БПОУ ВО «Грязовецкий политехнический техникум»

Рассмотрен

цикловой комиссией по общепрофессиональным дисциплинам и профессиональным модулям отделения «Электрификация и автоматизация сельского хозяйства»

Согласовано

зам. директора по ОМР
_____ Е. А. Ткаченко
«30» августа 2017 г.

Протокол № 1 от «30» августа 2017 г.

Председатель комиссии:
_____ Т. В. Невзорова

ПРАКТИЧЕСКИЕ (ЛАБОРАТОРНЫЕ) РАБОТЫ

ПМ.02. Организация сетевого администрирования

Специальность 09.02.02. Компьютерные сети

Грязовец
2017 г.

МДК 02.01. Программное обеспечение компьютерных сетей

Лабораторная работа
Тема: Изучение сетевых средств операционной системы MS Windows.

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

1.2. Задача лабораторной работы

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 вам или специалисту службы технической поддержки информацию, необходимую для поиска причин, вызвавших проблемы с сетью. Наблюдение за состоянием системы. 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 удается. Часто наблюдаются только симптомы, которые необходимо интерпретировать. Придется поэтапно в логической последовательности использовать ряд инструментальных средств, следовательно, пользователь должн быть осведомлен относительно принципов организации сетей и возможностей каждого сетевого инструментального средства.

Возможные проблемы связности сети:

1. Оконечные нагрузки ЛВС должным образом не подключены.
2. ЛВС-интерфейс не работоспособен.
3. ЛВС-интерфейс имеет не правильный IP-адрес.
4. Маска подсети имеет не верное значение.
5. Тот же IP-адрес используется другой системой.
6. Конфигурация таблицы маршрутизации настроена неправильно.
7. Маршрутизатор выключен.
8. Кабель ЛВС поврежден.
9. Длина сегмента ЛВС слишком велика.
10. Неправильно указан DNS-сервер.

1.3. Домашние задание для подготовки к лабораторной работе

При выполнении заданий лабораторной работы рекомендуется ознакомиться с материалами:

1. Встроенная помощь ОС MS Windows "Центр справки и поддержки": " Общие сведения о протоколе TCP/IP".
2. Вывод справочных сведений о командах. Встроенная помощь к программам OS MS Windows - при помощи команды: HELP ["команда"], конструкции ["команда"] /? [4]
3. Изучить [1, с.487][2, с.498]

1.4. Схема лабораторной работы

Для выполнения лабораторной работы достаточно одного компьютера, подключенного к какой либо сети, например, Internet или два компьютера соединенных кроссовером Ethernet.

1.5. Содержание работы

Собрать схему лабораторной работы. Провести анализ связности сети. Составить отчет.

1.6. Порядок выполнения работы

1.6.1. С помощью "Центра справки и поддержки" MS Windows собрать информацию о системе:

Вызовите "Центр справки и поддержки" MS Windows с помощью клавиши [F1] или с командной строки запустите: C:\WINDOWS\pchealth\helpctr\binaries\HelpCtr.exe. 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".

1.6.2. С помощью программы MS Windows "Сведения о системе" и systeminfo собрать информацию о системе:

1. Запустить командный процессор: *"Пуск"//"Выполнить"//"*cmd
2. Выполнить команду: cd C:\Program Files\Common Files\Microsoft Shared\MSInfo\
3. Выполнить команду: msinfo32
4. Выполнить команду: systeminfo

1.6.3. Проанализировать связность сети, к которой подключен компьютер.

С помощью команд MS Windows просмотрите и опишите подсоединение к локальной сети. С командной строки выполните команды, указанные в табл.1.1:

Таблица 1.1.

Команды	Содержание команды
netstat.exe –rn route print	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
ping 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)
arp -a	Просмотр записей кэш, использующихся для хранения IP-адресов и соответствующих им физических адресов Ethernet
finger @X.X.X.X	Отображает сведения о пользователе или пользователях конкретного удаленного компьютера (обычно с операционной системой UNIX), запускающего службу Finger или демон. *"Операционные системы Microsoft Windows 2000 и Microsoft Windows XP не предоставляют службу finger.*

1.6.4. Просмотреть текстовыми файлами содержащий номера портов для стандартных служб и файл содержащего сопоставления IP-адресов именам узлов:
Выполните следующие команды:

1. more C:\WINDOWS\system32\drivers\etc\services
2. more C:\WINDOWS\system32\drivers\etc\services | find "http"
3. type C:\WINDOWS\system32\drivers\etc\services | find "ftp"
4. type C:\WINDOWS\system32\drivers\etc\services | find "tcp" |more
5. type C:\WINDOWS\system32\drivers\etc\services | find "udp" | more

Ознакомьтесь с образцом файла HOSTS

1. cd C:\WINDOWS\system32\drivers\etc\
2. more hosts

1.7. Содержание отчета
В отчете описать полученные результаты: информация о сетевых настройках и подключениях компьютера.
1.8. Контрольные вопросы

- Что определяет связность сети?
- Какие утилиты используются в ОС Windows для анализа сетевых подключение компьютера?

Лабораторная работа
Тема: Изучение TFTP соединений.

1.1. Цель роботы. Ознакомиться с возможностью передачи файлов по протоколу TFTP
1.2. Задача лабораторной работы

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

В стеке TCP/IP протокол FTP предлагает наиболее широкий набор услуг для работы с файлами, однако он является и самым сложным для программирования. Приложения, которым не требуются все возможности FTP, могут использовать другой, более экономичный протокол - простейший протокол пересылки файлов TFTP (Trivial File Transfer Protocol). Этот протокол реализует только передачу файлов, причем в качестве транспорта используется более простой, чем TCP, протокол без установления соединения - UDP.
В силу своей простоты протокол tftp используется не только для передачи файлов, но и для загрузки X-терминалов, процедура загрузки которых предполагает использование протоколов RARP, TFTP и BOOTP

Администраторам сети часто приходится сохранять файлы конфигурации, системное программное обеспечение (IOS) или восстанавливать их на коммуникационное оборудование. Возможно два способа копирования образа IOS во флэш-память: через консоль по протоколу Xmodem или через порт Ethernet по протоколу TFTP. Первый способ характеризуется огромным временем выполнения операции (часы). Второй способ предполагает наличие TFTP сервера.

Встроенная поддержка TCP/IP MS Windows позволяет использовать протокол TFTP в цифровых сетях для передачи файлов между устройствами. Созданный в процессе лабораторной работы некоторый файл конфигурация может быть сохранен студентами на TFTP-серверы для последующего анализа или повторного использования.

1.3. Схема лабораторной работы

Собрать схему лабораторных работ. Установить tftp-соединение со своим компьютером или с другим компьютером. Для выполнения лабораторной необходимо два компьютера.

Для проведения работы необходима программа TFTPD.EXE и исходник пакетного файла make_10M.txt. *(см. п.1.9. Приложение).* Составить отчет.

1.4. Домашние задание для подготовки к лабораторной работе

При выполнении заданий лабораторной работы рекомендуется ознакомиться с материалами:

- Встроенная помощь ОС MS Windows "Центр справки и поддержки": поиск по ключу "tftp" [4].
- Встроенная помощь к программам OS MS Windows, (при помощи команды: tftp /?)
- Главу 4.5.4.1 "Протокол TFTP Семенов Ю.А. (ГНЦ ИТЭФ)" - http://book.itep.ru/4/45/tftp4541.htm Изучить главу "Стек TCP/IP"[1, с.156].

1.5. Содержание работы

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

1.6. Порядок выполнения работы

1.6.1. Сохранение на TFTP-сервер рабочей конфигурации маршрутизации компьютера.

<table>
<tr><th colspan="2">Команды</th><th>Содержание команды</th></tr>
<tr><td colspan="2">Запустите командный процессор</td><td>"Пуск"//"Выполнить"-->cmd</td></tr>
<tr><td colspan="2">Создайте рабочие каталоги</td><td>mkdir c:\temp\down
mkdir c:\temp\up
cd c:\temp\up</td></tr>
<tr><td colspan="2">В директории c:\temp\up создать файл конфигурации таблицы маршрутизации up.cnf</td><td>netstat -rn > c:\temp\up\up.cnf
type c:\temp\up\up.cnf</td></tr>
<tr><td colspan="2">В директории c:\temp\down создать файл текущих параметров сети TCP/IP down.cnf</td><td>ipconfig /all >
c:\temp\down\down.cnf
type c:\temp\down\down.cnf</td></tr>
<tr><td colspan="3">Запустить демон tftpd - программа для передачи фалов по протокол TFTP</td></tr>
<tr><td colspan="3">В окне программы TFTPD установить корневую директорию c:\temp\down</td></tr>
<tr><td rowspan="3">Для передачи файлов между компьютерами выполнить следующие команды, где в качестве IP-адреса может использоваться 127.0.0.1 или адрес соседнего компьютера.</td><td>Получить файл со своего компьютера. Результат записать в отчет.</td><td>dir /c/d c:\temp\up c:\temp\down
cd c:\temp\up
tftp 127.0.0.1 put up.cnf
dir /c/d c:\temp\up c:\temp\down</td></tr>
<tr><td>Отправить файл на свой компьютер. Результат записать в отчет.</td><td>tftp 127.0.0.1 get down.cnf</td></tr>
<tr><td>Отравить и получить файлы с соседнего компьютера. Результат записать в отчет.</td><td>tftp X.X.X.X put up.cnf
tftp X.X.X.X get down.cnf</td></tr>
</table>

1.6.2. Сохранение бинарного файла на TFTP-сервере.

В этом режиме файл передается в неизменном виде по байтам.

Команды	Содержание команды
Создать с помощью пакетного файла файл размером 10Mb:	Скопировать программу make_10M.txt в директорию C:\temp\up\. Переименовать make_10M.txt в make_10M.bat Запуститьmake_10M.bat. В результате этого должен создасться в директории C:\temp\up\ файл test_10.Mb (10000001 байт).

Выполнить в директории C:\temp\up\ передачу бинарного файла на loopback и на другой компьютер. Результат записать в отчет.	tftp -i 127.0.0.1 put test_10.Mb tftp -i X.X.X.X put test_10.Mb tftp -i 127.0.0.1 get test_10.Mb tftp -i X.X.X.X get test_10.Mb
В другом окне командного процессора просмотреть ожидаемых подключений по TFTP-протоколу. Результат записать в отчет.	netstat -an 1 | find "69" netstat -a 1 | find "tftp"

1.7. Содержание отчета

Записать полученные результаты передачи файлов на Loopback и на другой компьютер. Провести анализ скорости передачи и качества, описать возникшие ошибки передачи.

1.8. Контрольные вопросы

- Зачем нужен протокол TFTP?
- Какую из функций реализует протокол TFTP?
- Назначение пакета, если код операции в заголовке TFTP равен 1?
- Назначение пакета, если код операции в заголовке TFTP равен 2?
- Назначение пакета, если код операции в заголовке TFTP равен 3?
- Назначение пакета, если код операции в заголовке TFTP равен 4?
- Назначение пакета, если код операции в заголовке TFTP равен 5?
- К какому уровню модели ISO/OSI относится протокол TFTP?
- При tftp открывается только одно соединение!

1.9. Приложение

```
rem --< ####### -< пакетный файл make_10M.bat >- #########
rem --< Программа создания файла test_10.Mb размером 10Mb.
rem --<
###############################################

del *_.*
echo 1234567890124567890123 > 1_
copy *_ 2_ & copy *_ 3_ & copy *_ 4_ & copy *_ 5_
& copy *_ 6_ & copy *_ 7_
copy *_ 8_ & copy *_ 9_ & copy *_ 10_ & copy *_
11_ & copy *_ 12_ & copy *_ 13_
copy *_ 14_ & copy *_ 15_ & copy *_ 16_ & copy *_
17_ & copy *_ 18_ & copy *_ 19_ & copy *_ 20_
copy 20_+19_+14_+13_+11_+9_ test_10.Mb
del *_.*
```

Лабораторная работа

Тема: Создание web-страницы

1.1. Цель работы. Изучение средств диагностики сети, позволяющие предотвратить внештатные ситуации.

1.2. Задача лабораторной работы

1.3. Домашние задание для подготовки к лабораторной работе

1. Встроенная помощь ОС MS Windows "Центр справки и поддержки" поиск по ключу http, web:

2. Вывод справочных сведений о командах. Встроенная помощь к программам OS MS Windows. При помощи команды: HELP [<команда>], конструкции [<команда>] /?. evntcmd /?
3. Интернет ресурсы: Гипертекстный протокол HTTP , WWW

1.4. Схема лабораторной работы

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

1.5. Порядок выполнения работы

Для выполнения работы необходимо установить на компьютере с помощью "Мастера компонентов Windows" web-службу : С командной строки набрать: control.exe appwiz.cpl,@0,2 Установить компоненту MS Windows "Internet Information Services (IIS)", ~~(sysocmgr)~~ обеспечивающая поддержку создания web узлов. Далее отметить компоненты устанавливаемый в ОС MS Windows: 1. Оснастка IIS - интерфейс администрирования IIS в виде оснастки MMC. Установить компоненты. 2. Служба WWW - использует HTTP-протокол для отклика на запросы web-клиентов в TCP/IP сети. (состав: Служба WWW)	
sc qc w3svc sc qc iisadmin sc qc SamSS sc qc RPCSS	*Службы указанные в разделе* DEPENDENCIES *должны быть запущены. Если не запускается Веб-публикации установить причину, почему службы указанные в разделе* DEPENDENCIES *не работают.* Поместить в отчет
wmic service w3svc get StartMode /value wmic service iisadmin get StartMode /value wmic service SamSS get StartMode /value wmic service RPCSS get StartMode /value	Проверить тип запуска службы: Опция StartMode должна быть: Auto или Manual Для команды sc соответственно - AUTO_START или DEMAND_START. Поместить в отчет
sc config w3svc start= auto sc config iisadmin start= auto sc config SamSS start= auto sc config RPCSS start= auto	Установить тип запуска службы - авто. Поместить в отчет
sc query iisadmin sc query w3svc , если нет, то запустить эти службы: sc start iisadmin & sc start w3svc	Определить, работает ли IIS и WWW-служба: Сервис iisadmin - позволяет администрировать веб- и FTP-службы с помощью оснастки IIS. Сервис w3svc - Веб-публикации. Обеспечивает связь и администрирование веб-узла с помощью оснастки. Поместить в отчет
mkdir c:\temp\www cd c:\temp\www	Создать директорию c:\temp\www
%windir%\system32\inetsrv\inetmgr.exe	Проверить в IIS настройки WWW- сервера
mkdir c:\temp\down cd c:\temp\down	Создать директорию c:\temp\down
Скопировать в директорию c:\temp\down программу wget.exe	

В директории c:\temp\down создать пакетный файл http.bat, см. Приложение.	
start http://127.0.0.1/	Проверить созданную страницу. Поместить в отчет
wget.exe -r -nc -b http://127.0.0.1	Попытаться скачать все страницы указанного сайта в Интернете *(в данном случае на локальном компьютере)*
Просмотреть скаченную директорию	

1.6. Содержание отчета

~~Отчет не составляется.~~

1.7. Контрольные вопросы

Протокол HTTP.

1.8. Приложение

```
rem --< ################ -(пакетный файл - http.bat ########################
rem --<
rem --< Программа создания web_site с 2252 файлами в директории ./http
rem --<
rem --< ############################################################

mkdir http & mkdir http\1 & mkdir http\1\1 & mkdir http\1\1\1 & mkdir http\1\1\1\1
echo "<a href=1.htm>." > http\1\1\1\1\0.htm & echo "<a href=2.htm>." > http\1\1\1\1\1.htm
echo "<a href=3.htm>." > http\1\1\1\1\2.htm & echo "<a href=4.htm>." > http\1\1\1\1\3.htm
echo "<a href=5.htm>." > http\1\1\1\1\4.htm & echo "<a href=6.htm>." > http\1\1\1\1\5.htm
echo "<a href=7.htm>." > http\1\1\1\1\6.htm & echo "<a href=8.htm>." > http\1\1\1\1\7.htm
echo "<a href=9.htm>." > http\1\1\1\1\8.htm & echo "<a href=0.htm>." > http\1\1\1\1\9.htm
mkdir http\1\1\1\2 & mkdir http\1\1\1\3 & mkdir http\1\1\1\4 & mkdir http\1\1\1\5
echo "<a href=1/1.htm>." > http\1\1\1\1.htm & echo "<a href=2/1.htm>." > http\1\1\1\2.htm
echo "<a href=3/1.htm>." > http\1\1\1\3.htm & echo "<a href=4/1.htm>." > http\1\1\1\4.htm
echo "<a href=5/1.htm>." > http\1\1\1\5.htm
Xcopy http\1\1\1\1 /s http\1\1\1\2 & Xcopy http\1\1\1\1 /s http\1\1\1\3
Xcopy http\1\1\1\1 /s http\1\1\1\4 & Xcopy http\1\1\1\1 /s http\1\1\1\5
mkdir http\1\1\2 & mkdir http\1\1\3 & mkdir http\1\1\4 & mkdir http\1\1\5
echo "<a href=1/1.htm>." > http\1\1\1.htm & echo "<a href=2/1.htm>." > http\1\1\2.htm
echo "<a href=3/1.htm>." > http\1\1\3.htm & echo "<a href=4/1.htm>." > http\1\1\4.htm
echo "<a href=5/1.htm>." > http\1\1\5.htm
Xcopy http\1\1\1 /s http\1\1\2 & Xcopy http\1\1\1 /s http\1\1\3
Xcopy http\1\1\1 /s http\1\1\4 & Xcopy http\1\1\1 /s http\1\1\5
mkdir http\1\2 & mkdir http\1\3 & mkdir http\1\4 & mkdir http\1\5
echo "<a href=1/1.htm>." > http\1\1.htm & echo "<a href=2/1.htm>." > http\1\2.htm
echo "<a href=3/1.htm>." > http\1\3.htm & echo "<a href=4/1.htm>." > http\1\4.htm
echo "<a href=5/1.htm>." > http\1\5.htm
Xcopy http\1\1 /s http\1\2 & Xcopy http\1\1 /s http\1\3 & Xcopy http\1\1 /s http\1\4
mkdir http\02
echo "<a href=1/1.htm>." > http\1.htm & echo "<a href=02/1.htm>." > http\2.htm
Xcopy /s http\1 http\02
echo "<a href=http/1.htm>Page 1</a><p>" > index.htm & echo "<a href=http/2.htm>Page
2">> index.htm
```

Лабораторная работа
Тема: Настройки сетевой платы, связность сети, сетевые утилиты - ifconfig, ethtool, mii-tool

1. Цель работы. Целью настоящей работы является изучение сетевых настроек операционной системы Linux и решение проблем сети с помощью утилит операционной системы.
2. Задача лабораторной работы

Пакет Net-tools является набором программ для контроля сетевой подсистемы ядра Linux.

- arp используется для манипулирования кешем ARP ядра, обычно для добавления и удаления содержимого кеша или для сброса его содержимого в дамп.
- dnsdomainname отображает системное имя домена DNS.
- domainname отображает или устанавливает системное NIS/YP имя домена.
- hostname отображает или устанавливает имя текущего хоста.
- ifconfig это основная утилита для настройки сетевых интерфейсов.
- ipmaddr добавляет, удаляет и показывает широковещательные адреса интерфейса.
- iptunnel добавляет, изменяет, удаляет и показывает тунели для интерфейса.
- mii-tool проверяет или устанавливает статус единицы Media Independent Interface (MII) сетевого интерфейса.
- nameif именует сетевые интерфейсы, основанные на MAC адресах.
- netstat используется для отчета о сетевых подключениях, таблицах маршрутизации и статистике по интерфейсам.
- nisdomainname делает то же самое, что и domainname.
- plipconfig используется для управления параметрами PLIP устройства для улучшения его производительности.
- rarp используется для манипулирования таблицей RARP ядра.
- route используется для манипулирования таблицей IP маршрутизации.
- slattach подсоединяет сетевой интерфейс к последовательной линии. Это позволяет вам использовать обычные линии терминала для связи в режиме точка-точка с другими компьютерами.
- ypdomainname делает то же самое, что и domainname.

Иногда, при некоторых сочетаниях сети некоторые сетевые карты работают неправильно, если у них выставлено значение "автоопределение типа передачи". Возникает такая ситуация, что свойства сетевой карты настроены верно, а пакеты все равно не доходят. Поможет утилита mii-tool, которая всегда есть в /sbin. Эта утилита принудительно выставляет параметры связи 100 или 10 мбит/с, Full Duplex или Half Duplex.

Задачи:

- Рассмотреть настройки сетевой платы,
- Проверить связность сети,
- Рассмотреть сетевые утилиты

3. Схема лабораторной работы

Лабораторная работа выполняется на компьютерах с использованием следующих вариантов:

1. установленной на компьютере операционной системой Linux,
2. технологии LiveCD - *загрузочного диска с предустановленной операционной системой Linux.*

Возможные схемы выполнения лабораторных работ.

1. Вариант: Computer 1 ---(Концентратор)--- Computer 2
2. Вариант: Computer 1 ---(Internet)--- Страница в Internet
3. Вариант: Computer 1 ---(Virtual Mashine)--- Гостевая операционная система (Linux)

Работа тестировалась с операционной системой ОС Linux finnix-89.0.iso (Debian) с использованием виртуальной машиной Sun xVM VirtualBox (Version 1.6.0 Edition. Sun

Microsystems, Inc.). При этом в настройках созданной новой виртуальной машины указывалось:

1. Общие - Оперативная память не менее 64 Mb, Видеопамять не менее 8Mb
2. Жесткий диск - не подключать
3. CD/DVD-ROM - Образ finnix-89.0.iso
4. Сеть - Адаптер 0/PCnet-Fast III (Хост-интерфейс VirtualBox 1)
    - *В настройках сетевой карты "Хост-интерфейс VirtualBox 1" установить IP-адрес:* 192.168.0.1/255.255.255.0
5. USB - Фильтр устройств 1 (активно)
    - *Фильтр устройств USB:* указать свою флеш-карту

4. Содержание работы

1. Собрать схему лабораторной работы.
2. Подключить запоминающее устройство на USB (флэш память).
3. Просмотр данной страницы возможно: lynx linux_1.htm *(могут быть проблемы с русской кодировкой)*
4. Выполнить п 1.5, собрав данные в отчет. *Один из способов сохранения результата:* ethtool -k eth0 | tee ethtool.log

5. Порядок выполнения работы

Подключить запоминающее устройство на USB (флэш память). *Подробнее - "man mount"*	mount /dev/sda1 /mnt
Проверить настройки сетевой платы и установить минимальную конфигурацию: half-duplex 10Mb. *Подробнее - "man mii-tool"* ethtool - небольшая утилита для настройки и диагностики интерфейса Ethernet. *Подробнее - "man ethtool"*.	1. ethtool eth0 2. mii-tool -v 3. ethtool -s eth0 speed 10 duplex half autoneg off 4. mii-tool -v 5. ethtool -s eth0 autoneg on 6. mii-tool -v 7. ..... 8. ethtool -i eth0 9. ethtool -g eth0 10. ethtool -k eth0 11. ethtool -S eth0
Сделать вывод о связности сети с помощью следующих утилит:	1. ifconfig 2. netstat -rn 3. traceroute 4. ping
Пример настройки IP-адреса сетевой карты	ifconfig eth0 192.168.0.100
Команды для ознакомления	adduser labuser
	su labuser
	who -a
	chfn
	finger @labuser
Возможные утилиты для настройки сетевой карты	mii-diag
	net-diag
	ether-wake

6. Содержание отчета

Лабораторная работа выполняется студентом в HTML-формате, созданная любым редактором, например, FrontPage, только не средствами MS Office Word/Excel любой версии.

