля очень проста и похожа на структуру коаксиального электрического кабеля. Только вместо центрального медного провода здесь используется тонкое (диаметром около 1 – 10 мкм) стекловолокно, а вместо внутренней изоляции – стеклянная или пластиковая оболочка, не позволяющая свету выходить за пределы стекловолокна. В данном случае речь идет о режиме так называемого полного внутреннего отражения света от границы двух веществ с разными коэффициентами преломления (у стеклянной оболочки коэффициент преломления значительно ниже, чем у центрального волокна). Металлическая оплетка кабеля обычно отсутствует, так как экранирование от внешних электромагнитных помех здесь не требуется. Однако иногда ее все-таки применяют для механической защиты от окружающей среды (такой кабель иногда называют броневым, он может объединять под одной оболочкой несколько оптоволоконных кабелей).

Оптоволоконный кабель обладает исключительными характеристиками по помехозащищенности и секретности передаваемой информации. Никакие внешние электромагнитные помехи в принципе не способны исказить световой сигнал, а сам сигнал не порождает внешних электромагнитных излучений. Подключиться к этому типу кабеля для несанкционированного прослушивания сети практически невозможно, так как при этом нарушается целостность кабеля. Стоимость оптоволоконного кабеля постоянно снижается и сейчас примерно равна стоимости тонкого коаксиального кабеля.

Однако оптоволоконный кабель имеет и некоторые недостатки:

Самый главный из них – высокая сложность монтажа (при установке разъемов необходима микронная точность, от точности скола стекловолокна и степени его полировки сильно зависит затухание в разьеме).

Использование оптоволоконного кабеля требует специальных оптических приемников и передатчиков, преобразующих световые сигналы в электрические и обратно, что порой существенно увеличивает стоимость сети в целом.

Оптоволоконные кабели допускают разветвление сигналов (для этого производятся специальные пассивные разветвители (couplers) на 2–8 каналов), но, как правило, их используют для передачи данных только в одном направлении между одним передатчиком и одним приемником.

Оптоволоконный кабель менее прочен и гибок, чем электрический.

Чувствителен оптоволоконный кабель и к ионизирующим излучениям,

из-за которых снижается прозрачность стекловолокна, то есть увеличивается затухание сигнала.

Применяют оптоволоконный кабель только в сетях с топологией звезда и кольцо. Никаких проблем согласования и заземления в данном случае не существует. Кабель обеспечивает идеальную гальваническую развязку компьютеров сети. В будущем этот тип кабеля, вероятно, вытеснит электрические кабели или, во всяком случае, сильно потеснит их. Запасы меди на планете истощаются, а сырья для производства стекла более чем достаточно.

Существуют два различных типа оптоволоконного кабеля:

- многомодовый или мультимодовый кабель, более дешевый, но менее качественный;
- одномодовый кабель, более дорогой, но имеет лучшие характеристики по сравнению с первым.

Суть различия между этими двумя типами сводится к разным режимам прохождения световых лучей в кабеле.



Рисунок 12.8 – Распространение света в одномодовом кабеле

В одномодовом кабеле практически все лучи проходят один и тот же путь, в результате чего они достигают приемника одновременно, и форма сигнала почти не искажается. Одномодовый кабель имеет диаметр центрального волокна около 1,3 мкм и передает свет только с такой же длиной волны (1,3 мкм). Дисперсия и потери сигнала при этом очень незначительны, что позволяет передавать сигналы на значительно большее расстояние, чем в случае применения многомодового кабеля. Для одномодового кабеля применяются лазерные приемопередатчики, использующие свет исключительно с требуемой длиной волны. Затухание сигнала в одномодовом кабеле составляет около 5 дБ/км и может быть даже снижено до 1 дБ/км.