Это требование вызвано условием уменьшения суммарного трафика всех лабораторных работ, т.к. работы отправляются и получаются через Internet.

Лабораторная работа

Тема: Средства диагностики сети ОС Linux.

1. Цель работы. Целью настоящей работы является рассмотрение и изучение средств диагностики сети утилитами операционной системы ОС Linux.
2. Задача лабораторной работы

Программа Nmap предназначена для сканирования сетей с любым количеством объектов, определения состояния объектов сканируемой сети а также портов и соответствующих им служб. Для этого Nmap использует много различных методов сканирования, таких, как UDP, TCP connect(), TCP SYN (полуоткрытое), FTP proxy (прорыв через ftp), Reverse-ident, ICMP (ping), FIN, ACK, Xmas tree, SYN и NULL-сканирование.
Типы сканирования tnmap могут быть следующими:
-sS: TCP SYN сканирование
-sT: TCP-сканирование соединением
-sF: TCP FIN сканирование
-sX: TCP Xmas сканирование
-sN: TCP Null сканирование
-sR: TCP RPC сканирование
-I: Ident-сканирование
-sU: UDP-сканирование
-sP: Ping-сканирование
Дополнительная информация:

- icmp.ru\man\network\nmap_manpage-ru.html
- www.inattack.ru\print_article\48.html

Задачи лабораторной работы:

- Установить IP-адрес для сетевой платы,
- Проверить связность сети,
- Рассмотреть работу сетевых утилит ОС Linux сканирующих сеть: nmap и iptraf

3. Схема лабораторной работы

Работа тестировалась с операционной системой ОС Linux finnix-89.0.iso (Debian) с использованием виртуальной машиной Sun xVM VirtualBox (Version 1.6.0 Edition. Sun Microsystems, Inc.). При этом в настройках созданной новой виртуальной машины указывалось:

1. Общие - Оперативная память не менее 64 Mb, Видеопамять не менее 8Mb
2. Жесткий диск - не подключать
3. CD/DVD-ROM - Образ finnix-89.0.iso
4. Сеть - Адаптер 0/PCnet-Fast III (Хост-интерфейс VirtualBox 1)
    - *В настройках сетевой карты "Хост-интерфейс VirtualBox 1" установить IP-адрес:* 192.168.0.1/255.255.255.0
5. USB - Фильтр устройств 1 (активно)
    - *Фильтр устройств USB:* указать свою флеш-карту

4. Содержание работы

1. Собрать схему лабораторной работы.
2. Подключить запоминающее устройство на USB (флэш-память).
3. Выполнить п 1.5, собрав данные в отчет.

5. Порядок выполнения работы

Запустить OS Linux и выполнить следующие команды:

<table>
<tr><th>Описание</th><th colspan="2">Команды</th><th>Примечание</th></tr>
<tr><td>Настроить IP-адрес сетевой карты</td><td colspan="2">ifconfig eth0 192.168.0.100</td><td></td></tr>
<tr><td rowspan="2">nmap - the Network Mapper. Утилита для сканирования и исследования безопасности сети. Подробнее - "man nmap"
iptraf - Интерактивный IP LAN-монитор Подробнее - "man iptraf"</td><td rowspan="2">Для получение сканированной информации в сетевой карте от действия команды nmap: необходимо обе команды выполнить в двух терминальных окнах (переключение между терминалами в Linux: Alt-F1 или Alt-F2 ...Alt-F6).</td><td>nmap -vvv 192.168.0.1 > ./log_nmap</td><td rowspan="2">Поместить в отчет</td></tr>
<tr><td>iptraf -i eth0 -L ./log_nmap.txt</td></tr>
<tr><td rowspan="2">Команды для ознакомления</td><td>Просмотр состояния дискового пространства</td><td colspan="2">df -h</td></tr>
<tr><td>Просмотр производительности компьютера</td><td colspan="2">• top
• free
• ps
• slabtop
• vmstat
• w</td></tr>
<tr><td rowspan="5">Возможные утилиты и программы для сканирования сети</td><td>Снифферы</td><td colspan="2">Ethereal
Tcpdump
Etherape
Ntop</td></tr>
<tr><td colspan="3">iftop (см. man iftop)</td></tr>
<tr><td colspan="3">pcap</td></tr>
<tr><td colspan="3">driftnet</td></tr>
<tr><td>Мониторинг сети</td><td colspan="2">Gkrellm
Big Brother
Nagios
Tkined
MRTG
Rrdtool
PIKT
Autostatus
bcnu
mon
Sysmon
Spong
SNIPS
Ksysguard
OpenNMS</td></tr>
</table>

6. Содержание отчета

Лабораторная работа выполняется студентом в HTML-формате, созданная любым редактором, например, FrontPage, только не средствами MS Office Word/Excel любой версии.

Это требование вызвано условием уменьшения суммарного трафика всех лабораторных работ, т.к. работы отправляются и получаются через Internet.

Лабораторная работа
Тема: Настройки соединений компьютеров по сети с помощью Secure Shell

1. Цель работы. Целью настоящей работы является изучение сетевых настроек операционной системы Linux позволяющие производить удалённое управление операционной системой и передачу файлов.
2. Задача лабораторной работы

SSH (англ. *Secure Shell* — «безопасная оболочка») — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и передачу файлов. Сходен по функциональности с протоколами Telnet и rlogin, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования. SSH-клиенты и SSH-серверы имеются для большинства операционных систем.

SSH позволяет безопасно передавать в незащищенной среде практически любой другой сетевой протокол, таким образом, можно не только удаленно работать на компьютере через командную оболочку, но и передавать по шифрованному каналу звуковой поток или видео (например, с веб-камеры). Также SSH может использовать сжатие передаваемых данных для последующего их шифрования, что удобно, например, для удаленного запуска клиентов X Window System.

Большинство хостинг-провайдеров за определенную плату предоставляют клиентам доступ к их домашнему каталогу по SSH. Это может быть удобно как для работы в командной строке, так и для удаленного запуска программ (в том числе графических приложений). Через SSH можно работать с консолью удалённого сервера, как будто находясь рядом с ним.

Задачи:

- Рассмотреть настройки операционной системы для работы по протоколу SSH
- Сравнить трафики telnet и ssh.

3. Схема лабораторной работы

Работа тестировалась с операционной системой ОС Linux knoppix_5.0.iso (Debian) с использованием виртуальной машиной Sun xVM VirtualBox (Version 1.6.0 Edition. Sun Microsystems, Inc.). При этом в настройках созданной новой виртуальной машины указывалось:

1. Общие - Оперативная память не менее 64 Mb, Видеопамять не менее 8Mb
2. Жесткий диск - не подключать
3. CD/DVD-ROM - Образ knoppix_5.0.iso
4. Сеть - Адаптер 0/PCnet-Fast III (Хост-интерфейс VirtualBox 1)
    - *В настройках сетевой карты "Хост-интерфейс VirtualBox 1" установить IP-адрес:* 192.168.0.1/255.255.255.0
5. USB - Фильтр устройств 1 (активно)
    - *Фильтр устройств USB:* указать свою флеш-карту

4. Содержание работы

1. Ознакомиться с со следующей информацией:
    - http://ru.wikipedia.org/wiki/Ssh
    - Описание протокола SSH (Secure Shell)
    - Руководство по настройке и использованию SSH
    - Faq по OpenSSH в русской редакции
    - http://www.realcoding.net/article/view/656
2. Собрать схему лабораторной работы.
3. Подключить запоминающее устройство на USB (флэш-память). Выполнить п 1.5, собрав данные в отчет.

5. Порядок выполнения работы

Описание	Команды	Примечание

Запустить консоль	Пуск*(Alt-F1)//"Выполнить программу..."//*konsole	
Войти в систему суперпользователем (*root*)	su	
Установить IP-адрес для сетевой карты	ifconfig eth0 192.168.0.100	
Задать пароль для пользователя:	passwd *knoppix*	
Запустить ssh-сервис	sshstart	Поместить в отчет
Запустить программу анализатора трафика	*sshow*	Поместить в отчет результат комманды *sshow*
На другой машине запустить клиента ssh для Windows на IP-адрес виртуальной машины Linux:192.168.0.100	Скачать ssh-клиента putty.exe Запустисть с коммандной строки: putty 192.168.0.100	
Просмотреть действующие процессы:	*ps -ef* | *grep ssh*	Поместить в отчет результат комманды *ps*
Запустить программу анализатора трафика	*sshow*	Поместить в отчет результат комманды *sshow*
На основной машине запустить клиента sftp для Windows на IP-адрес виртуальной машины Linux:192.168.0.100	Скачать ssh-клиента psftp.exe Запустисть с коммандной строки: psftp.exe knoppix@192.168.0.100	
Просмотреть действующие процессы:	*ps -ef* | *grep ssh*	Поместить в отчет результат комманды *ps*
Дополнительная информация	SSH-серверы OpenBSD: OpenSSH Debian GNU/Linux: dropbear, lsh-server, openssh-server, ssh MS Windows: freeSSHd, OpenSSH sshd, WinSSHD	
	SSH-клиенты и оболочки Debian GNU/Linux: kdessh, lsh-client, openssh-client, putty, ssh MS Windows и Windows NT: PuTTY, SecureCRT, ShellGuard, Axessh, ZOC, SSHWindows, ProSSHD MS Windows Mobile: PocketPuTTy, mToken, sshCE, PocketTTY, OpenSSH, PocketConsole Mac OS: NiftyTelnet SSH Symbian OS: PuTTY Java: MindTerm, AppGate Security Server J2ME: MidpSSH	

6. Содержание отчета

Лабораторная работа выполняется студентом в HTML-формате, созданная любым редактором, например, FrontPage, только не средствами MS Office Word/Excel любой версии.
Это требование вызвано условием уменьшения суммарного трафика всех лабораторных работ, т.к. работы отправляются и получаются через Internet.

Лабораторная работа
Тема: Настройка DHCP-сервера и DHCP-клиента

1. Цель работы. Целью настоящей работы является изучение сетевых настроек операционных систем для управлением динамической адресацией в сети.
2. Задача лабораторной работы
Рассмотреть настройки операционных систем для работы по протоколу DHCP
3. Схема лабораторной работы

Работа тестировалась с операционной системой ОС Linux knoppix_5.0.iso (Debian) с использованием виртуальной машиной Sun xVM VirtualBox (Version 1.6.0 Edition. Sun Microsystems, Inc.). При этом в настройках созданной новой виртуальной машины указывалось:

1. Общие - Оперативная память не менее 64 Mb, Видеопамять не менее 8Mb
2. Жесткий диск - не подключать
3. CD/DVD-ROM - Образ knoppix_5.0.iso
4. Сеть - Адаптер 0/PCnet-Fast III (Хост-интерфейс VirtualBox 1)
    - *В настройках сетевой карты "Хост-интерфейс VirtualBox 1" установить IP-адрес:* любые настройки
5. USB - Фильтр устройств 1 (активно)
    - *Фильтр устройств USB:* указать свою флеш-карту

4. Содержание работы
    1. Ознакомиться с со следующей информацией:
        - http://www.citforum.idknet.com/internet/tifamily/dhcp.shtml
        - http://linux.opennet.ru/docs/RUS/dhcp/index.html
        - http://linux.opennet.ru/tips/info/924.shtml
        - http://linux.opennet.ru/docs/HOWTO-RU/mini/DHCP.html
    2. Собрать схему лабораторной работы.
    3. Подключить запоминающее устройство на USB (флэш-память).
    4. Выполнить п 1.5, собрав данные в отчет.
5. Порядок выполнения работы

Описание	Команды		Примечание
	Windows	Linux	
Запустить интерпретаторы командной строки	cmd	Пуск*(Alt-F1)//"Выполнить программу..."//*konsole	
Настроить сервис DHCP и параметры сетевой карты для работы по этому протоколу	ipconfig /all netstat -rn		
	sc query dhcp		
	netsh interface ip set address name="Хост-интерф *" source=dhcp		
	sc start dhcp		
Войти в систему суперпользователем (*root*)		su	

<table>
<tr><td colspan="2">Установить IP-адрес для сетевой карты</td><td>ifconfig eth0 192.168.0.1</td><td></td></tr>
<tr><td colspan="2">Любым редактором ОС Linux, например, NEdit или vi, заменить содержание файла: /etc/dhcp3/dhcpd.conf
Можно создать на host-машине файлы, далее передать на guest-машину любым способом,
не обязательно через флеш-память, например, можно посредством FTP или TFTP.</td><td>nedit /etc/dhcp3/dhcpd.conf
option domain-name "agtu.wan.laboratory.org";
subnet 192.168.0.0 netmask 255.255.255.0 {
range 192.168.0.100 192.168.0.200; }</td><td></td></tr>
<tr><td colspan="2">Запустить второй терминал (xterm или konsole), в котором включить просмотр системного журнала</td><td>su
syslogd
tail -f /var/log/syslog</td><td></td></tr>
<tr><td colspan="2">В первом терминале запустить сервис сервера динамической адресации</td><td>dhcpd3</td><td></td></tr>
<tr><td>Изменить IP-адрес сетевой карты по протоколу DHCP</td><td>ipconfig /all
ipconfig /renew "Хост-интерфейс VirtualBox 1"
ipconfig /all
netstat -rn</td><td>/etc/init.d/dhcp3-server status</td><td></td></tr>
<tr><td>Восстановить IP-адрес интерфейса в ОС Windows</td><td colspan="3">netsh interface ip set address name="Хост-интер*" source=static addr=192.168.0.1 mask=255.255.255.0</td></tr>
</table>

6. Содержание отчета

Лабораторная работа выполняется студентом в HTML-формате, созданная любым редактором, например, FrontPage, только не средствами MS Office Word/Excel любой версии.

Это требование вызвано условием уменьшения суммарного трафика всех лабораторных работ, т.к. работы отправляются и получаются через Internet.

Лабораторная работа
Тема: Протокол IPv6

1. Цель работы. Целью настоящей работы является изучение сетевых настроек операционных систем для работы по протоколу IP версии 6.

2. Задача лабораторной работы

Рассмотреть настройки операционных систем для работы по протоколу IP версии 6

3. Схема лабораторной работы

Работа тестировалась с операционной системой ОС Linux knoppix_5.0.iso (Debian) с использованием виртуальной машиной Sun xVM VirtualBox (Version 1.6.0 Edition. Sun Microsystems, Inc.). При этом в настройках созданной новой виртуальной машины указывалось:

1. Общие - Оперативная память не менее 64 Mb, Видеопамять не менее 8Mb
2. Жесткий диск - не подключать
3. CD/DVD-ROM - Образ knoppix_5.0.iso
4. Сеть - Адаптер 0/PCnet-Fast III (Хост-интерфейс VirtualBox 1)
    - *В настройках сетевой карты "Хост-интерфейс VirtualBox 1" установить*

IP-адрес: 192.168.0.1/255.255.255.0

5. USB - Фильтр устройств 1 (активно)
    - *Фильтр устройств USB:* указать свою флеш-карту

8.4. Содержание работы

1. Ознакомиться с со следующей информацией:
    - http://www.ipv6.ru/russian/documents/theory/address.php
    - http://www.ipv6.ru/russian/documents/practice/windows.php
    - http://www.ipv6.ru/russian/documents/practice/unix.php
    - http://www.ipv6.ru/russian/documents/theory/autoconf.php
    - http://www.ipv6.ru/russian/documents/theory/nat.php
    - http://oszone.ru/display.php?id=1415
    - http://www.netdocs.ru/articles/Crash-Course-IPv6-Part1.html
    - http://www.ing-ipv6.ru/
    - http://version6.ru/
    - W IPv6
2. Собрать схему лабораторной работы.
3. Подключить запоминающее устройство на USB (флэш-память). *(См. Лабораторная работа №4)*
4. Выполнить п 8.5, собрав данные в отчет.

5. Порядок выполнения работы

		Windows	Linux
		ipv6 install	su
		ipconfig	ifconfig eth0 192.168.0.100
Проверка IP стека 6-версии на данном компьютере		sc stop 6to4 ipconfig	
	Сам на себя: loopback	ping localhost ping loopback ping ::1	ping6 ::1
	Ethernet адаптер: Хост-интерфейс VirtualBox	ping fe80::2ff:cff:febf:a1ea *(Адрес* fe80::2ff:cff:febf:a1ea *указан при выполнении* ipconfig *и присваивается автоматически)*	ping6 -I eth0 fe80::a00:27ff:fec3:f8eb *(Адрес* fe80::a00:27ff:fec3:f8eb *указан при выполнении* ifconfig *и присваивается автоматически)*
Определить связность сети		ping6 fe80::a00:27ff:fec3:f8eb%5 *5- это номер индекса, определяется* ifconfig *или* ipv6 if. *Он является обязательным параметром (кроме* loopback *)- указывает через какой интерфейс передавать пакеты.*	ping6 -I eth0 fe80::2ff:cff:febf:a1ea
Добавить IP-адрес v6		ipv6 adu 5/fe80::100 ipconfig /all	ifconfig eth0 add fe80::200 ifconfig -v
Определить связность сети		ping fe80::200%5	ping6 -I eth0 fe80::100
Удалить IP-адрес v6		ipv6 adu 5/fe80::100 life 0 ipconfig	ifconfig eth0 del fe80::200 ifconfig

6. Содержание отчета

Лабораторная работа выполняется студентом в HTML-формате, созданная любым редактором, например, FrontPage, только не средствами MS Office Word/Excel любой версии.
Это требование вызвано условием уменьшения суммарного трафика всех лабораторных работ, т.к. работы отправляются и получаются через Interne

Лабораторная работа
Тема: Протокол IPv6 (часть 2)

1. Цель работы. Целью настоящей работы является изучение сетевых настроек операционных систем для работы по протоколу IP версии 6.
2. Задача лабораторной работы
Рассмотреть настройки операционных систем для работы по протоколу IP версии 6
3. Схема лабораторной работы

Работа тестировалась с операционной системой ОС Linux knoppix_5.0.iso (Debian) с использованием виртуальной машиной Sun xVM VirtualBox (Version 1.6.0 Edition. Sun Microsystems, Inc.). При этом в настройках созданной новой виртуальной машины указывалось:

1. Общие - Оперативная память не менее 64 Mb, Видеопамять не менее 8Mb
2. Жесткий диск - не подключать
3. CD/DVD-ROM - Образ knoppix_5.0.iso
4. Сеть - Адаптер 0/PCnet-Fast III (Хост-интерфейс VirtualBox 1)
    - *В настройках сетевой карты "Хост-интерфейс VirtualBox 1" установить IP-адрес:* 192.168.0.1/255.255.255.0
5. USB - Фильтр устройств 1 (активно)
    - *Фильтр устройств USB:* указать свою флеш-карту

4. Содержание работы
    1. Ознакомиться с со следующей информацией:
        - Выполнить лабораторную работу №8 Протокол IPv6
        - Встроенная помощь ОС MS Windows <Центр справки и поддержки>: Служебные программы IPv6
    2. Собрать схему лабораторной работы.
    3. Подключить запоминающее устройство на USB (флэш-память).
    4. Выполнить п 9.5, собрав данные в отчет.
5. Порядок выполнения работы

		Windows	Linux
		sc stop 6to4	su ifconfig eth0 192.168.0.100
Проверить стек IPv6		ping ::1	ping6 ::1
Добавить IP-адрес v6		ipv6 adu 5/fe80::100	ifconfig eth0 add fe80::200
Определить связность сети		ping fe80::200%5	ping6 -I eth0 fe80::100
Запрос ND (Neighbor Discovery) протокола IPv6 является набором сообщений и процессов,	Просмотреть кэш маршрутов	Выполнить посде выполнения команды ping	
		ipv6 rc	
	просмотреть кэш окружения	ipv6 nc	

определяющих отношения между соседними узлами.			
Вывод сведений об интерфейсах.		ipv6 if	
		ipv6 -v if 5 *5- это номер индекса интерфейса, определяется* ipv6 if.	
Отображение значений глобальных параметров для протокола IPv6.		ipv6 gp	
Отображение таблицы префиксов политики		ipv6 ppt	
Таблица маршрутизации протокола IPv6		ipv6 rt	
show address - Выводит IPv6-адреса. show bindingcacheentries - Выводит записи кэша привязок. show destinationcache - Выводит записи конечного кэша. show dns - Отображение адресов DNS-сервера. show global - Выводит общие параметры глобальной конфигурации. show interface - Выводит параметры интерфейса. show joins - Выводит адреса многоадресной рассылки IPv6. show mobility - Выводит параметры конфигурации мобильности. show neighbors - Выводит записи кэша соседей. show prefixpolicy - Выводит префиксные записи политики. show privacy - Выводит параметры конфигурации конфиденциальности. show routes - Выводит записи таблицы маршрутов. show siteprefixes - Выводит записи таблицы префиксов сайта. show state - Отображение состояния устаревшей функциональности. show teredo - Отображение состояния службы Teredo.		netsh interface IPv6 show address netsh interface IPv6 show destinationcache netsh interface IPv6 show global netsh interface IPv6 show interface netsh interface IPv6 show joins netsh interface IPv6 show mobility netsh interface IPv6 show neighbors netsh interface IPv6 show prefixpolicy netsh interface IPv6 show privacy netsh interface IPv6 show state netsh interface IPv6 show teredo netsh interface IPv6 show route	

6. Содержание отчета

Лабораторная работа выполняется студентом в HTML-формате, созданная любым редактором, например, FrontPage, только не средствами MS Office Word/Excel любой версии.

Это требование вызвано условием уменьшения суммарного трафика всех лабораторных работ, т.к. работы отправляются и получаются через Internet.

Лабораторная работа
Тема: Выбор аппаратной части сервера

Цель работы. Изучение состава аппаратного обеспечения сервера компьютерных сетей. Изучение программного обеспечения компьютерных сетей. Приобретение умения предоставлять общий доступ к принтеру локальной сети

План

1) Изучить назначение и основные функции аппаратного обеспечения сервера компьютерных сетей
2) Изучить программное обеспечение компьютерных сетей
3) Выполнить настройку общего доступа к принтеру локальной сети
4) Ответить на контрольные вопросы

Краткие сведения

При физическом соединении двух или более компьютеров образуется компьютерная сеть. Компьютерная сеть представляет собой комплекс технических, коммуникационных и программных средств, обеспечивающих эффективное распределение вычислительных ресурсов.

Уже сейчас есть сферы человеческой деятельности, которые принципиально не могут существовать без сетей (например, работа банков, крупных библиотек и т. д.) Сети используются при управлении крупными автоматизированными производствами, газопроводами, электростанциями и т.п.

В общем случае, для создания компьютерных сетей необходимо специальное аппаратное обеспечение - сетевое оборудование и специальное программное обеспечение - сетевые программные средства. Назначение всех видов компьютерных сетей определяется двумя функциями:

- ✓ обеспечение совместного использования аппаратных и программных ресурсов сети;
- ✓ обеспечение совместного доступа к ресурсам данных.

Например, все участники локальной сети могут совместно использовать одно общее устройство печати - сетевой принтер или, например, ресурсы жестких дисков одного выделенного компьютера - файлового сервера. Аналогично можно совместно использовать и программное обеспечение. Если в сети имеется специальный компьютер, выделенный для совместного использования участниками сети, он называется файловым сервером. Основными компонентами сети являются рабочие станции, серверы, передающие среды (кабели) и сетевое оборудование.

Рабочими станциями называются компьютеры сети, на которых пользователями сети реализуются прикладные задачи.

Серверы сети - это аппаратно-программные системы, выполняющие функции управления распределением сетевых ресурсов общего доступа. Сервером может быть это любой подключенный к сети компьютер, на котором находятся ресурсы, используемые другими устройствами локальной сети. В качестве аппаратной части сервера используется достаточно мощные компьютеры.