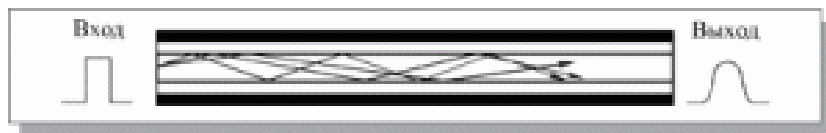


Рисунок 12.9 – Распространение света в многомодовом кабеле

В многомодовом кабеле траектории световых лучей имеют заметный разброс, в результате чего форма сигнала на приемном конце кабеля искажается. Центральное волокно имеет диаметр 62,5 мкм, а диаметр внешней оболочки 125 мкм (это иногда обозначается как 62,5/125). Для передачи используется обычный (не лазерный) светодиод, что снижает стоимость и увеличивает срок службы приемопередатчиков по сравнению с одномодовым кабелем. Длина волны света в многомодовом кабеле равна 0,85 мкм, при этом на-

блюдается разброс длин волн около 30 – 50 нм. Допустимая длина кабеля составляет 2 – 5 км. Многомодовый кабель – это основной тип оптоволоконного кабеля в настоящее время, так как он дешевле и доступнее. Затухание в многомодовом кабеле больше, чем в одномодовом и составляет 5 – 20 дБ/км.

Типичная величина задержки для наиболее распространенных кабелей составляет около 4–5 нс/м, что близко к величине задержки в электрических кабелях.

Беспроводные каналы связи

Кроме кабельных каналов в компьютерных сетях иногда используются также бескабельные каналы. Их главное преимущество состоит в том, что не требуется никакой прокладки проводов (не надо делать отверстий в стенах, закреплять кабель в трубах и желобах, прокладывать его под фальшполами, над подвесными потолками или в вентиляционных шахтах, искать и устранять повреждения). К тому же компьютеры сети можно легко перемещать в пределах комнаты или здания, так как они ни к чему не привязаны.

Радиоканал использует передачу информации по радиоволнам, поэтому теоретически он может обеспечить связь на многие десятки, сотни и даже тысячи километров. Скорость передачи достигает десятков мегабит в секунду (здесь многое зависит от выбранной длины волны и способа кодирования).

Особенность радиоканала состоит в том, что сигнал свободно излучается в эфир, он не замкнут в кабель, поэтому возникают проблемы совместимости с другими источниками радиоволн (радио- и телевещательными станциями, радарам, радилюбительскими и профессиональными передатчиками и т.д.). В радиоканале используется передача в узком диапазоне частот и модуляция информационным сигналом несущей частоты.

Главным недостатком радиоканала является его плохая защита от прослушивания, так как радиоволны распространяются неконтролируемо. Другой большой недостаток радиоканала – слабая помехозащищенность.

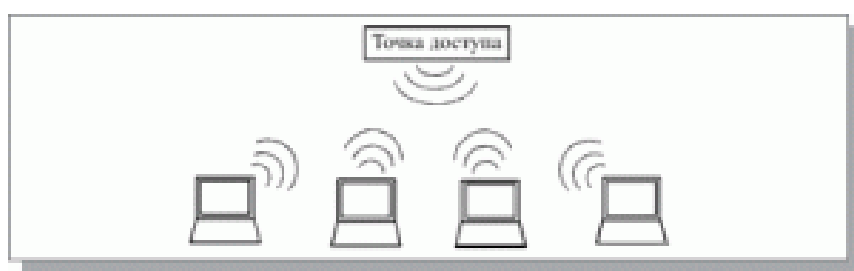


Рисунок 15.10 – Объединение компьютеров

Радиоканал широко применяется в глобальных сетях как для наземной, так и для спутниковой связи. В этом применении у радиоканала нет конкурентов, так как радиоволны могут дойти до любой точки земного шара.

Инфракрасный канал также не требует соединительных проводов, так как использует для связи инфракрасное излучение (подобно пульту дистанционного управления домашнего телевизора). Главное его преимущество по сравнению с радиоканалом – нечувствительность к электромагнитным поме-

хам, что позволяет применять его, например, в производственных условиях, где всегда много помех от силового оборудования. Правда, в данном случае требуется довольно высокая мощность передачи, чтобы не влияли никакие другие источники теплового (инфракрасного) излучения. Плохо работает инфракрасная связь и в условиях сильной запыленности воздуха.

Скорости передачи информации по инфракрасному каналу обычно не превышают 5–10 Мбит/с, но при использовании инфракрасных лазеров может быть достигнута скорость более 100 Мбит/с. Секретность передаваемой информации, как и в случае радиоканала, не достигается, также, требуются сравнительно дорогие приемники и передатчики.