Аппаратура локальной сети обычно состоит из кабеля, разъемов, Т-коннекторов (рис. 1), терминаторов и сетевых адаптеров. Кабель, очевидно, используется для передачи данных между рабочими станциями. Для подключения кабеля используются разъемы. Эти разъемы через Т-коннекторы подключаются к сетевым адаптерам - специальным платам, вставленным в слоты расширения материнской платы рабочей станции. Терминаторы подключаются к открытым концам сети.

Рис. 1. Т-коннектор

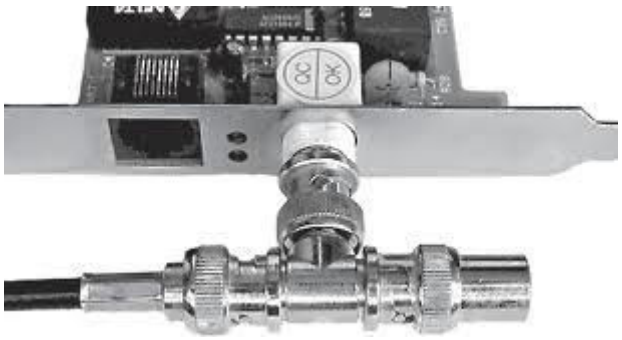


Рис. 2. Т-коннектор, присоединенный к сетевой карте

Для Ethernet (Ethernet — пакетная технология передачи данных преимущественно локальных компьютерных сетей) могут быть использованы кабели разных типов: тонкий коаксиальный кабель, толстый коаксиальный кабель и неэкранированная витая пара. Для каждого типа кабеля используются свои разъемы и свой способ подключения к сетевому адаптеру.

Сети можно создавать с любым из типов кабеля.

1. Витая пара (TP - Twisted Pair)– это кабель, выполненный в виде скрученной пары проводов (рис. 3). Он может быть экранированным и неэкранированным. Экранированный кабель более устойчив к электромагнитным помехам. Витая пара наилучшим образом подходит для малых учреждений. Недостатками данного кабеля является высокий коэффициент затухания сигнала и высокая чувствительность к электромагнитным помехам, поэтому максимальное расстояние между активными устройствами в ЛВС при использовании витой пары должно быть не более 100 метров.

Рис. 3 Кабель на основе витой пары

2. Коаксиальный кабель (рис. 4) состоит из одного цельного или витого центрального проводника, который окружен слоем диэлектрика. Проводящий слой алюминиевой фольги, металлической оплетки или их комбинации окружает диэлектрик и служит одновременно как экран против наводок. Общий изолирующий слой образует внешнюю оболочку кабеля. Коаксиальный кабель может использоваться в двух различных системах передачи данных: без модуляции сигнала и с модуляцией. В первом случае цифровой сигнал используется в таком виде, в каком он поступает из ПК и сразу же передается по кабелю на приемную станцию. Он имеет один канал передачи со скоростью до 10 Мбит/сек и максимальный радиус действия 4000 м. Во втором случае цифровой сигнал превращают в аналоговый и направляют его на приемную станцию, где он снова превращается в цифровой. Операция превращения сигнала выполняется модемом; каждая станция должна иметь свой модем. Этот способ передачи является многоканальным (обеспечивает передачу по десяткам каналов, используя для этого всего лишь один кабель). Таким способом можно

Рис. 4. Устройство коаксиального кабеля
1 — внутренний проводник (медная проволока),
2 — изоляция (сплошной полиэтилен),
3 — внешний проводник (оплётка из меди),
4 — оболочка (светостабилизированный полиэтилен).

передавать звуки, видео сигналы и другие данные. Длина кабеля может достигать до 50 км.

3. Оптоволоконный кабель (рис. 5) является более новой технологией, используемой в сетях. Носителем информации является световой луч, который модулируется сетью и принимает форму сигнала.

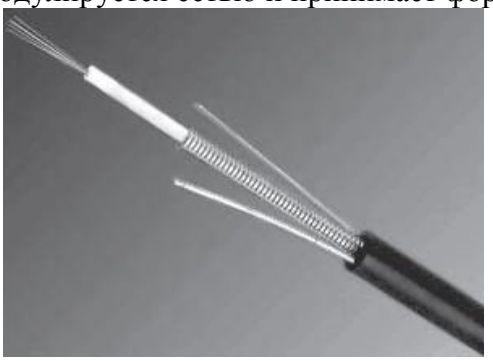


Рис. 5. Оптоволоконный кабель

Такая система устойчива к внешним электрическим помехам и таким образом возможна очень быстрая, секретная и безошибочная передача данных со скоростью до 2 Гбит/с. Количество каналов в таких кабелях огромно. Передача данных выполняется только в симплексном режиме, поэтому для организации обмена данными устройства необходимо соединять двумя оптическими волокнами (на практике оптоволоконный кабель всегда имеет четное, парное кол-во волокон). К недостаткам оптоволоконного кабеля можно отнести большую стоимость, а также сложность подсоединения.

4. Радиоволны в микроволновом диапазоне используются в качестве передающей среды в беспроводных локальных сетях, либо между мостами или шлюзами для связи между локальными сетями. В первом случае максимальное расстояние между станциями составляет 200 - 300 м, во втором - это расстояние прямой видимости. Скорость передачи данных - до 2 Мбит/с.

Выделяют следующие виды сетевого оборудования.

1. Сетевые карты – это контроллеры, подключаемые в слоты расширения материнской платы компьютера, предназначенные для передачи сигналов в сеть и приема сигналов из сети (рис. 6).

2. Терминаторы - это резисторы номиналом 50 Ом, которые производят затухание сигнала на концах сегмента сети.

3. Концентраторы (Hub) – это центральные устройства кабельной системы или сети физической топологии "звезда", которые при получении пакета на один из своих портов пересылает его на все остальные (рис. 7). В результате получается сеть с логической структурой общей шины. Различают концентраторы активные и пассивные. Активные концентраторы усиливают полученные сигналы и передают их. Пассивные концентраторы пропускают через себя сигнал, не усиливая и не восстанавливая его.

Рис. 6. Сетевая карта в виде платы расширения, устанавливаемой в PCI-слот

Рис. 7. Концентратор с фиксированным количеством портов

4. Повторители (Repeater)- устройства сети, усиливает и заново формирует форму входящего аналогового сигнала сети на расстояние другого сегмента (рис. 8). Повторитель

действует на электрическом уровне для соединения двух сегментов. Повторители ничего распознают сетевые адреса и поэтому не могут использоваться для уменьшения трафика. Повторители (repeater) представляют собой сетевые устройства, функционирующие на первом (физическом) уровне эталонной модели OSI. Для того чтобы понять работу повторителя, необходимо знать, что по мере того, как данные покидают устройство отправителя и выходят в сеть, они преобразуются в электрические или световые импульсы, которые после этого передаются по сетевой передающей среде. Такие импульсы называются сигналами (signals). Когда сигналы покидают передающую станцию, они являются четкими и легко распознаваемыми. Однако чем больше длина кабеля, тем более слабым и менее различимым становится сигнал по мере прохождения по сетевой передающей среде.

Рис. 8. Повторители (Repeater)

Целью использования повторителя является регенерация и ресинхронизация сетевых сигналов на битовом уровне, что позволяет передавать их по среде на большее расстояние. Термин повторитель (repeater) первоначально означал отдельный порт «на входе» некоторого устройства и отдельный порт на его «выходе». В настоящее время используются также повторители с несколькими портами. В эталонной модели OSI повторители классифицируются как устройства первого уровня, поскольку они функционируют только на битовом уровне и не просматривают другую содержащуюся в пакете информацию.

5. Коммутаторы (Switch) - управляемые программным обеспечением центральные устройства кабельной системы, сокращающие сетевой трафик за счет того, что пришедший пакет анализируется для выяснения адреса его получателя и соответственно передается только ему (рис.9).

Использование коммутаторов является более дорогим, но и более производительным решением. Коммутатор обычно значительно более сложное устройство и может обслуживать одновременно несколько запросов. Если по какой-то причине нужный порт в данный момент времени занят, то пакет помещается в буферную память коммутатора, где и дожидается своей очереди. Построенные с помощью коммутаторов сети могут охватывать несколько сотен машин и иметь протяженность в несколько километров.

Рис. 9. Коммутатор

6. Маршрутизаторы (Router) - стандартные устройства сети, работающие на сетевом уровне и позволяющее переадресовывать и маршрутизировать пакеты из одной сети в другую, а также фильтровать широковещательные сообщения (рис. 10).

7. Мосты (Bridge)- устройства сети, которое соединяют два отдельных сегмента, ограниченных своей физической длиной, и передают трафик между ними (рис.11). Мосты также усиливают и конвертируют сигналы для кабеля другого типа. Это позволяет расширить максимальный размер сети, одновременно не нарушая ограничений на максимальную длину кабеля, количество подключенных устройств или количество повторителей на сетевой сегмент.

Рис. 10. Беспроводной маршрутизатор

Рис. 11. Мосты (Bridge)-

8. Шлюзы (Gateway) - программно-аппаратные комплексы, соединяющие разнородные сети или сетевые устройства. Шлюзы позволяет решать проблемы различия протоколов или систем адресации. Они действует на сеансовом, представительском и прикладном уровнях модели OSI.

9. Мультиплексоры – это устройства центрального офиса, которое поддерживают несколько сотен цифровых абонентских линий. Мультиплексоры посылают и получают абонентские данные по телефонным линиям, концентрируя весь трафик в одном высокоскоростном канале для передачи в Internet или в сеть компании.

10. Межсетевые экраны (firewall, брандмауэры) - это сетевые устройства, реализующие контроль за поступающей в локальную сеть и выходящей из нее информацией и обеспечивающие защиту локальной сети посредством фильтрации информации. Большинство межсетевых экранов построено на классических моделях разграничения доступа, согласно которым субъекту (пользователю, программе, процессу или сетевому пакету) разрешается или запрещается доступ к какому-либо объекту (файлу или узлу сети) при предъявлении некоторого уникального, присущего только этому субъекту, элемента. В большинстве случаев этим элементом является пароль. В других случаях таким уникальным элементом является микропроцессорные карточки, биометрические характеристики пользователя и т. п. Для сетевого пакета таким элементом являются адреса или флаги, находящиеся в заголовке пакета, а также некоторые другие параметры. Таким образом, межсетевой экран - это программный и/или аппаратный барьер между двумя сетями, позволяющий устанавливать только авторизованные межсетевые соединения. Обычно межсетевые экраны защищают соединяемую с Internet корпоративную сеть от проникновения извне и исключает возможность доступа к конфиденциальной информации.

Беспроводные локальные сети считаются перспективным направлением развития ЛС. Их преимущество - простота и мобильность. Также исчезают проблемы, связанные с прокладкой и монтажом кабельных соединений - достаточно установить интерфейсные платы на рабочие станции, и сеть готова к работе.

Сердцем любой беспроводной сети является точка доступа (рис. 12), через которую конечные устройства по радио связываются с корпоративной сетью. Она определяет не только радиус действия и скорость передачи данных, но и решает элементарные задачи управления и обеспечения безопасности.

Хорошие точки доступа оснащаются двумя антеннами, причем в каждый момент времени работает антенна с лучшим качеством приема. Переключение антенн уже на удалении в несколько метров дает повышение качества и, соответственно, скорости передачи по сравнению с «однорукими» точками доступа. Обычно используемые ненаправленные антенны жестко крепятся к корпусу.

Радиохарактеристики точки доступа во многом определяются тем, какие антенны используются. Так, одну и ту же точку доступа с разными антеннами можно использовать для решения разных задач. Если, к примеру, точка доступа применяется в качестве радиомоста между зданиями, удаленными на 2 км или более (до 25 км), то предпочтительнее установить направленную антенну.

Рис. 12. Точка доступа

Программное обеспечение локальных сетей.

После подключения компьютеров к сети необходимо установить на них специальное сетевое программное обеспечение. Существует два подхода к организации сетевого программного обеспечения:

- ✓ сети с централизованным управлением;
- ✓ одно-ранговые сети. Сети с централизованным управлением.

В сети с централизованным управлением выделяются одна или несколько машин, управляющих обменом данными по сети. Диски выделенных машин, которые называются файл-серверами, доступны всем остальным компьютерам сети. На файл-серверах должна работать специальная сетевая операционная система. Обычно это мультизадачная OS, использующая защищенный режим работы процессора.

Остальные компьютеры называются рабочими станциями. Рабочие станции имеют доступ к дискам файл-сервера и совместно используемым принтерам, но и только. С одной рабочей станции нельзя работать с дисками других рабочих станций. С одной стороны, это хорошо, так как пользователи изолированы друг от друга и не могут случайно повредить чужие данные. С другой стороны, для обмена данными пользователи вынуждены использовать диски файл-сервера, создавая для него дополнительную нагрузку.

Есть, однако, специальные программы, работающие в сети с централизованным управлением и позволяющие передавать данные непосредственно от одной рабочей станции к другой минуя файл-сервер. Пример такой программы - программа NetLink. После ее запуска на двух рабочих станциях можно передавать файлы с диска одной станции на диск другой, аналогично тому, как копируются файлы из одного каталога в другой при помощи программы Norton Commander.

На рабочих станциях должно быть установлено специальное программное обеспечение, часто называемое сетевой оболочкой. Это обеспечение работает в среде той OS, которая используется на данной рабочей станции, - DOS, OS/2 и т.д.

Файл-серверы могут быть выделенными или невыделенными. В первом случае файл-сервер не может использоваться как рабочая станция и выполняет только задачи управления сетью. Во втором случае параллельно с задачей управления сетью файл-сервер выполняет обычные пользовательские программы в среде MS-DOS. Однако при этом снижается производительность файл-сервера и надежность работы всей сети в целом, так как ошибка в пользовательской программе, запущенной на файл-сервере, может привести к остановке работы всей сети. Поэтому не рекомендуется использовать невыделенные файл-серверы, особенно в ответственных случаях.

Существуют различные сетевые OS, ориентированные на сети с централизованным управлением. Самые известные из них - Novell NetWare, Microsoft Lan Manager (на базе OS/2), а также выполненная на базе UNIX System V сетевая OS VINES.

Контрольные вопросы

1. Что такое компьютерная сеть?
2. Что необходимо для создания компьютерных сетей?
3. Какова основная задача, решаемая при создании компьютерных сетей?
4. Что такое протоколы? Для чего они предназначены?
5. По какому принципу компьютерные сети делятся на локальные и глобальные?
6. Что такое интерфейсы?
7. Что такое серверы сети?
8. Какие сети называются одноранговыми?
9. Что такое рабочие станции?
10. Какие кабели можно использовать в качестве передающей среды в проводных сетях?
11. Что используются в качестве передающей среды в беспроводных локальных сетях?
12. Что представляет технология Ethernet?
13. Что такое сетевой адаптер?
14. Какие вы знаете топологии сетей?
15. Каковы преимущества беспроводных локальных сетей?
16. Каково назначение точки доступа?
17. Чем отличаются сети с выделенным сервером от одноранговых сетей?
18. Что такое технология клиент-сервер?
19. Приведите примеры сетевых операционных систем.
20. Что такое топология сети?
21. Что представляет собой проводник витая пара?
22. Каково устройство коаксиального кабеля?
23. Почему оптоволоконный кабель является приоритетным для проводных сетей? В чем его
    недостатки?
24. Что такое шлюзы? Какими могут быть шлюзы?
25. Зачем нужны повторители?
26. В чем состоят преимущества использования коммутаторов?
27. Для чего служит межсетевой экран (брандмауэр)?
28. Что такое концентратор?
29. Что такое маршрутизатор?
30. В чем заключаются преимущества и недостатки сетей с выделенным сервером?
31. Для чего предназначена программа NetLink?
32. Чем отличается выделенные файл-серверы от невыделенных?

Лабораторная работа
Конфигурирование web-сервера

Цель: освоить правила создания и конфигурирования web-сервера Apache и организации на нем хостинга.

Задание

- Изучить назначение и принцип работы web-сервера Apache.
- Сконфигурировать web-сервер Apache.

• Создать страницу wed-сайта, разместить на web-сервере и проверить ее доступность браузерам всех машин домена.

web-сервер Apache

web-сервер Apache (сервер HTTP) работает по принципу «запрос-ответ», принимая от клиентов (web-браузеров) запрос на получение определенного информационного ресурса, обозначаемого при помощи URL (Uniform Resource Locator – унифицированный указатель информационного ресурса), и передавая в ответ содержимое файла, который соответствует этому ресурсу.

Предоставление места на web-сервере для web-сайта и организация доступа к нему из сети называют хостингом.

Чтобы преобразовать Linux-систему в web-сервер, необходимо запустить /etc/rc.d/init.d/httpd, который будет прослушивать TCP-порт с номером 80 (в соответствии со стандартом HTTP). Основной конфигурационный файл службы httpd : /etc/httpd/conf/http.conf.

Конфигурирование web-сервера Apache

1. Войти в систему пользователем root, запустить Midnight Commander.
2. В конфигурационном файле /etc/httpd/conf/http.conf внести следующие изменения:

258 ServerName lin.ivanov.ibi : 80 – имя Web -сервера в своем домене

274 DocumentRoot " var/www/html " – корневой каталог Web-сервера

1044 <VirtualHost fir.ivanov.ibi :80> – параметры каждого Web-сайта

ServerAdmin webmaster@fir.ivanov.ibi

DocumentRoot /var/www/html/fir

ServerName fir.ivanov.ibi

ErrorLog logs/fir - error _ log

CustomLog logs/fir - access _ log common

</VirtualHost>

3. Создать каталог /var/www/html/fir, а в нем файл index.html со следующим содержанием:

<html>

<body bgcolor=green text=#ffffff>Проверка работы web-сервера </body>

</html>

4. При помощи утилиты setup включить web-службу httpd в начальную загрузку операционной системы (поставить звездочку клавишей пробел) и запустить эту службу командой service httpd start или путем перезагрузки операционной системы.

Регистрация web-сервера и web-ресурсов в службе DNS

5. На контроллере домена в службе DNS (Пуск–Программы–Администрирование–DNS) в своем домене, например, ivanov.ibi – Зоны прямого просмотра – ivanov.ibi прописать узел домена lin.ivanov.ibi (если его в домене нет; при этом поставить галочку Создать соответствующую RTR-запись) (рис. 1).

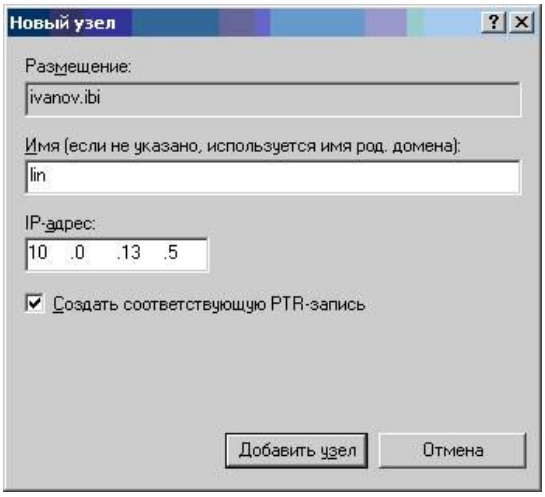


Рис. 1. Окно записи нового узла в службе DNS

6. Затем прописать созданный web-сайт (путем создания псевдонима fir.ivanov.ibi, присвоенного узлу с именем lin.ivanov.ibi) (рис. 2, 3).

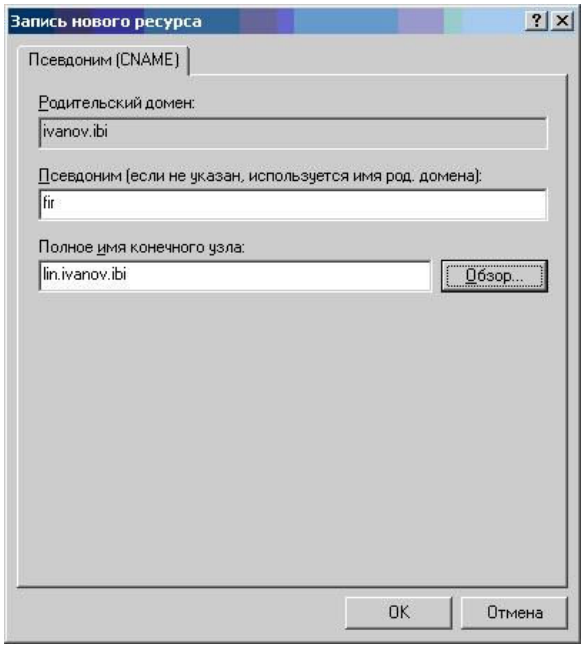


Рис. 2. Окно записи нового ресурса DNS

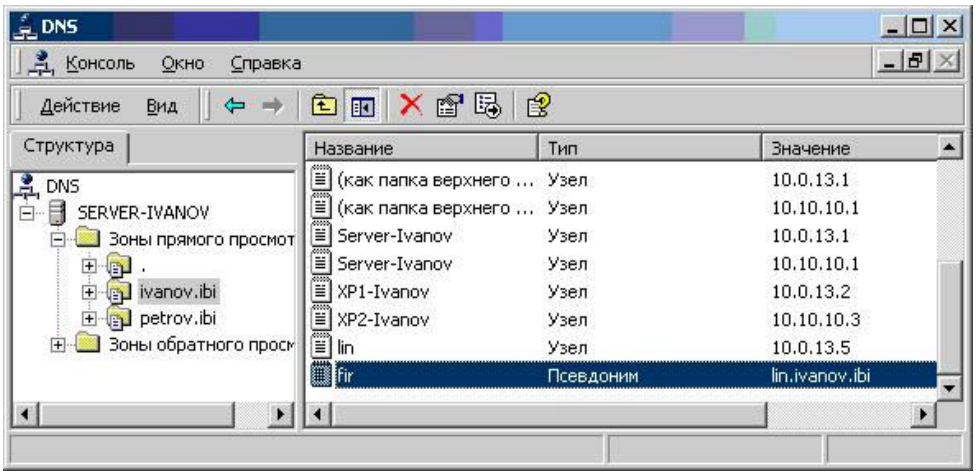


Рис. 3. Пример зоны прямого просмотра службы DNS

7. При помощи браузера (на всех компьютерах) проверить доступность созданного сайта (например, http://fir.ivanov.ibi). При этом автоматически должен открыться файл index.html.

Задание на самостоятельную работу

Исследовать возможности управления сервером HTTP в графическом режиме работы ОС Linux (рис. 4).

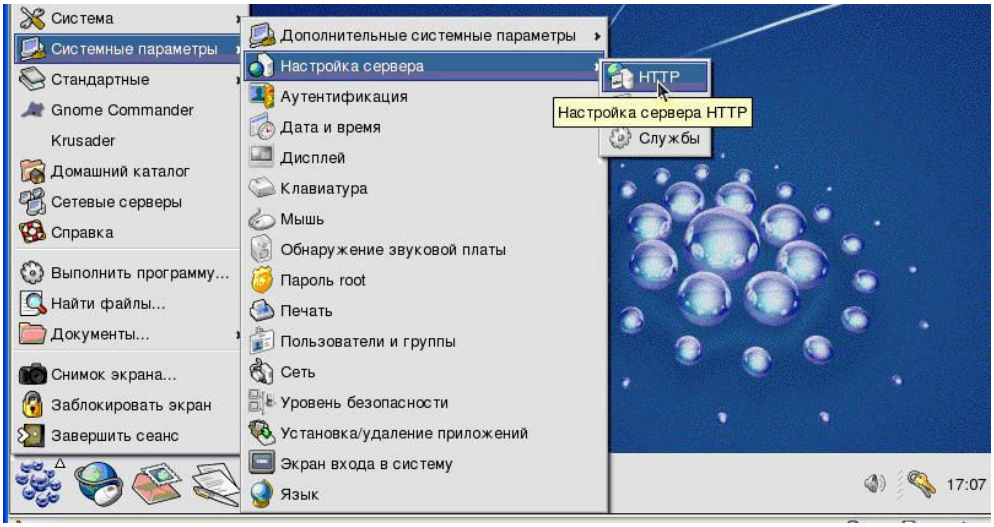


Рис. 4. Графический конфигуратор сервера HTTP в среде Gnom

При помощи графического конфигуратора создать новый web-ресурс на web-сервере Linux и проверить его доступность в сети Windows.