Аппаратная часть локальных сетей

Аппаратура локальных сетей обеспечивает реальную связь между абонентами. Выбор аппаратуры имеет важнейшее значение на этапе проектирования сети, так как стоимость аппаратуры составляет наиболее существенную часть от стоимости сети в целом, а замена аппаратуры связана не только с дополнительными расходами, но зачастую и с трудоемкими работами.

К аппаратуре локальных сетей относятся:

- кабели для передачи информации;
- разъемы для присоединения кабелей;
- согласующие терминаторы;
- сетевые адаптеры;
- репитеры;
- трансиверы;
- концентраторы.

О первых трех компонентах сетевой аппаратуры уже говорилось в предыдущих разделах, сейчас следует остановиться на функциях остальных компонентов.

Сетевые адаптеры

Сетевые адаптеры (они же контроллеры, карты, платы, интерфейсы, NIC – Network Interface Card) – это основная часть аппаратуры локальной сети. Назначение сетевого адаптера – сопряжение компьютера (или другого абонента) с сетью, то есть обеспечение обмена информацией между компьютером и каналом связи в соответствии с принятыми правилами обмена. Именно они реализуют функции двух нижних уровней модели OSI. Плата сетевого адаптера обычно имеет также один или несколько внешних разъемов для подключения к ней кабеля сети.

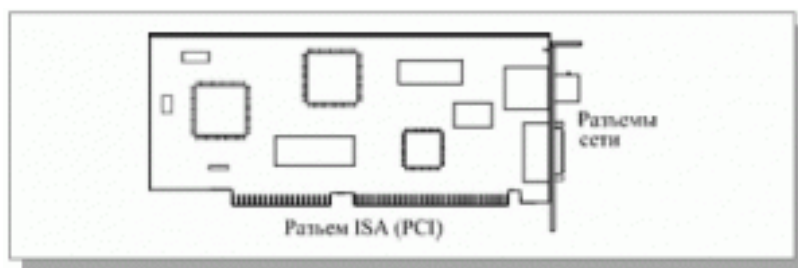


Рисунок 15.11 – Плата сетевого адаптера

К основным сетевым функциям адаптеров относятся:

- гальваническая развязка компьютера и кабеля локальной сети (для этого обычно используется передача сигналов через импульсные трансформаторы);
- преобразование логических сигналов в сетевые (электрические или световые) и обратно;
- кодирование и декодирование сетевых сигналов, то есть прямое и обратное преобразование сетевых кодов передачи информации (например, манчестерский код);
- опознание принимаемых пакетов (выбор из всех приходящих пакетов тех, которые адресованы данному абоненту или всем абонентам сети одновременно);
- преобразование параллельного кода в последовательный при передаче и обратное преобразование при приеме;
- буферирование передаваемой и принимаемой информации в буферной памяти адаптера;
- организация доступа к сети в соответствии с принятым методом управления обменом;
- подсчет контрольной суммы пакетов при передаче и приеме.

Все остальные аппаратные средства локальных сетей (кроме адаптеров) имеют вспомогательный характер, и без них часто можно обойтись. Это сетевые промежуточные устройства.

Трансиверы или приемопередатчики

Трансиверы или приемопередатчики (от английского TRANsmitter + reCEIVER) служат для передачи информации между адаптером и кабелем сети или между двумя сегментами (частями) сети. Трансиверы усиливают сигналы, преобразуют их уровни или преобразуют сигналы в другую форму (например, из электрической в световую и обратно). Трансиверами также часто называют встроенные в адаптер приемопередатчики.

Репитеры

Репитеры или повторители (repeater) выполняют более простую функцию, чем трансиверы. Они не преобразуют ни уровни сигналов, ни их физическую природу, а только восстанавливают ослабленные сигналы (их амплитуду и форму), приводя их к исходному виду. Цель такой ретрансляции сигналов состоит исключительно в увеличении длины сети.