Лабораторная работа
Тема: Увеличение производительности сервера

Цель работы: Изучить, как изменится производительность системы при настройке интерфейса пользователя.

Краткие сведения

1 Проверить, как изменятся ресурсы системы при включении\выключении графических эффектов ОС. Для этого:

1.1 Войдите в меню Производительность из Панели управления — Администрирование.

1.2 Перейдите в категорию Журнал счетчиков. Создайте в ней счетчики с именем GUI и GUI2. Оба журнала выключите. Выберите п. контекстного меню «Свойства» у каждого журнала. Выберите тип журнала — двоичный файл. Сохраните файл журнала в папке c:\temp, создав ее при необходимости. Добавьте в созданные журналы все возможные счетчики из разделов «Процессор» и «Память».

1.3 Переключите ОС в режим: «Обеспечить наилучшее быстродействие». Запустите журнал с именем GUI и дайте ему поработать ровно 2 минуты. По окончании времени остановите журнал. Щелкните по нему правой клавишей мыши и выберите меню «Сохранить параметры как...». Сохраните полученный файл в папке Мои документы под именем GUI.html.

1.4 Переключите ОС в режим: «Обеспечить наилучший вид». Запустите журнал с именем GUI2 и дайте ему поработать ровно 2 минуты. По окончании времени остановите журнал. Щелкните по нему правой клавишей мыши и выберите меню «Сохранить параметры как...». Сохраните полученный файл в папке Мои документы под именем GUI2.html.

1.5 Откройте оба журнала в браузере. Просмотрите полученную динамику. Заполните таблицу:

Параметр	Значение					
	В GUI.html			В GUI2.html		
	Максимум	Минимум	Среднее	Максимум	Минимум	Среднее
% использования выделенной памяти						
Байт кэш-памяти						
Доступно байт						
Свободных элементов таблицы страниц						
Прерываний/сек						
% загруженности процессора						
% работы в пользовательском режиме						
% работы в привилегированном режиме						

1.6 Сделайте вывод, каким образом визуальные настройки влияют на быстродействие системы.

План

1. Войти в систему. Логин: osis. Пароль: osis
2. Запустить программу Virtual Box
3. Запустить ОС Windows XP в программе Virtual Box
4. Запустите меню «Свойства системы» в панели управления.
5. Выберите категорию «дополнительно» - «быстродействие». Нажмите кнопку

Параметры. В открывшемся окне изучите, какие настройки повышения производительности доступны.
6. Выполните задания.
7. Позовите преподавателя для проверки
8. Ответьте на контрольные вопросы.

Контрольные вопросы

1. Что называют счетчиком?
2. Что понимают под привилегированным режимом работы процессора?
3. Что называют кэш памятью?
4. Что называют прерыванием?

Лабораторная работа
Тема: Разборка принципов работы хостингов нескольких web-узлов

Цель работы: Ознакомиться с возможностями и принципом работы почтовой службы Web-mail.

План

1. Создать электронный почтовый адрес на любом поисковом сервере, поддерживающем работу с Web-mail.
2. Подготовить письмо с присоединенным файлом.
3. Использовать адресную книгу.
4. Подготовить письмо для одновременной отправки по нескольким адресам.
5. Просмотреть папку входящей почты и обработать полученную корреспонденцию - рассортировать ее по созданным вами папкам.

Контрольные вопросы

Составить подробный отчет о проделанной работе.

Лабораторная работа
Тема: Регистрация и мониторинг состояния хостинга

Цель работы: В понятие хостинг (от англ. hosting) включается предоставление дискового пространства на сервере провайдера (хостера), осуществление подключения к серверу через протоколы http, ftp, ssh. При этом такому виртуальному серверу назначается доменное имя. Услуги хостинга предоставляются либо за плату, либо бесплатно с условием обязательного размещения рекламы на страницах Вашего сайта. Среди лучших компаний-хостеров, предоставляющих платные услуги, можно указать "masterhost.ru","majordomo.ru" и "selectel.ru". Основные параметры бесплатного хостинга представлены в таблице 1.

Таблица 1 - Параметры бесплатного хостинга

Параметр	Сервер хостера	
	ucoz.ru	hostinger.ru
Размер дискового пространства, Мбайт	неограничено	2048
Подключение к серверу через FTP	да	да

Подключение к серверу через SSH	нет	нет
Поддержка языка PHP	нет	да
Поддержка баз данных MySQL	нет	да
Реклама хостера на каждой странице	да	нет

План

1. Регистрация пользователя на hostinger.ru

Для регистрации на сайте хостера hostinger.ru необходимо заполнить анкету, расположенную на странице hostinger.ru/zakazat. В форме регистрации указать:
Ваше имя: ваше_имя
Ваш e-mail: почтовый@ящик (укажите email, оформленный в первой лабораторной работе)
Пароль: пароль_к_панеле_управления (пароль должен быть не короче 6 символов и состоять из цифр, строчных и/или прописных латинских символов, без пробелов)
Повторите пароль: пароль_к_панеле_управления
Укажите символы, видимые на картинке
Поставьте галочку рядом с текстом "Я соглашаюсь с условиями Договора"
Нажмите на кнопку "Создать аккаунт"

На указанный Вами email будет отправлено письмо со ссылкой на подтверждение создания аккаунта. Перейдите в свой почтовый ящик, откройте письмо и перейдите по указанной в нем ссылке.

2. Регистрация бесплатного домена

Зайдите в панель управления сайтами: cpanel.hostinger.ru. Введите логин и пароль, указанные при регистрации. В верхней части окна расположено меню. Выберите пункт меню "Хостинг->Новый аккаунт". Из появившехся вариантов выберите тарифный план "Бесплатный". В появившемся окне укажите следующую информацию:
Выберите Тип Домена: Субдомен
Субдомен: имя.esy.es
Пароль: Придумать и указать пароль для администрирования сайта
Подтвердите Пароль: Повторить пароль
Нажать на кнопку "Продолжить"

В появившемся окне указать символы с картинки и поставить галочку рядом с текстом "Я согласен с правилами использования", а затем нажать на кнопку "Заказать". Поздравляем, в скором времени будет создан домен имя.esy.es и адрес Вашего сайта будет иметь вид: http://имя.esy.es

3. Создание базы данных

В верхнем меню выберите пункт "Хостинг->имя.esy.es". В разделе "Базы Данных" выберите значок "Базы Данных MySQL". В появившемся окне заполните поля формы:
Имя базы данных MySQL: u906740311_data
Имя пользователя MySQL: u906740311_user
Пароль: пароль_к_базе_данных

Повторите пароль: пароль_к_базе_данных
Нажать на кнопку "Создать"

4. Управление файлами

В верхнем меню выберите пункт "Хостинг->имя.esy.es". В разделе "Файлы" выберите значок "FTP Доступ". В появившемся окне отображены параметры доступа с серверу по протоколу FTP. Установите на своем компьютере один из FTP-клиентов и настройте его в соответствии с указанными выше параметрами.

Как альтернативный вариант Вы можете для управления файлами в режиме онлайн использовать "Файловый менеджер". Для этого в верхнем меню выберите пункт "Хостинг->имя.esy.es". Затем в разделе "Файлы" выберите значок "Файловый менеджер". Укажите язык "Russian" и нажмите кнопку "Установить". Появится список файлов, размещенных на Вашем виртуальном хостинге. Для загрузки файлов с локального компьютера на сервер, вызовите контектное меню щелчком на правой кнопке мыши и выберите пункт меню "Загрузить файлы".

4. Заполнить таблицу параметров сервера

Используя данные о параметрах хостинга необходимо заполнить строки в таблице.
Образец заполнения таблицы представлен в приложении.
Информацию о параметрах FTP-сервера находится
Таблица 2 - Параметры доступа к виртуальному серверу

Номер п/п	Параметр	Значение
1	Панель управления	
3	Логин	
4	Пароль	ЗАПОМНИТЬ!
5	FTP-сервер	
6	Логин к FTP-серверу	
7	Пароль к FTP-серверу	ЗАПОМНИТЬ!
8	MySQL-сервер	
9	Название базы данных	
10	Логин к базе данных	
11	Пароль к базе данных	ЗАПОМНИТЬ!

Контрольные вопросы

3. Оформление отчета по лабораторной работе

Пример заполнения таблицы параметров виртуального сервера

Номер п/п	Параметр	Значение
1	Панель управления	cpanel.hostinger.ru
3	Логин	name
4	Пароль	b789lev9x7
5	FTP-сервер	ftp.name.esy.es
6	Логин к FTP-серверу	u906740311
7	Пароль к FTP-серверу	e718prm7c5
8	MySQL-сервер	mysql.hostinger.ru
9	Название базы данных	u906740311_data
10	Логин к базе данных	u906740311_user
11	Пароль к базе данных	b789lev9x7

Лабораторная работа
Тема: Безопасность каталогов

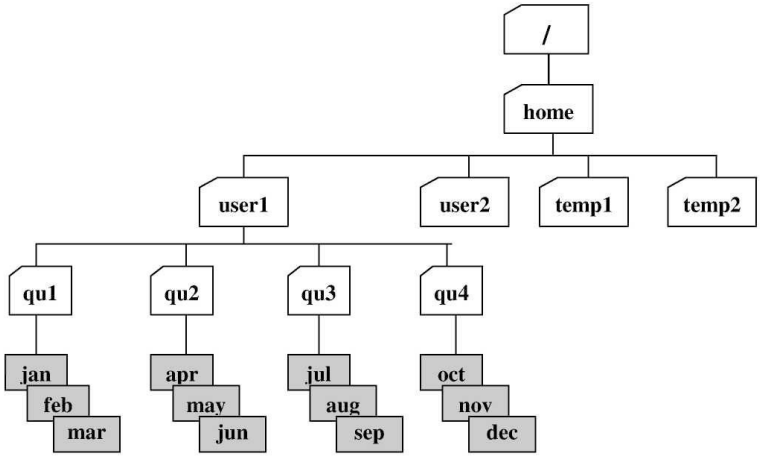
План

1. Создайте в ОС Linux двух пользователей (user1 и user2) и задайте их пароли. Зарегистрируйтесь в первой консоли как userl.

2. С помощью Ctrl+Alt+F2 (Alt+F2) откройте второй текстовый терминал и зарегистрируйтесь как user2.

3. Аналогично откройте третий текстовый терминал и зарегистрируйтесь в нем с правами суперпользователя.

4. Нажатием Ctrl+Alt-Fl (Alt-Fl) вернитесь в первую консоль. Теперь, переключая консоль, вы можете работать с объектами операционной системы от имени двух разных пользователей и администратора системы. Основная часть задания выполняется с правами обычного пользователя. Переходите в третью консоль и используйте права root только при выполнении соответствующих пунктов задания. Будьте внимательны при вводе команд! Помните, что операционная система не контролирует действий администратора и ваше ошибочное действие может привести к краху системы. Ориентируйтесь на приглашение к вводу команд.

5. 

5. С правами userl попробуйте войти в каталог /root. Объясните результат. С помощью команды ls -la / просмотрите список основных каталогов и укажите, каких прав доступа вам недостает для входа в каждый из каталогов.

6. ереключитесь в консоль администратора и создайте два новых временных каталога mkdir -m 777 /home/temp1 и mkdir -m 1777 /home/temp2. Проверьте права доступа к каталогам /home/user 1 и /home/user2: они должны быть установлены в 755. Вернитесь в консоль user1.

7. Пользуясь командой mkdir, создайте в домашнем каталоге пользователя /home/userl четыре каталога с именами: qul, qu2, qu3, qu4. При создании каталогов объявите следующие права доступа к ним: (qul - 777, qu2 - 404, qu3 - 1333, qu4 - 505. Пример: cd; mkdir -m 777 qu1). С помощью команды ls /home/userl убедитесь в том, что каталоги созданы. Какие из предоставленных прав кажутся Вам лишенными смысла? Почему?

8. Задайте права доступа к файлам "по умолчанию". Для этого установите umask 022. Поясните, какие права к вновь создаваемым файлам и каталогам будут предоставляться пользователю, членам его группы и остальным.

9. В каждом из каталогов создайте по три текстовых файла с именами (jan, feb, mar), (apr, may, jun), (jul, aug, sep), (oct, nov, dec). В каждый файл запишите календарь на определенный месяц текущего года. Например, команда cal 1 2010 > jan создает в текущем каталоге файл jan и записывает в него календарь на январь 2010 года. Не

забывайте, что использование относительного (короткого) имени файла требует, чтобы Вы находились в нужном ката логе. В противном случае следует указывать полный путь к создаваемому файлу. Для навигации по каталогам используйте команды cd и pwd. В каком случае создание файлов не удалось? Почему?

10. С помощью команды chmod измените нужные права доступа в "недоступные" каталоги qu2, qu4 и создайте там указанные файлы. После этого верни те каталогам прежние права доступа.

11. С помощью команд cd и ls войдите в каждый из созданных каталогов и просмотрите список созданных файлов. Для просмотра каталога необходимо по следовательно ввести две команды: cd и ls. При просмотре используйте два режима: ls без аргументов и ls -l. В каких случаях не удалось войти в ката лог? В каких случаях не удалось посмотреть список файлов? Почему?

12. Прочитайте содержимое одного из файлов в "темном" каталоге (например, cd /home/user1/qu3; cat aug). Сделайте выводы.

13. Перейдите во 2-ю консоль и с правами пользователя user2 войдите в каталог /home/user 1/qul. Создайте в каталоге /home/user2 новый файл quart1 путем конкатенации нескольких имеющихся (cat jan feb mar >/home/user2/quartl). С помощью команды file определите тип созданного файла. Попробуйте вывести его на экран командой cat. Что пред ставляет собой данный файл?

14. С помощью команды chmod установите права доступа 077 на созданный файл quart1. Вновь попробуйте прочесть его. Ответьте, почему владельцу файла запрещается доступ, если файл доступен для всех? Что необходимо сделать, чтобы вернуть владельцу права на доступ?

15. Установите для файла quatrl права на доступ 4700. Кому и какие права вы при этом предоставили? Как воспользоваться этими правами? Какие из предоставленных прав не имеют смысла?

16. Перейдите в консоль администратора и передайте право владения на файлы may и aug пользователю user2 (команда chown). Поочередно из консолей userl и user2 проверьте, как изменились права владения файлами после его передачи. Может ли пользователь user2 воспользоваться предоставленными правами?

17. С правами пользователя userl из каталогов /home/temp1 и /home/temp2 с по мощью команды ln создайте две "жесткие" ссылки на файл dec с именами dec_h1 и dec_h2 (пример: ln /home/user1/qu4/dec /home/templ/dec_hl). Чем созданные ссылки отличаются от исходного файла? На сколько байт уменьшилось дисковое пространство после создания этих ссылок?

18. С помощью команды ln -s создайте из каталогов /home/temp1 и /home/temp2 две символические ссылки на файл dec с именами dec_sl и dec_s2. Чем отличаются созданные ссылки от исходного файла? Попытайтесь прочитать содержимое файлов символических ссылок. Что они собой представляют?

19. С правами пользователя user2 с помощью команды ср создайте в каталогах /home/temp1 и /home/temp2 по одной копии файла dec с другим именем (dec_copyl). Чем отличаются исходный файл и его копия (обратите внимание на то, кто является владельцем исходного файла и его копии)? Чем отличаются права доступа на эти файлы? Вернитесь в консоль userl.

20. С помощью команды rm удалите файл dec. Что произошло с "жесткими" и символическими ссылками на данный файл? Что произошло с его копиями? Что нужно сделать для того, чтобы файл перестал существовать (на логическом уровне)?

21. С правами userl удалите файлы из каталогов /home/temp1 и /home/temp2. Какие файлы не удалось удалить? Почему? Попробуйте удалить оставшиеся файлы правами пользователя user2. Объясните результат.

22. Попробуйте удалить любой из каталогов qul, qu2, qu3, qu4 с помощью команды rmdir (не удаляя предварительно из них файлов). Объясните результат.

23. Войдите в консоль администратора и с правами root, пользуясь командой chattr, заблокируйте файл feb от любых изменений. Установите параметр запрета любых операций, кроме добавления данных для файла mar. Вернитесь в консоль userl. С помощью команды lsattr -1 проверьте наличие дополнительных атрибутов у файлов.

24. С правами пользователя userl добавьте одну строку finish в конец файлов feb и mar (воспользуйтесь для этого командой echo finish >> file_name). Убедитесь в успешном завершении операции, объясните результат.С правами пользователя userl с помощью команды rm -rf последовательно удалите ранее созданные каталоги qu2, qu3, qu4 вместе с файлами. Объясните результат.

25. С помощью команды md5sum вычислите и запишите контрольную сумму для одного из файлов в каталоге /home/user1/qul. Добавьте один символ в этот файл с помощью команды echo (например, echo a >> /home/userl/qul/jan). Вновь вычислите контрольную сумму файла и сравните два результата.

26. С помощью команды cat /dev/fdO попробуйте прочесть специальный файл устройства. Объясните результат? Для чего служат специальные файлы?

27. С помощью команды find с правами администратора найдите в корневом каталоге файлы:

> имеющие атрибуты SUID (find / -type f -perm -4000);

> файлы, которые разрешено модифицировать всем (find / -type f - perm -2);

> файлы, не имеющие владельца (find / -nouser);

> объясните, какой интерес могут представлять для администратора указанные категории файлов?

Зарегистрируйтесь в системе в консольном режиме с правами root. \

Работа с учетными записями пользователей

28. Используя команду cat с правами root, просмотрите содержимое файла /etc/passwd. Файл представляет собой таблицу, каждая строка которой представляет отдельную учетную запись, состоящую из 7 полей. Обратите внимание на характерные разделители полей (регистрационное имя, признак пароля, идентификатор пользователя, идентификатор группы, дополни тельная информация, "домашний" каталог, имя командного процессора) в виде двоеточия. Символ x вместо пароля указывает на то, что хэшированный пароль находится в другом файле - /etc/shadow.

29. Аналогично изучите содержимое файла /etc/shadow. Он также представляет собой таблицу, каждая строка которой состоит из 9 полей, разделенных двоеточиями (регистрационное имя, хэшированный пароль, контрольные сроки в днях, среди которых:

- число дней с 1.01.70 г. до дня последнего изменения пароля,
- минимальное число дней действия пароля со дня его последнего изменения,
- максимальное число дней действия пароля,
- за сколько дней до устаревания пароля система начнет выдавать предупреждения,
- число дней со времени обязательной смены пароля до блокировки учетной записи,
- день блокировки учетной записи.

Последнее, девятое поле зарезервировано и не используется.

31. Вам необходимо создать учетные записи и определить права доступа для десяти (10) сотрудников: w_gromov, n_kalinina, e_ivanova, r_klinova, b_rebrov, k_beglov, i_frolov, d_lavrov, m_kruglov, t_uporov, работающих в одном подразделении и занятых созданием и редактированием текстовых документов различного уровня

конфиденциальности. Разграничение доступа к информации должно быть произведено на основании следующих требований:

> допуск к секретным сведениям имеют четыре пользователя: w_gromov, n_kalinina, b_rebrov, k_beglov;

> три пользователя: n_kalinina, b_rebrov, k_beglov работают над созданием секретных документов, каждый по своему профилю. Их домашние каталоги и файлы должны быть полностью недоступными как друг для друга, так и для всех остальных, исключая w_gromov;

> три пользователя: i_frolov, d_lavrov, e_ivanova имеют допуск к конфиденциальной информации и работают над документами с соответствующим грифом. Они имеют право читать файлы с конфиденциальной информацией, созданные своими коллегами, без права их модификации;

> все секретоносители имеют право знакомиться с конфиденциальными файлами;

> три пользователя: r_klinova, m_kruglov, t_uporov могут работать только с открытой информацией. Их файлы должны быть доступны для чтения каждому сотруднику подразделения (без права модификации);

> w_gromov является редактором подразделения и имеет право читать и модифицировать файлы всех сотрудников и всех уровней конфиденциальности. Завершенные документы копируются пользователем w_gromov в его домашний каталог, который должен быть недоступен для всех остальных сотрудников подразделения.

32. Укажите в отчете, какие коллизии вы усматриваете в сформулированных требованиях? Как реализовать указанные требования таким образом, чтобы пользователи не могли по своему усмотрению изменять установленный по рядок?

33. С помощью команды groupadd создайте четыре пользовательских группы: alfa, beta, nabla, sigma. Формат команды groupadd -g GID group_name. Идентификатор группы GID можно назначать произвольно, начиная с номера 100 (например, groupadd -g 101 alfa).

34. Создайте учетные записи для вышеуказанных десяти новых пользователей. Регистрационные данные (кроме паролей и групп) сведены в таблицу. Пароли назначайте произвольно, длиной не менее 8 символов, не забывая фиксировать их в черновике отчета. Для пользователей e_ivanova, r_klinova задайте одинаковые пароли. Распределите сотрудников по группам таким образом, чтобы удовлетворить вышеперечисленным требованиям. Изобразите в отчете схему, поясняющую разграничение доступа сотрудников подразделения к компьютерной информации.

35. Пять первых пользователей (w_gromov, n_kalinina, e_ivanova, r_klinova, b_rebrov) зарегистрируйте с помощью команды useradd. Синтаксис коман ды: useradd -u UID -g group_name -d dir_home -m -p password -e date_del_user user_name. Например, useradd -u 501 -g sigma -d /home/n_kalinina -p v5g7K2S4 -e 2011-01-07 n_kalinina. Параметр -m обеспечивает создание домашнего каталога пользователя, если он еще не существует. Прочие параметры команды можно не указывать. Помните, имя пользователя не должно начинаться с цифры и содержать заглавных и русских букв, символов типа *#%л.... Идентификаторы пользователей UID назначаются, начиная с 500. Дата удаления учетной записи пользователя вводится в формате ГГГГ-ММ-ДД.

36. Пять последних пользователей зарегистрируйте с помощью командного файла adduser, которая запрашивает значения в интерактивном режиме. При вводе данных ориентируйтесь на подсказки системы [в квадратных скобках]. Все параметры, кроме имени пользователя, его идентификатора, имени группы, пароля и домашнего каталога можно игнорировать. Для ввода параметра по умолчанию вводить Enter. В некоторых дистрибутивах ОС Linux командный файл adduser отсутствует, и в этом

случае регистрацию остальных пользователей следует произвести аналогично пункту 8. При использовании adduser символ подчеркивания в имени пользователя не воспринимается. Если это так, замените этот символ в именах пользователей на символ дефиса.

Таблица 1

Пользователи	ID	Пароль	Группа	Домашний каталог	Дата удаления учетной записи
i_frolo				/home/i_frolov	T+ 10 дней
m_krug				/home/m_krug	T+ 30 дней
b_rebro				/home/b_rebro	T+ 12 дней
d_lavro				/home/d_lavro	T+ 60 дней
e_ivano				/home/e_ivano	T+ 30 дней
t_uporo				/home/t_uporo	T+ 15 дней
k_beglo				/home/k_beglo	T+ 45 дней
n_kalin				/home/n_kalini	T+ 30 дней
r_klino				/home/r_klino	T+ 90 дней
w_gro				/home/w_grom	не удалять

37. Переключаясь во вторую консоль, отслеживайте изменения, происходящие в файле /etc/passwd по мере ввода новых учетных записей.

38. Попробуйте с правами пользователя посмотреть файл /etc/shadow. Повторите попытку просмотра с консоли суперпользователя. Почему поля, отведенные для хэшированных паролей у пользователей e_ivanova и r_klinova различаются? Обратите внимание на то, что во многих дистрибутивах ОС утилита useradd работает некорректно и записывает пароли в файл в открытом виде! Поскольку система воспринимает эту запись в качестве хэш- функции пароля, у пользователя с подобной учетной записью нет никаких шансов войти в систему. Администратору в этом случае рекомендуется в ответ на соответствующий вопрос useradd ввести пустой пароль (в файле /etc/passwd в поле признака пароля при этом будет стоять восклицательный знак), а затем установить пароль пользователю с помощью команды passwd.

39. Из первой консоли с помощью команды su измените права администратора на права пользователя w_gromov. Почему система не запрашивает пароль? С помощью команды exit верните себе права администратора. Был ли запрошен пароль? (В различных дистрибутивах Linux возврат полномочий адми нистратора организован различным образом).

40. Запустите оболочку Midnight Commander в режиме редактирования (F4) файла паролей /etc/passwd и удалите в учетной записи пользователя n_kalinina символ признака пароля (между первым и вторым двоеточием), включая пробел. Сохраните изменения в файле, завершите сеанс в Midnight Commander, с помощью Ctrl+Alt+F2 (Alt+F2) откройте второй текстовый терминал и зарегистрируйтесь пользователем n_kalinina, но теперь с «пустым» паролем. Сделайте вывод относительно опасности предоставления прав на запись в этот файл. Завершите сеанс для пользователя n_kalinina с помощью команды exit.

41. Пользователь d_lavrov уволен за дисциплинарный проступок. С помощью команды userdel -r user_name удалите его учетную запись вместе с домашним каталогом. В реальных условиях необходимо вначале скопировать в другую директорию файлы пользователя, представляющие ценность для организации.

42. Зарегистрируйте вместо уволенного пользователя нового сотрудника f_mironov с предоставлением ему аналогичных прав (пароль должен быть новым!).

43. Пользователь r_klinova убыла в командировку сроком на две недели. Заблокируйте ее учетную запись, для чего с правами администратора войдите в режим редактирования файла паролей и вставьте во второе поле (между первым и вторым двоеточием) любой символ, который не разрешено использовать для пароля. Попытайтесь зарегистрироваться во второй консоли с правами r_klinova и убедитесь в том, что для этого пользователя система не доступна.

44. Зарегистрируйтесь во второй консоли с правами пользователя k_beglov, вызовите команду passwd и измените свой пароль. В качестве нового пароля введите qwerty.

45. Перейдите в консоль администратора и назначьте пользователю k_beglov новый пароль zxcvbnm. Затем с помощью команды chage (change aging - изменить информацию об устаревании) установите для этого пользователя минимальное время действия паролей, равное 5 дням. С какой целью устанавливается минимальный срок действия пароля?

46. Просмотрите электронную справку по файлу /etc/sudoers. Отредактируйте его таким образом, чтобы предоставить следующим пользователям дополни тельные права за счет использования команды sudo:

> пользователю e_ivanova - право монтировать файловые системы,

> пользователю b_rebrov - право изменения владельца файлов.

Ответьте, чем отличается предоставление прав пользователям с помощью sudo от использования эффективных идентификаторов SUID?

47. Из второй консоли с правами пользователя f_mironov создайте файл cal 2010 > /home/f_mironov/cal2010. С помощью команды su переключите консоль на пользователя b_rebrov и с помощью временно предоставленных ему привилегий передайте права на созданный f_mironov файл другому владельцу n_kalinina. Каким еще путем можно предоставить подобные права пользователям, не передавая им "опасных" полномочий администратора?

48. Просмотрите с правами администратора системные журналы в каталоге var/log и убедитесь, что система зафиксировала факты присвоения полномочий администратора.

Изучение и анализ отображаемой информации о процессах

49. Из консоли пользователя командой ps -ef l | more выведите расширенный поэкранный список исполняемых процессов (перечень параметров для расширенного вывода информации можно уточнить с помощью электронного справочника man ps). Разберитесь с выводимой информацией. Определите процессы:

> по типу: системные, демоны, пользовательские (тип процесса определяется по косвенным признакам, в частности, по имени),

> по состоянию S: (исполняющиеся - R или O, ожидающие записи на диск - D, ожидающие событий - S, приостановленные - T, зомби - Z и т.д.),

> по текущему динамическому приоритету PRI (наименьшее значение у высокоприоритетных процессов),

> по относительному приоритету N1.

50. В консоли суперпользователя запустите утилиту top для текущего контроля процессов. Утилита позволяет отобразить наиболее активные процессы (столько, сколько их помещается на экран) с достаточно полной информацией о них (для пользователя утилита представляет ограниченный набор выводимых параметров).

51. Из первой консоли создайте процесс od /dev/zero > /dev/null. В соответствии с введенной командой утилита od читает и выводит непрерывный поток нулевых байт из «рога изобилия» в нулевое устройство. Переключившись в другую консоль, с помощью команды top просмотрите список наиболее активных процессов. Найдите и идентифицируйте запущенный процесс, найдите по идентификатору PPID его «родителя», определите его приоритет (возможно это - величина переменная),

долю загрузки централь ного процессора %CPU и оперативной памяти %MEM.

52. Поочередно из первой и второй консолей с правами администратора и пользователя с помощью команды od /dev/zero > /dev/null & создайте по 2-3 одинаковых фоновых процесса.

53. По мере создания новых процессов отслеживайте в третьей консоли их текущий приоритет, загрузку процессора и памяти. Имеются ли различия в приоритете процессов, выполняемых от имени администратора и пользователя?

54. С консоли пользователя userl измените приоритет одного из принадлежащих ему процессов. Для этого воспользуйтесь командой renice -10 PID. Изменился ли относительный приоритет процесса?

55. Повторите предыдущий пункт с правами администратора.

56. Переключитесь в консоль пользователя и измените приоритет одного из принадлежащих ему процессов командой renice 5 PID. Произошло ли изменение приоритета?

57. Проконтролируйте из третьей консоли изменение приоритетов запущенных процессов.

58. Удалите созданные процессы командой kill.

Управление процессами

59.59. С правами пользователя создайте в своей директории сценарий с именем abcd. Сценарий можно создать с помощью команды cat:

60.cat >abcd

61.#! /bin/bash

62.while : rem обратите внимание на пробел перед двоеточием!

63.do

64.echo HELLO!

65.done

66.Ctrl+d

67.Используя команду chmod, присвойте пользователю полные права на чтение, запись и исполнение данного сценария. Запустите сценарий на исполнение (на экран должны непрерывно выводиться приветствия HELLO!)

68. Перейдите в третью консоль, с помощью команды top просмотрите список процессов и найдите в нем «зависший» процесс, запущенный пользователем (на самом деле это только имитация зависания, которое пользователь легко может прекратить сам). Прочитайте идентификатор процесса PID.

69.Нажатием Ctrl+C из второй консоли остановите процесс. Как изменилось при этом состояние процесса?

70.Повторно запустите из второй консоли процесс, перейдите в первую консоль и отправьте "зависшему" процессу сигнал на останов (команда kill -15 PID_process).

71.Перейдите в другую консоль и отправьте «непослушному» процессу сигнал kill -20 PID. Как реагирует процесс на данный сигнал? Посмотрите в электронном справочнике, что означает данный сигнал.

72. С помощью команды kill -9 PID отправьте этому процессу сигнал принудительного завершения. С другой консоли проконтролируйте выполнение команды. Остановился ли процесс? Остался ли он в списке процессов? Какая программа на самом деле перехватывает и исполняет команду kill -9 PID?

73. С помощью команды echo $PATH поочередно из консоли администратора и пользователя userl выведите список директорий, в которых производится поиск исполняемых файлов, заданных только по имени. В чем заключается различие выведенных списков? Почему в списке PATH администратора отсутствует текущий каталог (.)? Почему в списке PATH пользователя отсутствует каталог /sbin? Имеет ли пользователь возможность изменить порядок проверки каталогов для администратора?

74. Попробуйте запустить несколько утилит из второй консоли с правами

пользователя (например, renice -10 PID, date -s O). Как реагирует система на ваши попытки?

75. Перейдите в административную консоль и повторите запуск утилит с правами суперпользователя.

76. Убедитесь в том, что пользователю разрешен запуск указанных утилит. Объясните, почему пользователь не может запустить утилиты с некоторыми «критичными» параметрами? Где, по вашему мнению, расположен механизм контроля за ходом запуска (в ядре операционной системы, в командной оболочке, в самой утилите?). Ответ обоснуйте.

77. С правами пользователя скопируйте в свой рабочий каталог один из исполняемых файлов с параметром SUID каталога /bin (исполняемые файлы вы делены цветом и символом *, а параметр SUID отмечен символом «s» в правах владельца на исполнение). Как изменились права доступа к файлу после его копирования?

78.70. Из второй консоли с правами пользователя скопируйте в свой домашний каталог утилиту, которую разрешено запускать только администратору (напри мер, chattr). Копирование производите с параметрами, гарантирующими переход копии во владение пользователю. Убедитесь, что пользователь имеет на скопированный файл все необходимые права. Попробуйте использовать свою копию утилиты по ее назначению (в случае копирования утилиты chattr установите дополнительный атрибут +i одному из своих файлов). Сделайте выводы.

Контрольные вопросы

- Какие дополнительные атрибуты можно присвоить файлу в файловой систе ме EXT2FS? Как эти атрибуты влияют на обеспечение конфиденциальности, целостности и доступности информации?
- Для каких целей могут использоваться «темные» каталоги?
- Какие права по отношению к файлам и каталогам вам необходимо иметь для копирования файла? Как изменяются при этом атрибуты копии?
- Администратор по невнимательности ввел следующую команду: chmod -R 555 / . Что последует за выполнением этой команды?
- Какую опасность для системы представляют файлы, не имеющие владельца?
- Как можно найти файл по его inode?
- Достаточно ли трех базовых прав доступа к файлам для реализации в ОС Linux требуемой политики безопасности?
- Какие изъяны вы усматриваете в использованных утилитах регистрации учетных записей пользователей?
- Может ли пользователь закрыть для себя доступ к собственному файлу? Каким образом? Почему система не соотносит владельца файла ни с его группой, ни со всеми остальными?
- Существуют ли способы ограничения доступа суперпользователя к некоторым конфиденциальным файлам?
- Какие дополнительные права администратор может предоставить пользователям с помощью утилиты sudo и регистрационного файла /etc/sudoers?
- Чем отличаются системные процессы, «демоны» и пользовательские процессы?
- Почему пользователю не разрешается повышать приоритет процессов?
- Усматриваете ли вы какую-либо опасность в возможности понижения приоритета пользовательских процессов?
- В консоли, с которой вы работаете, произошло «зависание», вызванное неправильным исполнением одного из ваших процессов. Каким образом можно повлиять на возникшую ситуацию?
- Какие угрозы безопасности связаны с использованием эффективного

идентификатора SUID? Почему администратор должен учитывать и контролировать процессы с таким идентификатором?

- С помощью команды find найти в файловой системе:

-файлы, содержащие в имени некоторый шаблон (набор символов);
-файлы с установленными битами SUID и SGID;
-файлы, принадлежащие некоторому пользователю;
-файлы, не принадлежащие никакому пользователю;
-файлы, измененные после некоторой даты.

- Автоматизировать процесс сохранения md5sum для некоторого списка файлов (заданного в виде текстового файла) и последующей проверки совпадения текущих значений хеш-функции с сохраненными ранее.
- Реализовать защиту файла, содержащего хеш-функции контролируемого набора файлов с помощью механизма цифровой подписи.
- Написать и скомпилировать программу, отправляющую сообщения syslog и настроить запись сообщений данной программы в отдельный log – файл.

Лабораторная работа

Тема: Отключение прав пользователей хостинга

Цель работы: Изучить файловые операции в python
Ознакомиться с принципами тестирования и библиотеками тестирования

План

1. Доработать сервер из предыдущей лабораторной работы так, чтобы он выдавал клиенту содержимое файловой системы. Корень сервера должен задаваться через параметры командной строки или через конфигурационный файл.
2. Дополнительное задание. Написать тест, проверяющий отображение полного списка файлов в папке. Написать тест, проверяющий соответствие выдачи сервера содержимому файловой системы. Написать тест, проверяющий статусы ответов (404 — файл не найден, 403 — ошибка доступа, 200 — OK)
3. Сохранить результат работы в системе контроля версий.

Описать следующие шаги работы:

- проектирование приложения
- проверка работоспособности и правильности работы (ручная или автоматизированная)

Если вы не знакомы с Django, лучше начать с предыдущей работы.
Для отправной точки можете взять за основу этот код и доработать его:

view rawfunctions.py hosted with ❤ by GitHub

Дополнительная цель этой работы - научиться устанавливать и использовать модули. Установить библиотеку - задача не совсем простая. Считайте, что ПВК - это shared хостинг, где вы не имеете прав администратора. Вобщем-то, это единственно правильная точка зрения при разработке любого ПО. Администратор нужен для установки ПО а не для его разработки.
У каждого проекта есть свои библиотеки. Кто-то использует Django, кто-то Flask, где-то вресии этих библиотек могут пересекаться, а хуже - противоречить друг другу. В Linux по большому счёту нельзя поставить две версии одной и той же библиотеки. Как быть? На помощь приходят среды окружения.
Buildout разработан в корпорации Zope, поэтому пакет называется zc.buidlout.
Buildout мы не будем устанавливать в систему, а будем его бутстрапить. Для этого в папке проекта делаем следующий маневр:

```
curl -O http://downloads.buildout.org/2/bootstrap.py
```

```
C:\Python27\python.exe bootstrap.py
```

Рядом создаем файл с именем buildout.cfg следующего содержания:

```
[buildout]
parts = main

[main]
recipe = zc.recipe.egg
eggs = Django
      South >=0.7,!=0.7.4
      python-dateutil ==1.5
;     xhtml2pdf ==0.0.3
      django-tastypie >=0.9,<1.0
interpreter = python
```

Питоновские пакеты хранятся на сайте PYPI и его зеркалах. О соглашениях про номера версий можете прочитать здесь и здесь.
Если у вас есть права на запуск сетевых приложений, можно использовать связку virtualenv + pip. Установить их довольно просто, если у вас есть пакетsetuptools. Устанавливается командой

```
easy_install virtualenv
```

А для убунтоводов есть пакет python-virtualenv.
В двух словах, как пользоваться:
Создаете среду командой

```
1.  virtualenv env
```

Должна появиться папка env, в которой будет python и его библиотеки.

1. Активировать среду

```
2.  <\path\to\env>\Scripts\activate
```

Устанавливать пакеты через pip install имя_пакета
Выключить режим “среды” командой deactivate

Лабораторная работа

Настройка файрвола iptable

Цель работы: Ознакомиться с принципами работы межсетевого экрана netfilter, встроенного в ядро ОС Linux на примере дистрибутива OpenSuSE. Изучить правила построения фильтров и процедуру настройки файрвола с помощью утилит iptables и SuSEfirewall2.

Общие сведения

Межсетевой экран (файрвол, брандмауэр) — это средство контроля и управления трафиком, проходящим через сетевой интерфейс(ы). Основной задачей файрвола является защита узлов сети от несанкционированного доступа. Общий принцип как аппаратных, так и программных межсетевых экранов сводится к фильтрации проходящих пакетов на основе заданного набора правил. Дополнительно файрволы могут выполнять трансляцию адресов (NAT) и перенаправление адресов/портов.

Задания к работе

1. Вывести список текущих правил (iptables -Lnv)
2. Сохранить текущие настройки в файле iptables.backup (iptables-save > iptables.backup, имя файла может быть любое).
3. Очистить все правила файрвола
4. Создать скрипт, загружающий следующий набор фильтров:
   - все исходящие пакеты с локального хоста разрешить;
   - все входящие ICMP-пакеты разрешить;
   - все входящие пакеты на TCP- и UDP- порты выше 1024 разрешить;
   - все входящие пакеты на TCP-порты 20, 21 разрешить
   - все входящие пакеты на порты 22, 139 журналировать и отбрасывать
   - все входящие пакеты на TCP-порт 80, 443, 8080 разрешить
   - все остальные входящие пакеты запретить
5. Подключить скрипт в автоматическую загрузку при запуске системы;
6. Протестировать работоспособность созданного набора фильтров;
7. Удалить все правила и снова протестировать систему;
8. Вернуть сохраненные настройки файрвола (из резервного файла).

Файрвол или брандмауэр?

В русском языке для обозначения межсетевого экрана используют заимствованные слова «файрвол» (анг. *firewall*) и «брандмауэр» (нем. *Brandmauer*), которые оба дословно переводятся как «огненная стена» и обозначают противопожарный барьер между зданиями. Дискуссию о том, какая транскрипция англоязычного термина будет более правильной: *файрволл, файрвол, файервол или фаервол*, — оставим на забаву филологам.

Методические указания

Межсетевой экран netfilter

Ядро операционной системы Linux с версии 2.0.x имеет встроенный межсетевой экран, разрабатываемый и поддерживаемый в рамках открытого проекта netfilter.org. Файрволл Linux традиционно называют iptables, хотя правильным названием является netfilter.

Netfilter представляет собой набор структур данных и функций перехвата («хуков», от анг. hooking), реализованных на уровне ядра системы и позволяющих замещать стандартные системные вызовы стека TCP/IP на callback-функции, обрабатывающие каждый сетевой пакет. Перехватываемые пакеты сопоставляются с набором правил, представленных в виде таблиц с регулярной структурой (ip_tables). Правила описывают условия соответствия и указывают дальнейшие действия над пакетом, попадающим под заданные условия: фильтрация, трансляция адресов (NAT) и прочие преобразования.

Основные возможности

- Поддержка протоколов IPv4 и IPv6.
- Фильтрация сетевого уровня (без контроля состояния — stateless).
- Контроль состояния (фильтрация сеансового уровня — stateful).
- Все виды трансляции адресов и портов (NAT/NAPT).
- Несколько слоев API для расширений сторонних разработчиков.

Этот брандмауэр может использоваться для контроля трафика как на маршрутизаторах с несколькими сетевыми интерфейсам, так и на персональных рабочих станциях: алгоритм обработки пакетов будет одинаковым в обоих случаях (рис. 1).

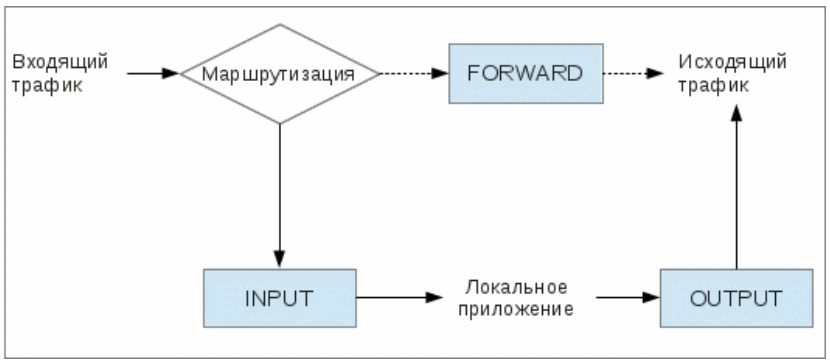


Рис. 1. Концепция обработки пакетов файрволом netfilter

Некоторые пояснения к рис. 1:

1. Для каждого входящего пакета, захваченного файрволом, определяется адресат и дальнейший маршрут.
2. Если адресатом является локальный процесс, то пакет поступает в *цепочку* INPUT, где он проверяется на предмет соответствия *правилам* этой цепочки. К пакету применяется первое подходящее правило. Если пакет не соответствует ни одному правилу цепочки, то он отбрасывается.
3. Если в системе несколько сетевых интерфейсов и настроена переадресация, а пакет предназначен для другого сетевого интерфейса, то он передается для обработки в цепочку FORWARD. Если переадресация не используется или система не знает как обработать принятый пакет, то он отбрасывается.
4. Наконец, локальный процесс может инициировать отправку пакетов. Исходящие пакеты поступают в цепочку OUTPUT.

Правила, цепочки и *таблицы* - это названия основных «строительных блоков» netfilter/iptables:

- **Правило** — структура, описывающая критерии соответствия, применяемое действие и счетчика. Если пакет соответствует критерию, к нему применяется указанное действие, и этот факт фиксируется счетчиком.
- **Цепочка** — упорядоченный набор правил, последовательно применяемых к пакету. На рис. 1 цветом отмечены цепочки INPUT, FORWARD и OUTPUT. Они, а также цепочки PREROUTING и POSTROUTING, являются *базовыми* и создаются при инициализации таблиц. Помимо базовых, iptables позволяет создавать *пользовательские* цепочки.
- **Таблица** — совокупность базовых и пользовательских цепочек, объединенных общим функциональным назначением.

Связь между перечисленными элементами проиллюстрирована на рис. 2.

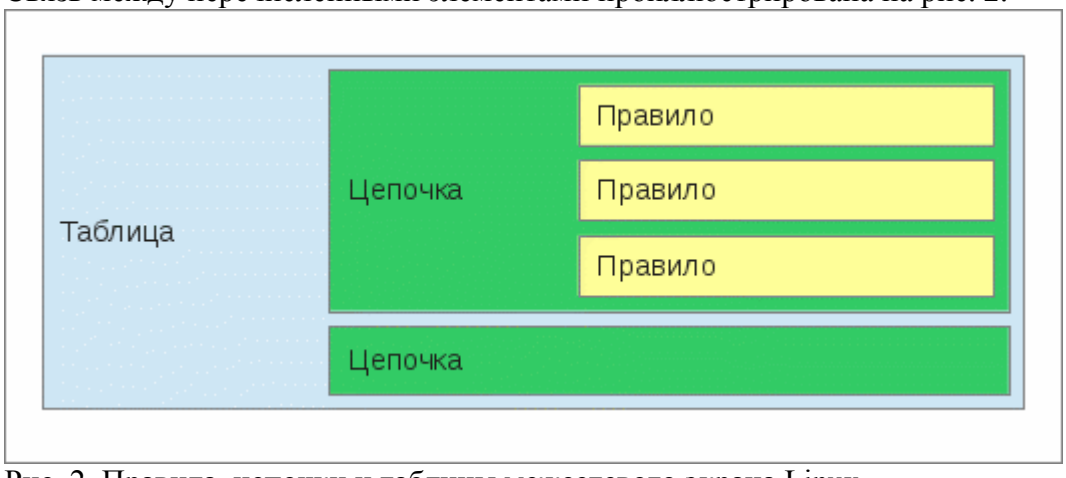


Рис. 2. Правила, цепочки и таблицы межсетевого экрана Linux.

Таблицы

В текущей версии межсетевого экрана (iptables v1.4.16.3) поддерживаются 4 встроенные таблицы.

Filter

Таблица filter содержит цепочки правил фильтрации пакетов. Пакеты могут пропускаться далее, либо отвергаться (действия ACCEPT и DROP соответственно), в зависимости от их содержимого. Эта таблица используется по умолчанию и представляет 3 цепочки:

- INPUT – правила фильтрации входящих пакетов.
- OUTPUT – фильтр исходящего трафика, сгенерированного локально.
- FORWARD – фильтрация маршрутизуемого транзитного трафика.