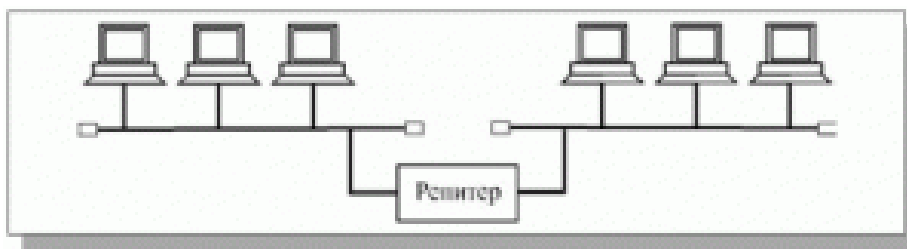


Рисунок 15.12 – Соединение репитером двух сегментов сети

Концентраторы

Концентраторы (хабы, hub), как следует из их названия, служат для объединения в сеть нескольких сегментов. Концентраторы (или репитерные концентраторы) представляют собой несколько собранных в едином конструктиве репитеров, они выполняют те же функции, что и репитеры.

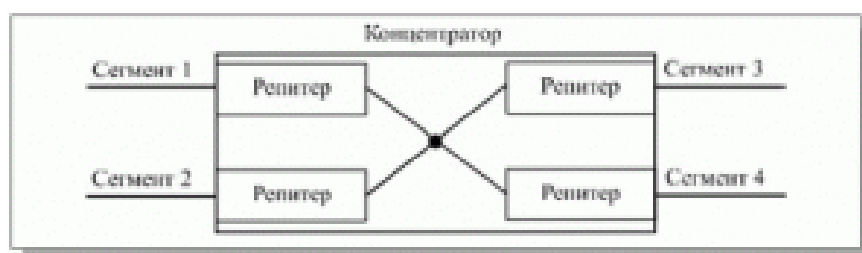


Рисунок 15.13 – Схема концентратора

Преимущество подобных концентраторов по сравнению с отдельными репитерами в том, что все точки подключения собраны в одном месте, это упрощает реконфигурацию сети, контроль и поиск неисправностей. К тому же все репитеры в данном случае питаются от единого качественного источника питания.

Коммутаторы

Коммутаторы (свичи, коммутирующие концентраторы, switch), как и концентраторы, служат для соединения сегментов в сеть. Они также выполняют более сложные функции, производя сортировку поступающих на них пакетов.

Коммутаторы передают из одного сегмента сети в другой не все поступающие на них пакеты, а только те, которые адресованы компьютерам из другого сегмента. Пакеты, передаваемые между абонентами одного сегмента, через коммутатор не проходят. При этом сам пакет коммутатором не принимается, а только пересылается.

Стандарты линий связи

10-BASE-5

В качестве среды передачи используется толстый (желтый) коаксиальный кабель с волновым сопротивлением 50 Ом. Максимальная длина сегмента сети составляет 500 м, общая длина всех сегментов не более 2500 м. Общее число участников на один сегмент не более 100. Расстояние между участниками кратно 2.5 м.

Соединение участников с линией связи производится через трансиверы (устройства приема/передачи информации). Длина кабеля, соединяющего участника с трансивером не более 50 м.

Сегменты заканчиваются терминаторами, один из которых должен быть заземлен.

Скорость 10Мбит/с

Характеристики:

- низкая скорость
- + высокое качество

10–BASE–2

В качестве среды передачи используется тонкий коаксиальный кабель с волновым сопротивлением 50 Ом. Максимальная длина сегмента сети составляет 185 м, общая длина всех сегментов, соединенных через повторители не более 925 м. Общее число участников на один сегмент не более 30. Расстояние между соседними станциями не менее 0.5 м.

Сегменты заканчиваются терминаторами, один из которых должен быть заземлен. Ответвления от сегмента недопустимы.

Скорость 10Мбит/с

Характеристики:

- низкая скорость
- + низкая стоимость

10–BASE–T

В качестве среды передачи используется неэкранированная витая пара третьей категории (кабель состоит из 4-х пар проводов и сертифицирован на частоту до 10МГц).

Для приема/передачи используются две пары проводов. Максимальная длина кабеля между соседними участниками 100м, а общий размер сети не более 500м. Количество станций в сети не более 1024.

В качестве разъемов применяются 8–ми канальные разъемы типа RJ-45. Производится соединение типа «точка–точка», физическая топология сети – «звезда».

Скорость 10 Мбит/с.

Характеристики:

- низкая скорость
- + большой размер сети

100–BASE–T

Среда передачи – неэкранированная витая пара пятой категории (4 пары проводов, сертифицированных на частоту 100МГц).