NAT

Таблица NAT используется для преобразования сетевых адресов (Network Address Translation). Через эту таблицу проходит только первый пакет из потока. Преобразования адресов автоматически применяется ко всем последующим пакетам.

- PREROUTING – Модификация пакета *перед* маршрутизацией, выполняемая сразу после того, как он попадает в систему. Обычно используется для DNAT (destination NAT, преобразование адреса получателя).
- POSTROUTING – Правила, применяемые *после* маршрутизации. Модификация пакетов выполняется перед выходом их из системы и, как правило, используется для изменения (сокрытия) источника, т.н. source NAT (SNAT).
- OUTPUT – Правила трансляции адресов у пакетов, сгенерированных локальными процессами.

Mangle

Raw

Использование iptables

Основным средством настройки брандмауэра Linux является консольная утилита *iptables*. Эта программа позволяет управлять набором правил пакетного фильтра и трансляцией адресов протокола IPv4. Для протокола IPv6 используется утилита ip6tables. Далее будут кратко рассмотрена настройка файрвола на примере iptables (подробности — в man iptables и на сайте проекта netfilter.org).

Для получения краткой справки по использованию утилиты можно вызвать ее с параметром --help:

```
aag@aag:~> /usr/sbin/iptables --help
iptables v1.4.16.3
```

Контрольные вопросы

1. Что такое межсетевой экран?
2. Каковы типовые действия фильтра над пакетами?
3. Какие цепочки правил имеются по умолчанию?
4. Основной синтаксис утилиты iptables

Лабораторная работа
Анализ пакетного трафика

Цель работы: знакомство с принципами работы программы анализа пакетного трафика Wireshark; практическое освоение приемов работы сбора и анализа трафика с помощью утилиты Wireshark.

Ход работы

1. **Запустите программу Wireshark.**

2. Выполните команду меню *Capture* -> *Options*. В открывшемся диалоговом окне устанавливаются следующие параметры захвата кадров (рис. 2.1):

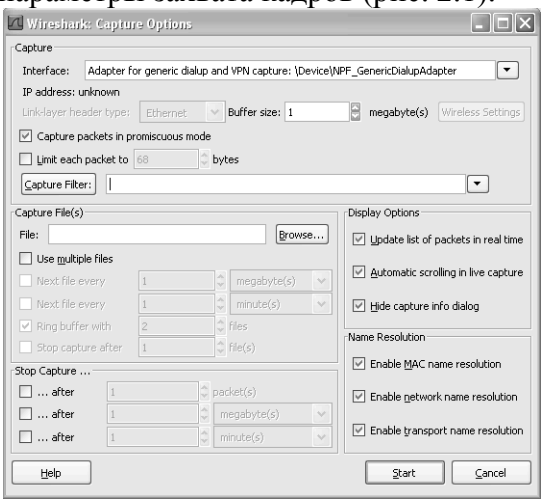


Рис. 2.1. Окно настройки параметров захвата

− Interface — сетевой адаптер;

Очень важно выбрать соответствующий сетевой адаптер, иначе запись кадров будет производиться из другого сегмента сети. В компьютере, имеющем всего один сетевой адаптер, среди возможных сетевых интерфейсов часто присутствует контроллер удаленного доступа.

− Buffer size — размер буфера захвата (по умолчанию 1 Мб);

При малом размере буфера существует опасность того, что при его заполнении запись новых кадров будет производиться поверх записанных ранее.

− Capture packets in promiscuous mode — использование режима беспорядочного захвата.

− Limit each packet to — запись только нескольких первых байт (определяется установленным значением параметра) каждого кадра;

− Capture Filter — фильтр захвата;

Фильтр захвата экономит объем буфера, отбрасывая «лишний мусор», однако увеличивает нагрузку на процессор, вследствие чего некоторые кадры могут быть потеряны. Поэтому в некоторых случаях вместо фильтра записи предпочтительнее использовать фильтр отображения кадров в буфере, а запись производить без фильтрации.

− Capture File(s) — файл захвата;

Опция полезна при осуществлении захвата трафика в течение длительного периода времени.

− Stop Capture — условия автоматического завершения захвата;

− Display Options — отображение пакетов в реальном времени и автоматический скроллинг окна информации;

Опции увеличивают нагрузку на процессор, вследствие чего некоторые кадры могут быть потеряны.

− Name Resolution — разрешение имен на физическом, сетевом и транспортном уровнях.

3. Уберите маркер напротив опции «Capture packets in promiscuous mode» для захвата только «своих» кадров (кадры с широковещательным адресом также будут захватываться). В таком режиме работы число захваченных пакетов будет существенно меньше, что облегчит выполнение заданий.

4. В командной строке сеанса MS-DOS для очистки кэша протокола ARP выполните команду arp -d. В Wireshark для запуска процесса захвата нажмите кнопку «Capture». В командной строке выполните команду ping <имя_сервера> (в качестве

параметра команды можно использовать IP-адрес сервера). По завершении команды Ping остановите захват, нажав кнопку «Stop».

На экране монитора в программе Wireshark вы увидите несколько панелей с отображением сетевых пакетов, только что записанных в буфер. Общий вид окна приложения представлен на рисунке 2.2.

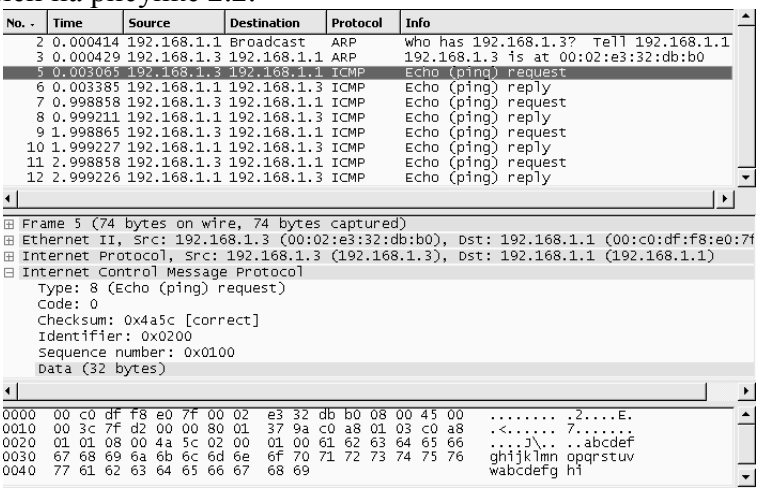


Рис. 2.2. Общий вид приложения Wireshark

Пользовательский интерфейс программы содержит следующие компоненты:

− меню команд и панель инструментов;

− фильтр отображения пакетов;

− список пакетов в буфере;

− панель отображения декодера протоколов;

− панель отображения пакета в шестнадцатеричном коде и символах ASCII.

Панель со списком пакетов построчно отображает характеристики того или иного пакета (номер по порядку в буфере, время захвата, адреса источника и получателя, тип протокола и общая информация о нем). Перемещение по списку осуществляется с помощью мыши или клавиатуры, причем информация на двух других панелях обновляется автоматически. На панели декодера протоколов, нажимая указателем мыши на символы «+» или «–», можно отображать информацию о полях заголовков протоколов с требуемым уровнем детализации. При выборе того или иного служебного поля в заголовке оно автоматически выделяется на нижней панели, где отображается текущий пакет в шестнадцатеричном виде.

С помощью фильтра отображения можно быстро убрать «мусор». Выражение фильтрации может представлять собой просто название протокола, который присутствует в пакете на том или ином уровне вложенности. Например: arp — для отображения пакетов протокола ARP, tcp — для отображения пакетов, в которых присутствует заголовок протокола TCP.

5. Для отображения только ICMP-сообщений в строке ввода «Filter» наберите «icmp» и нажмите кнопку «Apply».

Более сложные выражения фильтрации строятся с помощью зарезервированных слов, обычно представляющих собой названия полей заголовков того или иного протокола, знака операции сравнения и конкретного значения в шестнадцатеричном или десятичном виде.

Например, выражение с операцией сравнения «Равно» записывается с помощью двойного знака равенства «==» (допустимо использование «eq»). Другие операции сравнения записываются с помощью следующих операторов:

a. != (ne)— не равно, пример: eth.type != 0x0800;

b. > (gt)— больше, пример: tcp.srcport > 1023;

c. < (lt)— меньше, пример: frame.pkt_len lt 60;

d. >= (ge)— больше или равно, пример: frame.pkt_len ge 60;

e. <= (le)— меньше или равно, пример: tcp.dstport <=1023.

6. Выясните, что будет отображено в буфере захвата в случае использования фильтра, описанного с помощью выражений, приведенных в качестве вышеописанных примеров.

Значение любого выражения фильтрации возвращает переменную булевского типа. Таким образом, выражение udp означает присутствие в кадре заголовка протокола UDP, по аналогии с этим выражение tcp.flags.syn означает присутствие в заголовке протокола TCP бита синхронизации сессии в установленном состоянии (значение 1). К любому из выражений можно применить операцию логического отрицания, заключив его в скобки и поставив перед ним знак отрицания «NOT» или «!». Например, выражение !(ip.addr == 10.0.0.1) означает, что из буфера отображения необходимо убрать все пакеты, в которых встречается IP-адрес 10.0.0.1.

7. Объясните разницу между результатами использования выражений фильтрации !(ip.addr == X.X.X.X) и ip.addr != X.X.X.X. Для выполнения упражнения в выражениях фильтрации используйте вместо адреса X.X.X.X реальный IP-адрес вашего узла. В качестве выражений фильтрации можно использовать и составные выражения, которые образуются с помощью следующих логических операторов:

a. && (AND) — логическое «И», пример: (ip.dst==10.0.0.1) AND tcp.flags.syn;

b. || (OR) — логическое «ИЛИ», пример: (ip.addr==10.0.0.1) OR (ip.addr==10.0.0.2).

Другой удобный способ ввода выражения фильтрации состоит в следующем. На панели декодера протоколов отображается требуемое поле, в контекстном меню выбирается пункт «Apply as Filter» и далее исполняется либо команда «Selected», либо «Not Selected» в зависимости от задачи фильтрации (рис. 2.3).

8. Отобразите только ICMP-запросы (используйте поле «тип» в заголовке ICMP). Укажите результирующее выражение фильтрации с необходимыми пояснениями. После просмотра результата для отображения пакетов без фильтрации нажмите кнопку «Clear» в строке фильтра.

При необходимости создания сложного выражения фильтрации в меню «Apply as Filter» (рис.2.3) выбирайте команды, начинающиеся с многоточия, при этом новое выражение будет добавлено к результирующему выражению фильтрации.

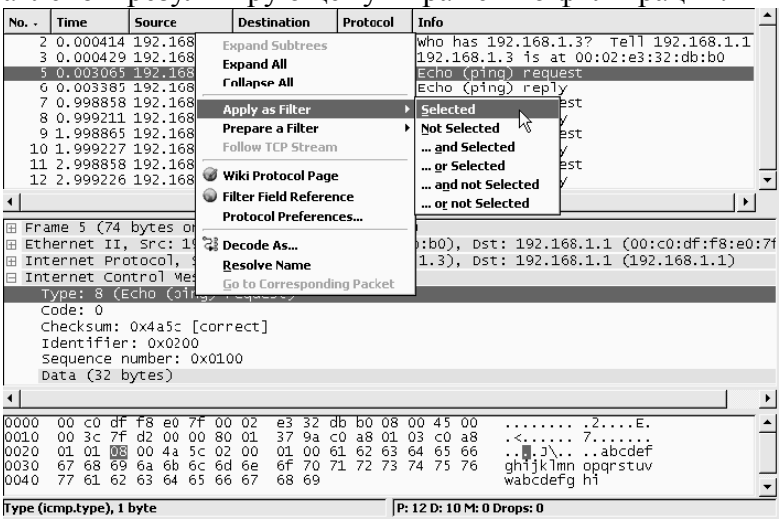


Рис. 2.3. Контекстное меню создания фильтра

9. Отобразите все кадры, переданные вашим узлом, исключая сообщения ICMP.

При создании выражения фильтрации имейте в виду, что в буфере могут находиться кадры других узлов.

Укажите результирующее выражение фильтрации с необходимыми пояснениями. После просмотра результата для отображения пакетов без фильтрации нажмите кнопку

«Clear» в строке фильтра.

В выражениях фильтрации первый операнд операции сравнения допускает использование указателя диапазона, если второй операнд представляет собой массив байт или строку символов. Указатель диапазона определяется с помощью квадратных скобок и может быть использован как применительно к кадру в целом (frame), так и с любым полем заголовка. Указатель диапазона допускает следующий синтаксис:

a. [i:j] начальное смещение i, длина j;

b. [i-j] начальное смещение i, конечное смещение j, включительно;

c. [i] начальное смещение i, длина 1;

d. [:j] начальное смещение 0, длина j;

e. [i:] начальное смещение i, до конца поля.

Например, записи frame[6:3] и eth.src[:3] идентичны и могут быть использованы для указания на код фирмы-производителя сетевого адаптера, передавшего кадр. Начальное смещение может иметь отрицательное значение, в этом случае оно отсчитывается от конца поля, причем последний байт поля имеет смещение, равное –1, предпоследний –2 и так далее. Например, выражение frame[-5:] == "hello" определяет кадр, оканчивающийся строкой «hello».

Строка, как видно из предыдущего примера, записывается в кавычках. Запись массива байт осуществляется побайтно в шестнадцатеричном виде с разделителем «.» или «:», например 00.45.f5.2d.

Используя символ «,» в указателе диапазона, можно перечислить несколько непересекающихся диапазонов, объединив их в одном операнде. Например, выражение tcp[2,10,13-16] == 00.01.c0.f8.01.66 сравнивает в заголовке протокола TCP поле «Тип обслуживания» с «0x00», поле «Протокол» с «0x01» и поле «IP-адрес источника» с «0xc0f80166».

10. Отобразите ICMP-ответы, используя в выражении фильтрации операнд «frame» с указателем диапазона.

При создании выражения фильтрации имейте в виду, что в буфере могут находиться кадры других узлов.

Укажите результирующее выражение фильтрации с необходимыми пояснениями. После просмотра результата для отображения пакетов без фильтрации нажмите кнопку «Clear» в строке фильтра.

Быстро вернуться к тому или иному ранее вводимому выражению фильтрации можно с помощью списка истории ввода, доступ к которому осуществляется нажатием на кнопку с символом «▼», расположенную в строке фильтра (не забывайте нажимать кнопку «Apply» для применения того или иного фильтра к буферу кадров).

Поиск кадров в буфере, удовлетворяющих тем или иным критериям, осуществляется с помощью команды меню ***Edit -> Find Packet***. Диалоговое окно определения критериев поиска пакетов изображено на рис.2.4.

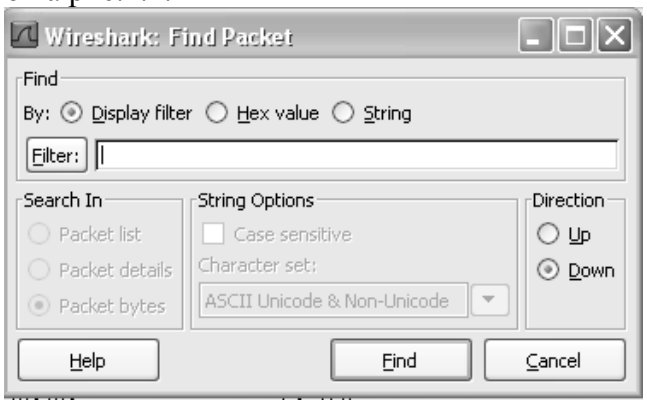


Рис.2.4. Диалоговое окно определения критериев поиска кадров

Критерии поиска можно определять в виде выражения фильтрации (Display filter), шаблона в шестнадцатеричном виде (Hex value) и текстовой строки (String) в кодировке

ASCII и (или) Unicode. В первом случае можно использовать все допустимые выражения фильтрации и их логические комбинации. Во втором случае указывается шаблон для поиска в шестнадцатеричном коде. Поиск в строке может осуществляться в области общей информации о пакете (Packet list), в панели декодера протоколов (Packet details) и непосредственно в самом пакете (Packet bytes). Поиск может производиться вверх или вниз по списку пакетов (Direction).

Команды меню **Edit -> Find Next** и **Edit -> Find** Previous используются для поиска с заданными критериями следующего или предыдущего пакета соответственно.

11. Найдите все пакеты с помощью выражения фильтрации «icmp.type==0».

12. Найдите все пакеты по строке «reply» в области общей информации о пакете.

13. Найдите все пакеты по строке «reply» в панели декодера протоколов.

14. Проанализируйте результаты при разных вариантах поиска и дайте им объяснение.

В списке буфера ключевые или наиболее важные для дальнейшего анализа пакеты можно помечать с помощью команды Edit -> Mark Packet (toggle) основного меню или команды Mark Packet (toggle) контекстного меню. Эта возможность полезна при дальнейшем поиске таких пакетов в большом буфере, так как они выделяются другим цветом, а также при сохранении, экспортировании и печати пакетов.

Информация о маркированных пакетах нигде не сохраняется, поэтому все маркеры будут потеряны при выгрузке файла данных.

15. Пометьте первый и последний пакеты, относящиеся к функционированию команды Ping.

Сохранение данных в файле производится из меню File -> Save или File -> Save As. Диалоговое окно сохранения данных изображено на рис.2.5.

Обратите внимание, что сохранить можно все пакеты (All packets), только отображаемые (Displayed), выбранный пакет (Selected packet only), ранее маркированные с помощью основного или контекстного меню (Marked packet only и From first to last marked packet) или указанный диапазон пакетов (Specify a packet range). По умолчанию Wireshark сохраняет данные в файле типа Libpcap, совместимом по формату с файлами программы TcpDump, но путем указания определенного формата в строке ввода «File Type» этого диалогового окна данные захвата можно сохранять для экспорта в другие программы анализа трафика (около двадцати поддерживаемых в настоящее время форматов).

Не забывайте сохранять данные, прежде чем начинать другой сеанс записи.

16. Сохраните все захваченные кадры в файле с именем «arp-ping» в каталоге, предлагаемом программой по умолчанию.

17. Сохраните в файле с именем «ping» только трафик команды Ping.

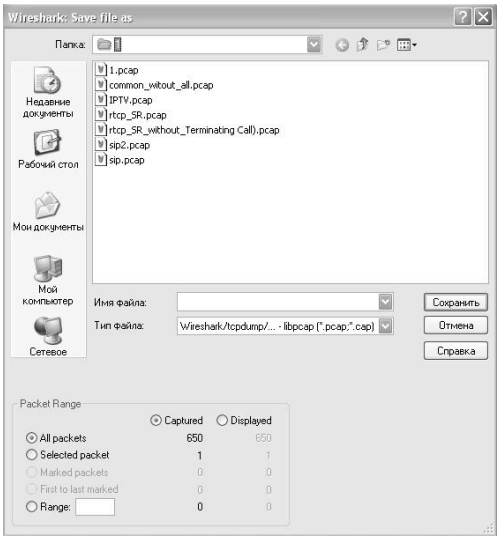


Рис.2.5. Диалоговое окно сохранения данных

Распечатка информации о том или ином пакете или их множестве осуществляется посредством выполнения команды Print основного или контекстного меню. Диалоговое окно печати данных изображено на рис.2.6.

При печати есть возможность осуществить вывод в указанный файл (Output to file) в виде простого текста (Plain text), определив диапазон распечатываемых пакетов (Packet Range) и формат вывода информации (Packet Format). Опции панели «Packet Range» полностью идентичны опциям соответствующей панели диалогового окна сохранения данных. При определении формата вывода в панели «Packet Format» есть возможность включить общую характеристику пакета (информацию верхней панели основного окна — «Packet summary line»), информацию, отображаемую на панели декодера протоколов с той или иной степенью детализации (Packet details) и собственно сам пакет в шестнадцатеричном виде (Packet bytes).

18. Выберите указателем мыши в списке пакетов первый ICMP-запрос и сохраните в файле «1.txt» информацию о нем с максимально возможной детализацией всех заголовков в декодере протоколов.

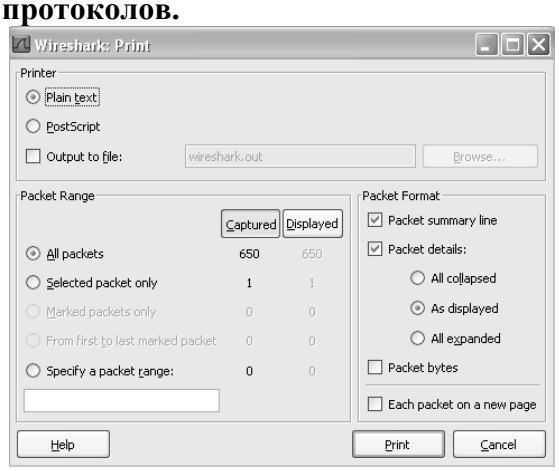


Рис. 2.6. Диалоговое окно печати данных

При составлении отчетов с использованием «скриншотов», а иногда и при анализе данных для просмотра двух пакетов одновременно удобно использовать возможность отображения пакета в отдельном окне.

Это реализуется с помощью команды «Show Packet in New Window» контекстного или основного меню программы «View». Окна, отображающие различные пакеты, показаны на рис. 2.7.

19. Пользуясь информацией об изображенных на рис. 2.7 пакетах, приведите обоснованные доводы, доказывающие их взаимосвязь.

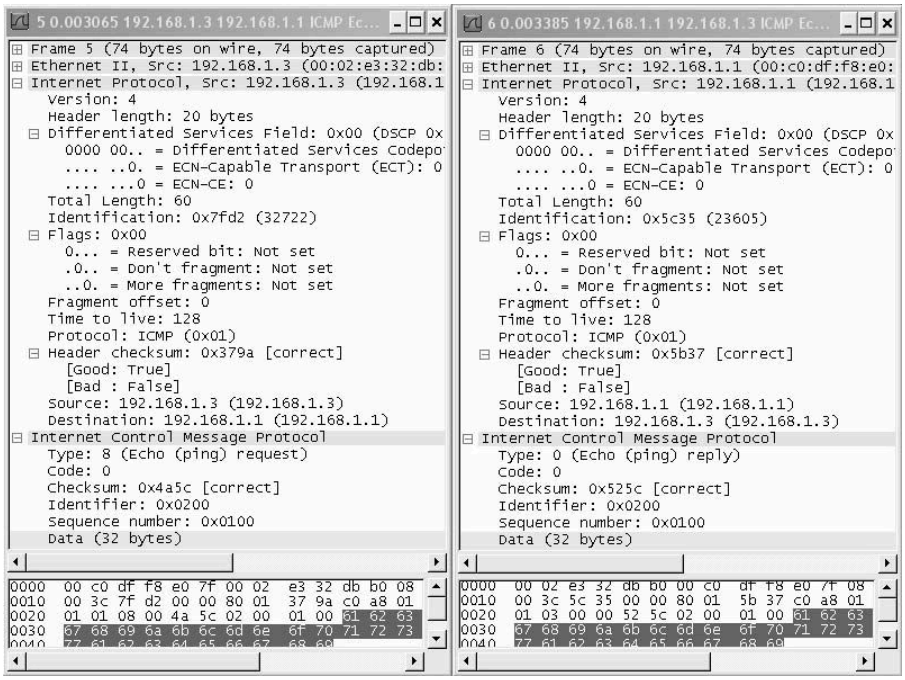


Рис.2.7. Отображение пакетов в отдельных окнах

20. Сохраните все захваченные пакеты в файле lab1.pcap.