Скорость передачи 100Мбит/с.

Характеристики:

- + хорошая скорость

- + наибольшая распространенность для витой пары

100–BASE–FL

Среда передачи – оптоволоконный кабель. Этот стандарт предназначен для соединения станций с концентратором. Для этого используются два оптоволоконных кабеля для приема и передачи.

Для многомодового кабеля длина сегмента до 2 км, для одномодового – при дуплексном режиме работы концентратора и станции больше 100 км, при стандартном оборудовании – до 10 км.

Скорость 100Мбит/с.

Характеристики:

- + хорошая скорость
- высокая стоимость

Группа стандартов GIGABIT

Используется несколько стандартов передачи данных со скоростями тысячи Мбит/с. Наиболее распространенные:

1000–BASE–F – Данные передаются по оптоволоконному кабелю

1000–BASE–T – Используется витая пара категории 5+. Данные передаются по двум парам (прием/передача) сигналами 4–х уровней на расстояние до 25м.

1000–BASE–T4 – Использует витую пару категории 5+. Для приема и передачи используется по две пары проводов длиной до 100м.

Характеристики:

- + высокая скорость
- высокая стоимость

Построить схему сети университета и ее модель с указанием топологии сетей и стандартов линий связи.

Основными критерием выбора должны быть: экономичность и достаточная пропускная способность. Сделать приблизительный расчет количества материалов и стоимости такой сети с учетом «сетевой» аппаратуры.

Задание для самостоятельного выполнения

Исходные данные приведены в таблице.

Вариант 1

№ корпуса	Количество классов	Количество ПК в классе
1	12	15
2	10	
3	6	
4	8	

Вариант 2

№ корпуса	Количество классов	Количество ПК в классе
1	8	10
2	13	
3	9	
4	5	

Вариант 3

№ корпуса	Количество классов	Количество ПК в классе
1	4	19
2	17	
3	2	
4	1	

Вариант 4

№ корпуса	Количество классов	Количество ПК в классе
1	8	5
2	19	
3	12	
4	16	

Вариант 5

№ корпуса	Количество классов	Количество ПК в классе
1	12	2
2	20	
3	26	
4	18	

Объяснить, чем руководствовались при выборе тех или иных элементов сети и указать их преимущества, отразить результат и обоснование критериев выбора в отчете.

Контрольные вопросы

1. Какие топологии сетей вы знаете?

2. Чем отличается локальная сеть от глобальной?
3. Может ли быть компьютер одновременно клиентом и сервером?
4. Сколько проводов в витой паре?
5. Можно ли назвать соединение шина с соединенными концами – кольцом?
6. Чем отличается свитч (switch) от хаба (hub)?
7. Для чего нужен Терминатор?
8. Каково назначение сетевого адаптера?
9. Чем отличается витая пара в стандартах 100-BASE-T и 1000-BASE-T?
10. Чем обусловлена задержка в оптоволоконных и электрических кабелях?

16 ИЗУЧЕНИЕ МАРШРУТИЗАЦИИ IP

Цель работы

Изучить правила адресации сетевого уровня, научиться распределять адреса между участниками сети передачи данных и организовывать маршрутизацию между сегментами сети

Теоретические сведения

Сетевой уровень отвечает за возможность доставки пакетов по сети передачи данных – совокупности сегментов сети, объединенных в единую сеть любой сложности посредством узлов связи, в которой имеется возможность достижения из любой точки сети в любую другую.

Архитектуру сетевого уровня удобно рассматривать на примере сетевого протокола IP – самого распространенного в настоящее время, основного протокола сети Интернет. Термин «стек протоколов TCP/IP» означает «набор протоколов, связанных с IP и TCP (протоколом транспортного уровня)».

Архитектура протоколов TCP/IP предназначена для объединенной сети, состоящей из соединенных друг с другом шлюзами отдельных разнородных пакетных подсетей, к которым подключаются разнородные машины.

Каждая из подсетей работает в соответствии со своими специфическими требованиями и имеет свою природу средств связи.