В отчете по первой части работы привести

1. схему рабочего места с проставленными IP-адресами всех задействованных интерфейсов устройств,
2. результат выполнения пункта 5,
3. результат выполнения пункта 6,
4. выражение фильтрации из пункта 8 и пакеты, оставшиеся после применения выражения фильтрации,
5. выражение фильтрации из пункта 9 и пакеты, оставшиеся после применения выражения фильтрации,
6. выражение фильтрации из пункта 10 и пакеты, оставшиеся после применения выражения фильтрации,
7. вид окна для пункта 11,
8. результаты при разных вариантах поиска и объяснения из пункта 14,
9. взаимосвязь пакетов из пункта 19,
10. выводы.

Лабораторная работа
Анализ протоколов IP и ICMP

Цель работы: анализ протоколов IP и ICMP.

Ход работы

1. Для дальнейшей работы используйте файл lab1.pcap.

2. Переключитесь в текстовый редактор и выделите различными цветами поля заголовка IP в шестнадцатеричном представлении пакета. Опишите назначение этих полей.

3. Загрузите созданный вами файл «ping». Сохраните два кадра «запрос — ответ» с требуемой детализацией для анализа полей ICMP и опишите назначение этих полей.

4. Захватите сетевой трафик вашего узла при трассировке маршрута к поисковой системе Google (команда TraceRt) и ответьте на следующие вопросы:

a. Почему MAC-адреса назначения и источника у всех кадров одинаковы и чьи это адреса?

b. Почему узлы присылают ICMP сообщение «type 11»?

c. Почему различные узлы присылают ICMP сообщение «type 11» на запрос к одному и тому же узлу?

d. Сколько таких узлов, какие у них IP-адреса?

e. Какова структура ICMP сообщения «type 11»?

f. Какие поля ICMP одинаковы, а какие различны в последних трех запросах?

5. С помощью фильтра отобразите только ICMP-запросы. Приведите выражение фильтрации и объясните, почему выражения icmp.type == 8 и ip.src == X.X.X.X (где X.X.X.X — IP-адрес вашего узла) не приводят к желаемому результату.

6. Ответьте на следующие вопросы:

a. Каковы размеры кадров Ethernet, заголовков IP и сообщений ICMP, меняются ли они в процессе выполнения команды?

b. Фрагментируются ли IP-дейтаграммы, передаваемые узлом?

c. Какие поля заголовка IP меняются, а какие остаются неизменными в каждом пакете трафика?

d. Какое поле заголовка IP изменяется в каждой тройке передаваемых кадров, и для каких целей оно служит?

e. Каким образом можно быстро определить число промежуточных маршрутизаторов на маршруте, если известно, что последний запрос, находящийся в буфере, достиг целевого узла?

7. С помощью фильтра отобразите только ICMP-сообщения, получаемые вашим узлом, и ответьте на следующие вопросы:

a. Меняются ли в процессе выполнения команды размеры заголовков IP и сообщений ICMP? Чем можно объяснить данную ситуацию?

b. Имеются ли в буфере кадры, которые нельзя фрагментировать, и от какого узла они получены?

8. Захватите сетевой трафик функционирования команды Ping при проверке доступности сервера Google с параметром «r», равным 5. Сохраните данные в файле с именем «ping-r5». Ответьте на следующие вопросы:

a. Поясните назначение параметра -r в команде Ping.

b. Каким образом в кадрах передается информация о маршруте?

c. Почему значение параметра -r в команде Ping не может быть больше 9?

d. Каким образом ведут себя значения полей идентификатора и последовательного номера в заголовке ICMP захваченных кадров?

9. Захватите сетевой трафик функционирования команды Ping при проверке доступности сетевого узла вашего компьютерного класса с параметром «s», равным 4. Сохраните данные в файле с именем «ping-s4». Ответьте на следующие вопросы:

a. Поясните назначение параметра -s в команде Ping.

b. Каким образом в кадрах передается штамп времени?

c. Почему значение параметра -s в команде Ping не может быть больше 4?

10. Захватите сетевой трафик функционирования команды Ping при проверке доступности сетевого узла вашего компьютерного класса с параметром «l», равным

3500, и «n», равным 1. Сохраните данные в файле с именем «ping3500». Ответьте на следующие вопросы:

a. Сколько кадров передано и получено вашим узлом?

b. Сколько IP-дейтаграмм передано и получено вашим узлом?

c. Были ли IP-дейтаграммы подвергнуты фрагментации, какие поля заголовка IP указывают на это?

d. Сколько фрагментов IP-дейтаграмм оказалось в буфере захвата?

e. Какой размер исходной дейтаграммы, подвергнувшейся дефрагментации?

f. Какие размеры разных фрагментов одной и той же дейтаграммы?

g. Меняется ли идентификатор дейтаграммы в ее фрагментах, каково его значение?

h. Какие поля заголовка IP предназначены для сборки исходной дейтаграммы из фрагментов в правильной последовательности?

i. В каких фрагментах исходных дейтаграмм присутствует заголовок ICMP?

j. Проанализируйте результаты и приведите схему обмена сообщениями ICMP между узлами.

11. С указанием значений всех необходимых полей заголовков покажите взаимосвязь кадров в рамках обмена «запрос — ответ» протокола ICMP.

В отчете привести:

1. схему рабочего места с проставленными IP-адресами всех задействованных интерфейсов устройств,

2. приведите заголовок IP одного из пакетов в шестнадцатеричном представлении, выделив каждое поле, опишите назначение полей,

3. вид окон с пакетами запроса и ответа протокола ICMP, как на рис. 2.7 и опишите назначение полей,

4. ответы на вопросы пункта 4,

5. выражение фильтрации из пункта 5,

6. ответы на вопросы пункта 6,

7. выражение для фильтра отображения пункта 7 и ответы на вопросы,

8. ответы на вопросы пункта 8, 9, 10,

9. результат выполнения пункта 11,

10. выводы.

Лабораторная работа
Анализ протокола TCP

Цель работы: анализ протокола TCP; получение навыков выработки правил фильтрации на основе анализа заголовков пакетов протокола TCP; освоение возможностей программы Wireshark

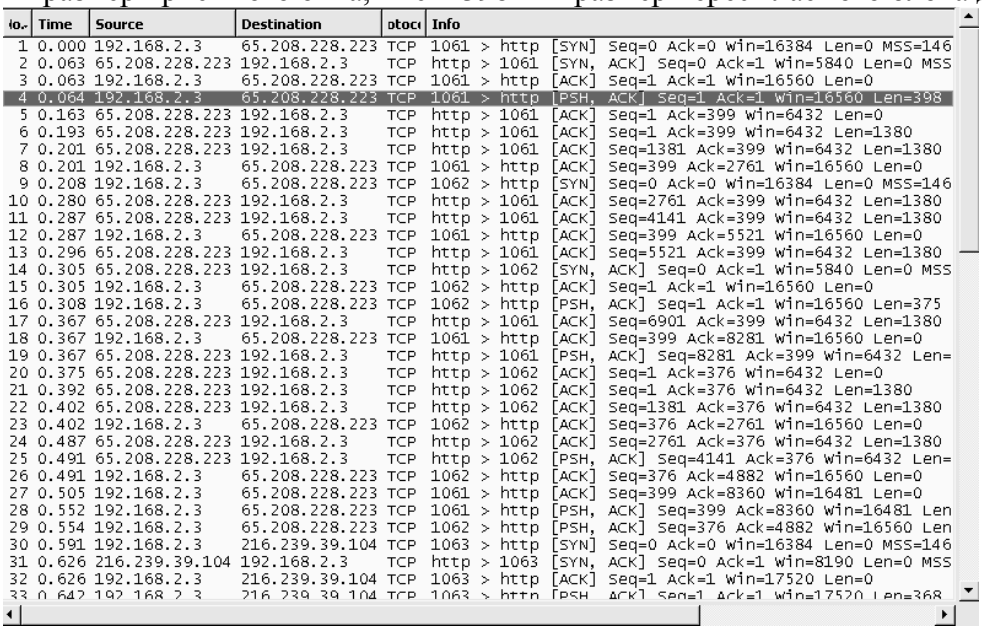
Ходя работы

1. Захватите сетевой трафик при обращении к стартовой странице сервера www.wireshark.com. Для отображения в буфере кадров с протоколом TCP примените соответствующее выражение фильтрации.

В буфере захвата у вас находятся кадры, принадлежащие обмену клиента с сервером по протоколу HTTP, но в рамках текущего упражнения прикладной протокол нас не интересует, поэтому отключите анализ протокола HTTP. Фрагмент панелей со списком кадров после отключения анализа протокола FTP показан на рис. 2.9.

Обратите внимание, что теперь по каждому захваченному кадру приводится информация, касающаяся только протокола TCP. Например, для пакета № 4 (рис. 1.9) запись

«1061> ftp» означает порты источника и назначения, «[PSH, ACK]» — установленные биты флагов, «Seq=1» — последовательный номер, «Ack=1» — номер подтверждения, «Win=16560» — размер приемного окна, «Len=398» — размер пересылаемого блока данных.



No.	Time	Source	Destination	Protocol	Info
1	0.000	192.168.2.3	65.208.228.223	TCP	1061 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=146
2	0.063	65.208.228.223	192.168.2.3	TCP	http > 1061 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
3	0.063	192.168.2.3	65.208.228.223	TCP	1061 > http [ACK] Seq=1 Ack=1 Win=16560 Len=0
4	0.064	192.168.2.3	65.208.228.223	TCP	1061 > http [PSH, ACK] Seq=1 Ack=1 Win=16560 Len=398
5	0.163	65.208.228.223	192.168.2.3	TCP	http > 1061 [ACK] Seq=1 Ack=399 Win=6432 Len=0
6	0.193	65.208.228.223	192.168.2.3	TCP	http > 1061 [ACK] Seq=1 Ack=399 Win=6432 Len=1380
7	0.201	65.208.228.223	192.168.2.3	TCP	http > 1061 [ACK] Seq=1381 Ack=399 Win=6432 Len=1380
8	0.201	192.168.2.3	65.208.228.223	TCP	1061 > http [ACK] Seq=399 Ack=2761 Win=16560 Len=0
9	0.208	192.168.2.3	65.208.228.223	TCP	1062 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=146
10	0.280	65.208.228.223	192.168.2.3	TCP	http > 1061 [ACK] Seq=2761 Ack=399 Win=6432 Len=1380
11	0.287	65.208.228.223	192.168.2.3	TCP	http > 1061 [ACK] Seq=4141 Ack=399 Win=6432 Len=1380
12	0.287	192.168.2.3	65.208.228.223	TCP	1061 > http [ACK] Seq=399 Ack=5521 Win=16560 Len=0
13	0.296	65.208.228.223	192.168.2.3	TCP	http > 1061 [ACK] Seq=5521 Ack=399 Win=6432 Len=1380
14	0.305	65.208.228.223	192.168.2.3	TCP	http > 1062 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
15	0.305	192.168.2.3	65.208.228.223	TCP	1062 > http [ACK] Seq=1 Ack=1 Win=16560 Len=0
16	0.308	192.168.2.3	65.208.228.223	TCP	1062 > http [PSH, ACK] Seq=1 Ack=1 Win=16560 Len=375
17	0.367	65.208.228.223	192.168.2.3	TCP	http > 1061 [ACK] Seq=6901 Ack=399 Win=6432 Len=1380
18	0.367	192.168.2.3	65.208.228.223	TCP	1061 > http [ACK] Seq=399 Ack=8281 Win=16560 Len=0
19	0.367	65.208.228.223	192.168.2.3	TCP	http > 1061 [PSH, ACK] Seq=8281 Ack=399 Win=6432 Len=
20	0.375	65.208.228.223	192.168.2.3	TCP	http > 1062 [ACK] Seq=1 Ack=376 Win=6432 Len=0
21	0.392	65.208.228.223	192.168.2.3	TCP	http > 1062 [ACK] Seq=1 Ack=376 Win=6432 Len=1380
22	0.402	65.208.228.223	192.168.2.3	TCP	http > 1062 [ACK] Seq=1381 Ack=376 Win=6432 Len=1380
23	0.402	192.168.2.3	65.208.228.223	TCP	1062 > http [ACK] Seq=376 Ack=2761 Win=16560 Len=0
24	0.487	65.208.228.223	192.168.2.3	TCP	http > 1062 [ACK] Seq=2761 Ack=376 Win=6432 Len=1380
25	0.491	65.208.228.223	192.168.2.3	TCP	http > 1062 [PSH, ACK] Seq=4141 Ack=376 Win=6432 Len=
26	0.491	192.168.2.3	65.208.228.223	TCP	1062 > http [ACK] Seq=376 Ack=4882 Win=16560 Len=0
27	0.505	192.168.2.3	65.208.228.223	TCP	1061 > http [ACK] Seq=399 Ack=8360 Win=16481 Len=0
28	0.552	192.168.2.3	65.208.228.223	TCP	1061 > http [PSH, ACK] Seq=399 Ack=8360 Win=16481 Len
29	0.554	192.168.2.3	65.208.228.223	TCP	1062 > http [PSH, ACK] Seq=376 Ack=4882 Win=16560 Len
30	0.591	192.168.2.3	216.239.39.104	TCP	1063 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=146
31	0.626	216.239.39.104	192.168.2.3	TCP	http > 1063 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS
32	0.626	192.168.2.3	216.239.39.104	TCP	1063 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
33	0.642	192.168.2.3	216.239.39.104	TCP	1063 > http [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=368

Рис. 2.9. Отображение информации о протоколе TCP

Каждая TCP-сессия (причем при обращении к одной странице сессий может быть несколько!) начинается с обмена тремя TCP-сегментами с установленными битами SYN, SYN-ACK и ACK. На рис. 2.9 можно видеть открытие трех сессий TCP (кадры с номерами 1, 2, 3; 9, 14, 15; 30, 31, 32 соответственно).

2. Определите количество сеансов TCP в буфере захваченных пакетов.

На рис. 1.9 также видно, что сеансы TCP начинаются с относительных последовательных номеров, равных нулю. Для того чтобы отобразить реальные последовательные номера, выбранные узлами при взаимодействии, необходимо выполнить команду меню ***Edit -> Preferences***, в появившемся диалоговом окне (фрагмент диалогового окна см. на рис. 2.10) выбрать протокол TCP и убрать маркер в строке параметра «Relative sequence numbers and window scaling».

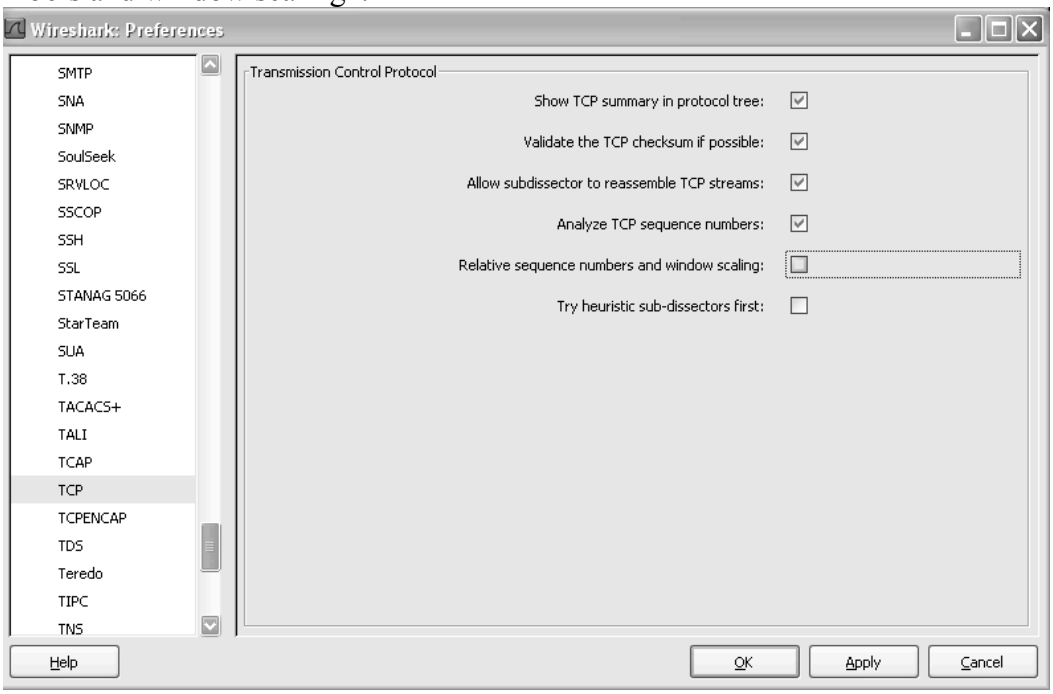


Рис. 2.10. Параметры анализа протокола TCP

3. Отобразите реальные последовательные номера в рамках сеансов TCP.

4. Проанализируйте третий кадр в рамках какого-либо сеанса TCP и ответьте на следующие вопросы:

a. Какие порты используются клиентом и сервером?

b. Какой начальный последовательный номер выбран клиентом?

c. Присутствует ли в этом кадре поле подтверждения, каково его значение?

d. Какая длина заголовка TCP, присутствуют ли данные в этом кадре?

e. Какой бит флагов установлен и для чего он служит?

f. Какие дополнительные опции TCP передаются клиентом в этом кадре?

g. Сохраните кадр и выделите различным цветом поля заголовка TCP, пояснив их назначение.

Немаловажная возможность программы Wireshark по анализу TCP трафика состоит в том, что с помощью команды меню ***Statistics -> Conversations*** можно быстро определить все сеансы, имеющиеся в буфере. В диалоговом окне для отображения сеансов TCP необходимо выбрать закладку TCP (рис. 2.11).

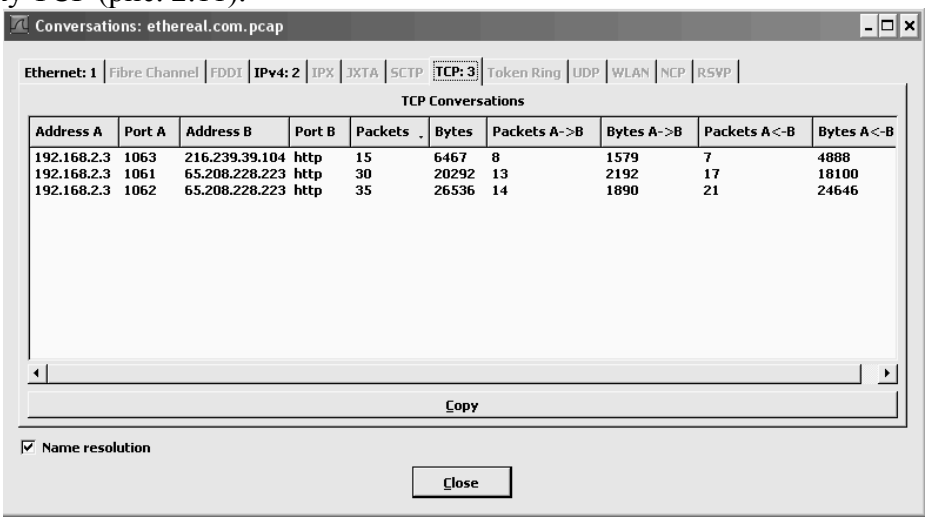


Рис. 2.11. Статистика по сеансам TCP

5. Отобразите статистику сеансов TCP.

6. Выберите первый сеанс и с помощью контекстного меню *Apply as Filter -> Selected -> A<—>B* отобразите в буфере кадры, принадлежащие этому сеансу.

Для того чтобы быстро просмотреть передаваемые данные в рамках того или иного сеанса, используют команду меню ***Analyze -> Follow TCP Stream***. После выполнения команды на экране появится диалоговое окно, в котором разными цветами будут отображены как запросы клиента, так и ответы сервера.

Кнопка «Entire conversation» с раскрывающимся списком позволяет отобразить обе стороны, участвующие в обмене, или только одну из них. Диалоговое окно позволяет отобразить данные в различных форматах (ASCII, EBCDIC, Hex Dump, C Arrays, Raw) и сохранить их в файл. При обнаружении в сеансе кадров с каким-либо файлом можно отобразить лишь поток соответствующего направления, выбрать необходимый формат и сохранить его на диск.

7. Определите, что передавалось в рамках захваченных вами сеансов TCP.

В отчете привести:

1. схему рабочего места с проставленными IP-адресами всех задействованных интерфейсов устройств,

2. анализ третьего кадра сеанса TCP и ответы на вопросы пункта 4,

3. окно статистики по TCP,

4. результат выполнения пункта 7,

5. выводы.

МДК 02.02. Организация администрирования компьютерных сетей

Лабораторная работа

Тема: Установка и настройка сетевой операционной системы: установка Windows Server 2003

Цель занятия: Получить навыки установки и первоначальной настройки серверной ОС семейства Windows

Продолжительность занятия: 4 часа.

Краткие теоретические и справочно-информационные материалы по теме занятия.

Операционная система (ОС) – это совокупность программных средств, осуществляющая управление ресурсами компьютера, запуск прикладных программ и их взаимодействие с внешними устройствами и другими программами, а также обеспечивающая диалог пользователя с ЭВМ. Ресурсом является любой компонент ЭВМ и предоставляемые им *возможности*: центральный процессор, оперативная и внешняя память, внешнее устройство, программа и т.д. ОС загружается в оперативную память при включении компьютера и предоставляет пользователю удобный способ общения (*интерфейс*) с вычислительной системой.

Назначение серверной операционной системы - это управление приложениями, обслуживающими всех пользователей корпоративной сети, а нередко и внешних пользователей. К таким приложениям относятся современные системы управления базами данных, средства управления сетями и анализа событий в сети, службы каталогов, средства обмена сообщениями и групповой работы, Web-серверы, почтовые серверы, корпоративные брандмауэры, серверы приложений самого разнообразного назначения, серверные части бизнес-приложений. Требования к производительности и надежности указанных операционных систем очень высоки; нередко сюда входят и поддержка кластеров (набора ряда однотипных компьютеров, выполняющих одну и ту же задачу и делящих между собой нагрузку), и возможности дублирования и резервирования, и переконфигурации программного и аппаратного обеспечения без перезагрузки операционной системы.

Выбор серверной операционной системы и аппаратной платформы для нее в первую очередь определяется тем, какие приложения под ее управлением должны выполняться (как минимум, выбранные приложения должны существовать в версии для данной платформы) и какие требования предъявляются к ее производительности, надежности и доступности.

Windows

Серверные версии операционной системы **Windows (*WindowsNT,Windows 2000, WindowsServer 2003*)** сегодня применяются довольно широко - благодаря удобству администрирования и невысокой совокупной стоимости владения.

WindowsNT

Первая полностью 32-разрядная операционная система этого семейства, появилась вскоре после выпуска **Windows 95**. Самой популярной стала версия**WindowsNTServer 4.0**, существовавшая в варианте не только для *Intel-совместимых компьютеров*, но идля *RISC-систем*. Данная операционная система обладала привычным пользовательским интерфейсом **Windows 95**, удобными средствами администрирования, встроенным Web-сервером, средствами диагностики сети, управления процессами и задачами, интеграции с другими операционными системами (например, с ***NovellNetWare***), а также утилитами и службами управления рабочими станциями. Чуть позже для этой операционной системы появились такие сервисы, как монитор транзакций и сервер приложений**MicrosoftTransactionServer**, сервер управления очередями сообщений **MicrosoftMessageQueueServer**, а также ряд коммерческих продуктов, в том числе

серверные СУБД, средства групповой работы и обмена сообщениями, серверы приложений как от компании **Microsoft**, так и от других производителей.