Однако предполагается, что каждая подсеть может принять пакет информации (данные с соответствующим сетевым заголовком) и доставить его по указанному адресу в этой конкретной подсети. Не требуется, чтобы подсеть гарантировала обязательную доставку пакетов и имела надежный сквозной протокол. Таким образом, две машины, подключенные к одной подсети, могут обмениваться пакетами.

Когда необходимо передать пакет между машинами, подключенными к разным подсетям, то машина-отправитель посылает пакет в соответствующий шлюз (шлюз подключен к подсети также как обычный узел). Шлюз (gateway) – любое сетевое оборудование с несколькими сетевыми интерфейсами и осуществляющее продвижение пакетов между сетями на уровне протоколов сетевого уровня.

Из шлюза пакет направляется по определенному маршруту через систему шлюзов и подсетей, пока не достигнет шлюза, подключенного к той же подсети, что и машина-получатель; там пакет направляется к получателю.

Таким образом, шлюз выполняет маршрутизацию – процедуру нахождения в структуре сети пути достижения получателя (построение пути доставки пакетов).

Если хост подключен к нескольким сетям, он должен иметь несколько сетевых адресов, как минимум столько, сколько каналов к нему подключено.

Даже если хост не является шлюзом между подсетями, все равно в нем присутствует таблица маршрутизации, ведь любой хост должен отправлять пакеты напрямую членам своей подсети, через какой-то шлюз другим подсе-

тям и не передавать в сеть пакеты, предназначенные самому себе (заворачивать их по внутренней петле 127.0.0.1).

Правила маршрутизации

Правила маршрутизации определяют куда и как должны посылаться пакеты для разных сетей.

Каждое правило состоит из следующих компонентов:

Начальный адрес подсети, порядок достижения которой описывает правило.

Маска подсети, которую описывает правило.

Шлюз показывает, на какой адрес будут посланы пакеты, идущие в сеть назначения. Если пакеты будут идти напрямую, то указывается собственный адрес (точнее тот адрес того канала, через который будут передаваться пакеты).

Интерфейс показывает через какой сетевой адаптер (его номер или IP-адрес) должен посылаться пакет в заданную сеть;

Метрика показывает время за которое пакет может достигнуть сети получателя (величина условная и может быть изменена при маршрутизации). Если имеется несколько правил достижения одной сети, пакеты посылаются по правилу с наименьшей метрикой.

Применение правила заключается в определении, принадлежит ли хост назначения сети, указанной в правиле, и если принадлежит, то пакет отправляется на адрес шлюза через интерфейс.

Правила маршрутизации сведены в таблицу маршрутизации (где расположены по степени уменьшения маски), которую можно посмотреть с помощью команды ROUTE PRINT.

Правила применяются в порядке уменьшения масок.

Правила с равными масками применяются в порядке увеличения метрики.

Пример таблицы маршрутизации

Рассмотрим таблицу маршрутизации, имеющую следующий вид:

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
0.0.0.0	0.0.0.0	192.168.200.1	192.168.200.47	30
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.192.0	255.255.240.0	192.168.200.47	192.168.200.47	30
192.168.200.47	255.255.255.255	127.0.0.1	127.0.0.1	30
192.168.200.255	255.255.255.255	192.168.200.47	192.168.200.47	30
224.0.0.0	240.0.0.0	192.168.200.47	192.168.200.47	30
255.255.255.255	255.255.255.255	192.168.200.47	192.168.200.47	1

Проанализируем вышеприведенную таблицу маршрутизации, пересортировав правила:

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
255.255.255.255	255.255.255.255	192.168.200.47	192.168.200.47	1
192.168.200.47	255.255.255.255	127.0.0.1	127.0.0.1	30
192.168.200.255	255.255.255.255	192.168.200.47	192.168.200.47	30
192.168.192.0	255.255.240.0	192.168.200.47	192.168.200.47	30
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
224.0.0.0	240.0.0.0	192.168.200.47	192.168.200.47	30
0.0.0.0	0.0.0.0	192.168.200.1	192.168.200.47	30

255.255.255.255	255.255.255.255	192.168.200.47	192.168.200.47	1
-----------------	-----------------	----------------	----------------	---

Обратите внимание на маску сети в первом правиле. Она описывает подсеть размером в 1 хост с адресом 255.255.255.255 – это широковещательный адрес. Пакеты будут посылаться на адрес 192.168.200.47 через интерфейс 192.168.200.47. Это наш адрес, т.е. пакеты будут отправляться напрямую.

192.168.200.255	255.255.255.255	192.168.200.47	192.168.200.47	30
-----------------	-----------------	----------------	----------------	----

Опять широковещательный адрес. Смотри предыдущий комментарий.

192.168.200.47	255.255.255.255	127.0.0.1	127.0.0.1	30
----------------	-----------------	-----------	-----------	----

Опять такая же маска, но адрес нашего хоста. Отправлять будем через внутреннюю петлю.

192.168.192.0	255.255.240.0	192.168.200.47	192.168.200.47	30
---------------	---------------	----------------	----------------	----

А вот и наша подсеть. Отправляем напрямую.

127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
-----------	-----------	-----------	-----------	---

Все, что начинается со 127, отправляем через внутреннюю петлю.

224.0.0.0	240.0.0.0	192.168.200.47	192.168.200.47	30
-----------	-----------	----------------	----------------	----

Класс D – отправляем напрямую.

0.0.0.0	0.0.0.0	192.168.200.1	192.168.200.47	30
---------	---------	---------------	----------------	----

Самое интересное правило. Маска покрывает ВСЕ возможные адреса! Пакеты отправляются через наш интерфейс на адрес 192.168.200.1. Правило применяется последним, поэтому его можно озвучить так: по всем адресам, которые не подошли по предыдущим правилам, пакеты отправляем на адрес 192.168.200.1. Такой адрес обычно имеется в любой сети и называется

ся шлюзом по умолчанию (defaultgateway). Этот адрес скрывает от хостов и пользователей структуру сети и позволяет упростить таблицы маршрутизации и снять нагрузку с хостов, перенеся маршрутизацию на специально выделенные шлюзы – маршрутизаторы.

Нетрудно догадаться, что все адреса в колонке Адрес шлюза должны достигаться напрямую, т.е. входить в нашу подсеть.

Разбиение сети на подсети

Одной из основных задач, стоящих при проектировании сетей, является распределение по подсетям сетевых адресов из заданного диапазона, т.е. разделение сети на подсети.

При разделении сети на подсети следует учитывать следующие правила:

Размер подсетей должен быть степенью двойки.

Имеются запрещенные адреса.

Начальный адрес подсети должен быть кратен ее размеру.

В качестве шлюза по умолчанию можно использовать любой узел, но, исходя из увеличения пропускной способности сети и уменьшения времени передачи пакетов, следует в качестве шлюза по умолчанию использовать либо ближайший узел, либо узел, соединенный с максимальным количеством сетей, т.е. следует учитывать топологию сети.

Программа ROUTE

Для работы с таблицами маршрутизации в составе ОС имеется программа route (упоминалась ранее). Выводит на экран и изменяет записи в локальной таблице IP-маршрутизации.

route [-f] [-p] [команда [конечная_точка] [mask маска_сети] [шлюз] [metric метрика]] [if интерфейс]

Параметры:

-f – Очищает таблицу маршрутизации от всех записей, которые не являются узловыми маршрутами (маршруты с маской подсети 255.255.255.255), сетевым маршрутом замыкания на себя (маршруты с конечной точкой 127.0.0.0 и маской подсети 255.0.0.0) или маршрутом многоадресной рассылки (маршруты с конечной точкой 224.0.0.0 и маской подсети 240.0.0.0). При использовании данного параметра совместно с одной из команд (таких, как add, change или delete) таблица очищается перед выполнением команды.

-p – При использовании данного параметра с командой add указанный маршрут добавляется в реестр и используется для инициализации таблицы IP-маршрутизации каждый раз при запуске протокола TCP/IP. При использовании параметра с командой print выводит на экран список постоянных маршрутов. Все другие команды игнорируют этот параметр.

команда – Указывает команду, которая будет запущена на удаленной системе. В следующей таблице представлен список допустимых параметров.

Команда	Назначение
---------	------------

Add	Добавление маршрута
change	Изменение существующего маршрута
Delete	Удаление маршрута или маршрутов
Print	Печать маршрута или маршрутов

конечная_точка – Определяет конечную точку маршрута. Конечной точкой может быть сетевой IP-адрес (где разряды узла в сетевом адресе имеют значение 0), IP-адрес маршрута к узлу, или значение 0.0.0.0 для маршрута по умолчанию.

maskмаска_сети – Указывает маску сети в соответствии с точкой назначения. Маска сети может быть маской подсети соответствующей сетевому

шлюз – Указывает IP-адрес пересылки или следующего перехода, по которому доступен набор адресов, определенный конечной точкой и маской подсети

metric метрика – Задаёт целочисленную метрику стоимости маршрута (в пределах от 1 до 9999) для маршрута, которая используется при выборе в таблице маршрутизации одного из нескольких маршрутов, наиболее близко соответствующего адресу назначения пересылаемого пакета.

if интерфейс – Указывает индекс интерфейса, через который доступна точка назначения. В случае, когда параметр if пропущен, интерфейс определяется из адреса шлюза.

/? – Отображает справку в командной строке.

Задания для самостоятельного выполнения

С помощью программы routepoint посмотрите таблицу маршрутизации Вашего компьютера. Объясните все правила.

Посмотрите таблицу маршрутизации хоста, имеющего несколько каналов. Объясните все правила.

Посмотрите таблицу маршрутизации маршрутизатора. Объясните все правила.

Добавьте новое правило в таблицу маршрутизации для сети 192.168.0.0/24 через шлюз в вашей сети с последним байтом в адресе 125 и метрикой 12.

Удалите это правило.

В соответствии с таблицей и схемами выполните задание на распределение адресов по подсетям (согласно варианта). Постройте таблицы маршрутизации для всех шлюзов и для одного хоста для каждого сегмента.

№Варианта	Количество хостов в подсети					Диапазон адресов	
	A	B	C	D	E	от	до
1	5	10	20	15	50	10.0.20.0	10.0.20.255
2	20	15	6	70	25	192.168.0.0	192.168.0.255
3	15	25	5	40	5	112.38.25.128	112.38.25.255
4	24	32	8	10	2	196.13.49.0	196.13.49.128
5	50	16	64	20	15	68.76.115.0	68.76.115.255
6	40	6	10	12	5	211.3.45.0	211.3.45.128

Разделите сеть, состоящую из трех сегментов, имеющую диапазон адресов 192.168.0.32 – 192.168.0.159 на подсети, содержащие 64, 20 и 44 хостов (включая шлюзы).

Контрольные вопросы

1. Сколько адресов может иметь хост?
2. Может ли у хоста быть прописано несколько шлюзов и почему?
3. Может ли у хоста быть прописано несколько шлюзов по умолчанию и почему?
4. Чем отличаются таблицы у разных классов сетевых устройств и почему?
5. Почему начальный адрес подсети должен быть кратен ее размеру?
6. Чем Вы руководствовались при выборе шлюзов по умолчанию?
7. Может ли физический сегмент сети содержать несколько сетевых подсетей?

ЛИТЕРАТУРА

1. Урбанович, П. П. Компьютерные сети: учебное пособие / П. П. Урбанович, Д. М. Романенко. — Москва, Вологда: Инфра-Инженерия, 2022. — 460 с.— Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/124197.html>, экземпляров неограниченно.
2. Дятлов, П. А. Принципы построения и организация компьютерных сетей: учебное пособие / П. А. Дятлов. — Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2022. — 127 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/125710.html>, экземпляров неограниченно.
3. Смирнова, Е. В. Построение коммутируемых компьютерных сетей: учебное пособие / Е. В. Смирнова, И. В. Баскаков, А. В. Пролетарский, Р. А. Федотов. — 3-е изд. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 428 с.— Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/89464.html>, экземпляров неограниченно.
4. Артюшенко, В. В. Компьютерные сети и телекоммуникации : учебно-методическое пособие / В. В. Артюшенко, А. В. Никулин. — Новосибирск: Новосибирский государственный технический университет, 2020. — 72 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/99345.html>, экземпляров неограниченно
5. Сергеев, М. Ю. Компьютерные сети: практикум / М. Ю. Сергеев, Т. И. Сергеева, С. А. Олейникова. — Воронеж: Воронежский государственный технический университет, ЭБС АСВ, 2019. — 154 с.— Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/93261.html>, экземпляров неограниченно