Windows 2000

На данный момент является самой популярной операционной системой **Microsoft**в корпоративном секторе. К серверным операционным системам этого семейства относятся **Windows 2000 Server**- универсальная сетевая операционная система для серверов рабочих групп и отделов, **Windows 2000 AdvancedServer**- операционная система для эксплуатации бизнес-приложений и приложений для электронной коммерции и**Windows 2000 DatacenterServer**- ОС для наиболее ответственных приложений, осуществляющих обработку данных. В состав **Windows 2000 Server**, по сравнению с **WindowsNT 4.0**, включены и дополнительные службы, облегчающие управление серверами, сетями и рабочими станциями, например, службы каталогов ***ActiveDirectory***, позволяющие создать единое хранилище учетных записей пользователей, клиентов, серверов и приложений**Windows**, дополнительные средства конфигурирования сетей и подключения удаленных пользователей, терминальные службы для удаленного управления компьютерами. Кроме того, в данную операционную систему были добавлены службы компонентов, являющиеся дальнейшим развитием ***MicrosoftTransactionServer***, что позволило создавать для этой ОС корпоративные приложения, обладающие масштабируемостью и надежностью.

WindowsServer 2003

Создание семейства **WindowsServer 2003** стало следующим шагом в развитии операционных систем **Windows 2000**. Основными особенностями данного семейства операционных систем являются наличие в их составе платформы **Microsoft .NETFramework**, а также поддержка **Web-сервисов XML**.**WindowsServer 2003** существует в четырех редакциях:

WindowsServer 2003 WebEdition- операционная система для развертывания и обслуживания *Web-приложений* и *Web-сервисов*, включая приложения**.ASP .NET**; ***WindowsServer 2003 StandardEdition***- сетевая операционная система для выполнения серверной части бизнес-решений и рассчитанная на применение в небольших компаниях и подразделениях. Здесь имеются средства совместного использования ресурсов и централизованного развертывания приложений для настольных компьютеров, а также реализована поддержка до 4 Гбайт оперативной памяти и симметричной многопроцессорной обработки с использованием двух процессоров; ***WindowsServer 2003 EnterpriseEdition***- ОС, которая прежде всего предназначена для средних и крупных компаний. Она поддерживает серверы на базе 64-разрядных процессоров (до восьми штук) и объем оперативной памяти до 64 Гбайт и выпускается в версиях для 32- и 64-разрядных платформ;

WindowsServer 2003 DatacenterEdition- операционная система, которая служит для создания критически важных технических решений с высокими требованиями к масштабируемости и доступности. К таким решениям относятся приложения для обработки транзакций в режиме реального времени, а также решения, основанные на интеграции нескольких серверных продуктов. В данной ОС реализована поддержка симметричной многопроцессорной обработки с использованием до 32 процессоров, а также имеются службы балансировки нагрузки и создания кластеров, состоящих из восьми узлов. Эта ОС доступна для 32- и 64-разрядных платформ.

Процесс установки серверной ОС семейства **Windows**практически ничем не отличается от установки других ОС указанного семейства, кроме необходимости указания в процессе установки количества одновременных подключений.

UNIX

Операционная система ***UNIX***относится к «долгожителям» рынка серверных операционных систем она была создана в конце 60-х годов в**Bell**

Laboratoriesфирмы **AT&T**. Отличительной особенностью этой ОС, обусловившей

ее
«живучесть» и популярность, было то, что ядро операционной системы, написанной на ассемблере, было невелико, тогда как вся оставшаяся часть операционной системы была написана на языке С. Такой подход делал легко переносимой на самые разнообразные аппаратные платформы и саму операционную систему, и созданные для нее приложения. Важным достоинством ***UNIX***стала ее открытость, позволившая одновременно существовать как коммерческим, так и некоммерческим версиям ***UNIX***.

Общими для всех версий ***UNIX***особенностями являются многопользовательский режим со средствами защиты данных от несанкционированного доступа, реализация мультипрограммной обработки в режиме разделения времени, использование механизмов виртуальной памяти и свопинга, унификация операций ввода-вывода, иерархическая файловая система, разнообразные средства взаимодействия процессов, в том числе межсетевого.

Solaris (SunMicrosystems)

Операционная система ***SunSolaris***сегодня входит в число самых известных коммерческих версий ***UNIX***. Эта ОС обладает развитыми средствами поддержки сетевого взаимодействия и представляет собой одну из самых популярных платформ для разработки корпоративных решений - для нее существует около 12 тыс. различных приложений, в том числе серверов приложений и СУБД почти от всех ведущих производителей. ***Solaris***соответствует многим промышленным стандартам и характеризуется высокой масштабируемостью. Для подавляющего большинства приложений эта операционная система обеспечивает практически линейный рост производительности при увеличении числа процессоров за счет симметричных многопроцессорных вычислений. В настоящее время Solaris поддерживает процессоры **SPARC**и **Intelx86**. Из *особенностей **Solaris 9*** следует отметить поддержку до 1 млн. одновременно работающих процессов, до 128 процессоров в одной системе и до 848 процессоров в кластере, до 576 Гбайт физической оперативной памяти, поддержку файловых систем размером до 252 Тбайт, наличие средств управления конфигурациями и изменениями, встроенную совместимость с ***Linux***. Операционная система ***Solaris 9*** представляет собой основу открытой сетевой среды **SunOpenNetEnvironment (SunONE)**. В комплект поставки ***Solaris 9*** входят ключевые приложения **Sun ONE:** *Application Server, Directory Server, Integration Server, Message Queue, Portal Server, Web Server*.

HP-UX (Hewlett-Packard)

Операционнаясистема***HP-UX***, разработаннаявкомпании**Hewlett-Packard**, являетсяпотомком**AT&T System V**. Еепоследняяверсия, **HP-UX 11i**, доступнадлядвухаппаратныхплатформ - **PA_RISC** и**Itanium** - иориентированаглавнымобразомнасерверыпроизводства**Hewlett-Packard**. Из *особенностей **HP-UX 11i***нужно назвать средства интеграции с ***Windows***и ***Linux***, в том числе средства переноса *Java- приложений*, разработанных для этих платформ, а также средства повышения производительности *Java- приложений*. Кроме того, ***HP-UX 11i***поддерживает ***LinuxAPI***, что гарантирует перенос приложений между ***HP-UX***и ***Linux***. Отметим, что приложения для ***HP-UX 11i***переносятся между двумя поддерживаемыми ею аппаратными платформами без изменений и перекомпиляции.

Говоря о производительности и масштабируемости ***HP-UX 11i***, следует отметить, что одна копия операционной системы поддерживает до 256 процессоров; поддерживаются также кластеры размером до 128 узлов. К тому же данная платформа поддерживает подключение и отключение дополнительных процессоров, замену аппаратного обеспечения, динамическую настройку и обновление операционной системы без необходимости перезагрузки, резервное копирование в режиме *on-line*и дефрагментацию дисков без выключения системы.

Выбор программного обеспечения для данной операционной системы весьма широк - это и серверы приложений ведущих производителей, и Web- и WAP-серверы, и поисковые

серверы, и средства кэширования, и службы каталогов.

Linux и FreeBSD

Операционная система ***Linux***- это некоммерческий продукт категории **OpenSource**для платформы **Intel**, который в течение десяти лет создавали тысячи энтузиастов. Список серверных продуктов для ***Linux***, пожалуй, не менее внушителен, чем для ***Solaris, HP-UX и AIX***, и включает такие популярные продукты, как **Web-сервер Apache**, серверные СУБД и серверы приложений практически от всех производителей.

Одним из серьезных преимуществ ***Linux***является низкая стоимость ее приобретения (хотя сама операционная система является некоммерческим продуктом, сертифицированные дистрибутивы ***Linux***- обычно продукты коммерческие). Кроме того, ряд компаний, в частности **IBM**, вкладывают значительные средства в развитие ***Linux***как серверной платформы, одновременно стремясь реализовать совместимость с ***Linux***в своих коммерческих версиях ***UNIX***в расчете на возможный переход с ***Linux***на указанные операционные системы.

NetWare (Novell)

В начале и середине 90-х годов ***NovellNetWare***была доминирующей сетевой операционной системой. Хотя в настоящее время снизилась доля серверов, управляемых***NetWare***, как и количество создаваемых для нее приложений и инфраструктурного программного обеспечения, эта операционная система по-прежнему популярна благодаря надежности, масштабируемости, способности управлять большим количеством рабочих станций.

Основными особенностями последней версии, данной операционной системы, ***NovellNetWare 6.5***, являются возможность создания географически распределенных кластеров, наличие средств поддержки мобильных и удаленных пользователей, инструментов управления удаленными сетевыми ресурсами, а также средств синхронизации информации о пользователях и приведения в соответствие между собой каталогов в смешанных средах. Защита данных в ***NovellNetWare 6.5*** осуществляется с помощью служб каталогов **NDSeDirectory**.

В состав ***NovellNetWare 6.5*** входят известные **OpenSource**-продукты, а именно: ***Web-сервер Apache, СУБД MySQL, сервер приложений ApacheTomcat***. Кроме того, в ***NetWare 6.5*** включены сертифицированный на соответствие спецификации **J2EE** сервер приложений и среда разработки **Novellextend**и так называемый виртуальный офис, позволяющий через Web-интерфейс обращаться к бизнес-ресурсам пользователя, включая файлы, электронную почту, средства календарного планирования.

MacOSX (Apple)

Операционная система ***MacOSX***, созданная компанией **Apple**совместно с рядом университетских ученых, основана на ***BSDUNIX***. В 1999 году версия***MacOSXServer***была выпущена в виде продукта **OpenSource**, что позволило разработчикам адаптировать***MacOSX***для конкретных заказчиков, а также привлечь их к дальнейшему развитию этой операционной системы.

MacOSXхарактеризуется наличием менеджера виртуальной памяти, возможностью полной изоляции приложений друг от друга, поддержкой многозадачности, сравни- мой с аналогичной поддержкой в **Windows**. В ***MacOSX***имеются эмулятор предыдущих версий ***MacOS***, средства редактирования графических изображений, встроенная поддержка **OpenGL**, почтовый клиент, средства управления паролями для доступа к Web- ресурсам. В целом ***MacOSX***представляется многообещающей серверной операционной системой, и для нее уже начали выпускаться серверные СУБД и иное инфраструктурное программное обеспечение, хотя корпоративные пользователи пока относятся к ней достаточно осторожно.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

Задание 1. Установите Windows 2003 server.

1. Создайте виртуальную машину VM-2 в ***VirtualBox***
2. Запустите приложение ВМ ***VirtualBox***и подключите к созданной ранее виртуальной машине **VM-2** образ установочного диска **Windows 2003 Server**.
3. Запустите ВМ и начните установку ОС.
4. Ознакомьтесь с информацией программы установки и нажмите ***Enter***.

Рисунок 1. Программа установки.

5. Ознакомьтесь с лицензионным соглашением и согласитесь с ним (клавиша**F8**).
6. Создайте раздел для ОС на всем жестком диске клавишей ***ENTER***.

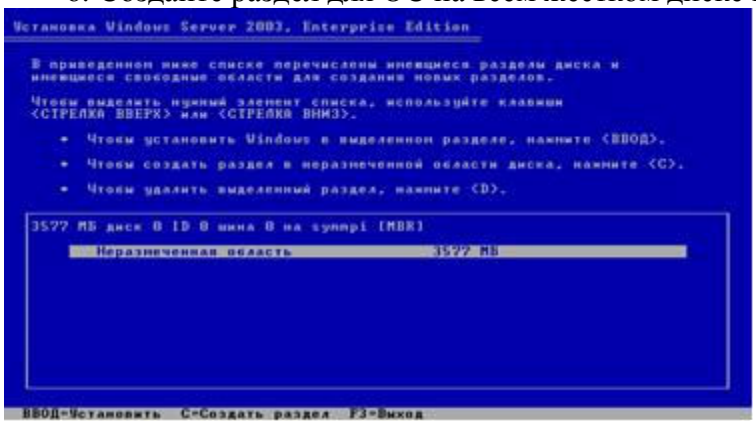


Рисунок 2. Создание раздела на жестком диске.

7. Выполните форматирование созданного раздела в файловой системе **NTFS**- нажмите***ENTER***.

Дождитесь окончания форматирования раздела, и копирования файлов установки на него. В процессе копирования компьютер перезагрузится и продолжит установку автоматически.

8. Самостоятельно укажите параметры языка и раскладки клавиатуры и перейдите к следующему шагу кнопкой ***Далее***.

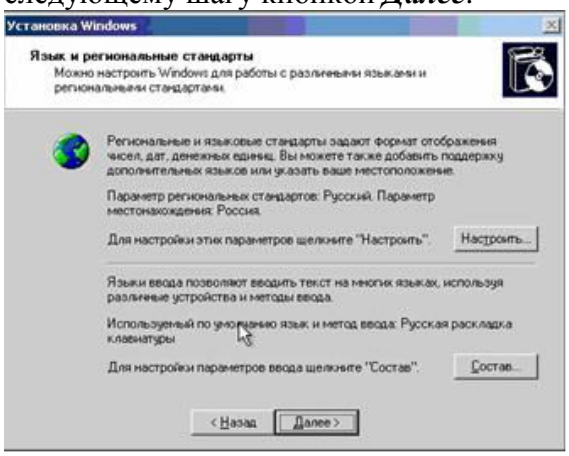


Рисунок 3. Язык и региональные стандарты.

9. Укажите регистрационные данные:
   - ведите в поле **Имя** – ***USER***
   - ведите в поле **Организация** – ***MSPU***
   - завершите ввод кнопкой ***Далее***.

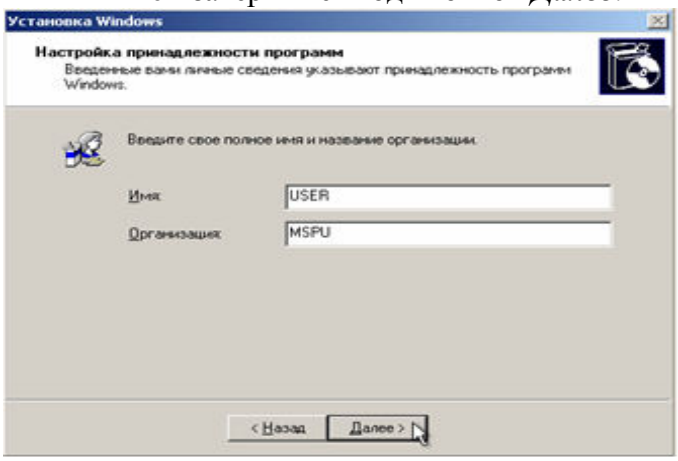


Рисунок 4. Имя пользователя и название организации

10. Введите в поле **Ключ продукта** лицензионный ключ и щелкните ***Далее***.

11. Укажите вариант лицензирования, при котором для каждого подключения требуется отдельная лицензия:
   - установите радиокнопку *На сервере*;
   - введите в текстовое поле количество одновременных подключений, например,***10***;
   - подтвердите параметры кнопкой ***Далее***.

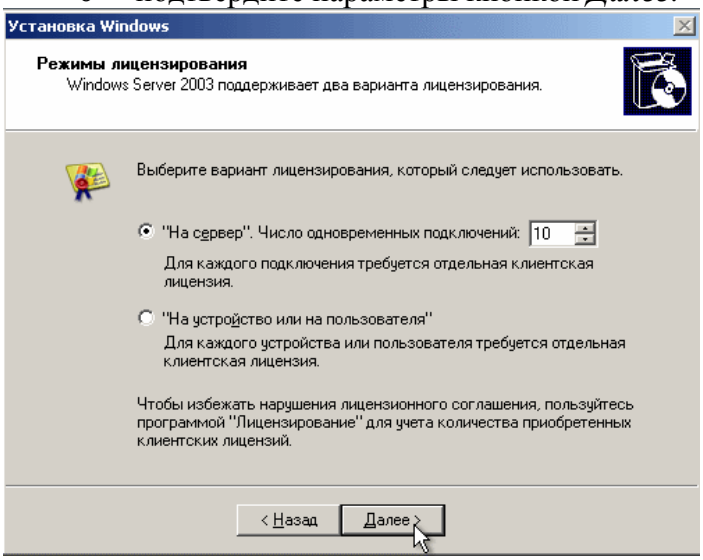


Рисунок 5. Вариант лицензирования.

12. Укажите имя компьютера и пароль администратора:
   - Введите в поле **Имя компьютера** – ***WIN2003***;
   - Введите в поле **Пароль администратора** – ***123456***;
   - Введите в поле **Подтверждение** - ***123456***.
   - Подтвердите сделанные изменения кнопкой ***Далее***. *Появится диалоговое окно, сообщающее о том, что пароль слишком простой.*
   - Ознакомьтесь с информацией о том, что вы указали простой пароль и продолжите установку кнопкой ***Да***.

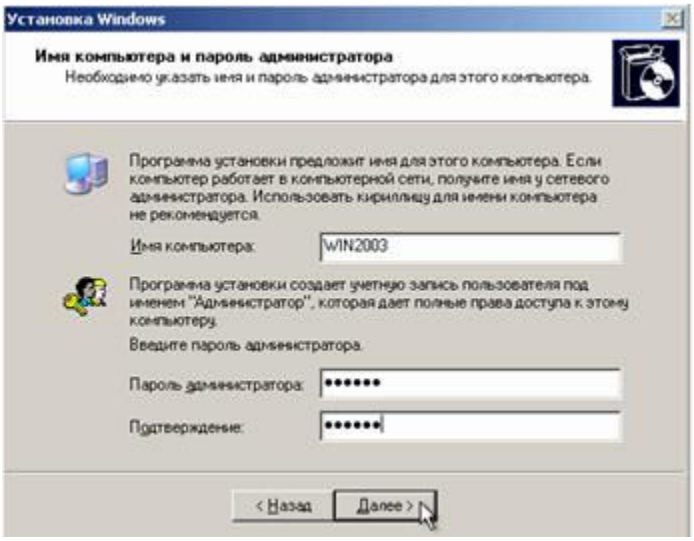


Рисунок 6. Имя компьютера и пароль администратора.

13. Укажите *дату и время* и щелкните ***Далее***.
14. Установите сетевые параметры для использования статического IP-адреса:
    - выберите радиокнопку *Обычные параметры* и щелкните ***Далее***;
15. Укажите сетевую группу, например,*Workgroup*и щелкните ***Далее***.
16. Дождитесь окончания выполнения установки ОС.

По окончании установки компьютер перезагрузится. После этого загрузится операционная система ***Windows 2003 Server***.

Задание 2. Выполните первоначальную настройку ОС:

1. Выполните вход в систему на сервере:
    - вызовите в ВМ событие *нажатие комбинации клавиш CTRL+ALT+DEL*, для этого нажмите **RCTRL+DEL**;
    - введите **пароль администратора** – *123456*;
    - подтвердите введенные данные кнопкой ***ОК***.
2. Ознакомьтесь с информацией диалогового окна **Послеустановочные обновления безопасности WindowsServer**(***Готово***).

После нажатия кнопки ***Готово****появится окно, предупреждающее о том, что после этого будет разрешено подключение по сети к вашему серверу.*

3. Подтвердите закрытие диалогового окна кнопкой ***Да***.
4. Ознакомьтесь с информацией в окне ***Управление данным сервером*** и закройте его.
5. Выполните настройку сетевого интерфейса:
    - откройте диалоговое окно **Состояние подключения по локальной сети (*Пуск/Панель управления/Сетевые подключения/Подключение по локальной сети*)**;
    - откройте диалоговое окно свойств подключения по локальной сети кнопкой***Свойства***;
    - откройте диалоговое окно **Параметры протокола Интернет TCP/IP**двойным щелчком;
    - включите использования статического адреса соответствующей радиокнопкой и укажите следующие данные:

IP-адрес – *192.168.1.2*;
Маска подсети – *192.168.255.255*;
Основной шлюз – *192.168.1.1*;

        - завершите ввод параметров кнопкой ***ОК***;
    - закройте диалоговое окно свойств подключения по локальной сети кнопкой ***ОК***;

- закройте диалоговое окно **Состояние подключения по локальной сети** кнопкой ***Закрыть***.

6. Установите дополнения гостевой ОС:
   - запустите **Мастер дополнений гостевой ОС** (***Устройства/Установить дополнение гостевой ОС***);
   - ознакомьтесь с информацией мастера и щелкните ***Next***;
   - ознакомьтесь с лицензионным соглашением и согласитесь с ним (***IacceptthetermsinLicenseAgreement/Next***)
   - подтвердите путь установки дополнений по умолчанию кнопкой ***Install***;
   - подтвердите установку графического адаптера **VirtualBoxGraphicAdapter**кнопкой ***Продолжить***;
   - разрешите ОС доверять устанавливаемому драйверу графического адаптера кнопкой ***ДА***;
   - завершите установку дополнений кнопкой ***Finish***.

После этого компьютер перезагрузиться

7. Самостоятельно установите в ВМ более высокое разрешение экрана, например,**1024x768**.
8. Остановите виртуальную машину.

Контрольные вопросы

1. Что такое контроллер домена?
2. Для чего предназначена служба DNS?
3. Почему у сервера DNS должен быть статический IP- адрес?
4. Для чего предназначен протокол DHCP?
5. Назовите необходимые действия и их порядок для добавления клиентской машины в домен.

Лабораторная работа

Тема: Установка и настройка сетевой операционной системы: установка и просмотр Active Directory. Подключение компьютера к домену

Цель занятия: Получить навыки установки и просмотра Active Directory; научится подключать компьютеры к домену

Продолжительность занятия: 4 часа

Краткиетеоретические и справочно-информационныематериалыпо темезанятия.

*ActiveDirectory*является**LDAP**(***LightweightDirectoryAccessProtocol***—«облегчѐнныйпротоколдоступаккаталогам»)-совместимойреализацией**службыкаталогов**(этосредствоиерархическогопредставленияресурсов,принадлежащихнекоторойотдельновзятойорганизации,и информацииоб этихресурсах)корпорации**Microsoft**для операционныхсистемсемейства**WindowsNT**. *ActiveDirectory*позволяетадминистраторамиспользоватьглобальныеполитики,развѐртывать программынамножествекомпьютеров(черезглобальные политикиилипосредством**MicrosoftSystemsManagementServer 2003**) иустанавливать важныеобновления навсехкомпьютерахвсети(сиспользованием**WindowsServerUpdateServices(WSUS);SoftwareUpdateServices(SUS)**ранее).*ActiveDirectory*хранитданныеинастройкисредывцентрализованнойбазеданных.Сети*ActiveDirectory*могутбытьразличногоразмера: от несколькихсотендо несколькихмиллионов объектов.

Помимообычныхдляслужбкаталоговзадач,*ActiveDirectory*способнаудовлетворитьширокийспектрпотребностейпообработкеимен,обслуживаниюзапросов,регистрации,администрированию

иустранениюконфликтов.В*ActiveDirectory*используетсятесноувязанныйнабор**API**ипротоколов,такчтоонаможетработатьснесколькимипространствамиимен,собиратьипредоставлятьинформациюокаталогахиресурсах,находящихсявудаленныхфилиалахиподуправлениемразныхОС. *ActiveDirectory*имеетследующие возможности ихарактеристики:

Поддержкаоткрытыхстандартовдляоблегчениямежплатформныхоперацийскаталогами,вт.ч.доменной системыимен***DNS***и стандартныхпротоколов, такихкак**LDAP(*LightweightDirectoryAccessProtocol*—** «облечённыйпротоколдоступакаталогам»).

Поддержкастандартныхформатовимен дляпростоты миграциии эксплуатации.Богатыйнабор**API**, которыемогутиспользоватьсякак для командныхсценариев,

так и в программахна**C/C++**.

Простой и интуитивнопонятныйпроцесс администрированияблагодаря несложной иерархическойдоменнойструктуре и использованию технологии«перетащить и оставить».

Возможностьрасширениянабора объектов в каталогах, за счет гибкойлогическойсхемы.

Быстрый поиск по глобальномукаталогу.

Быстрое иудобное обновление информациипосредствоммногоуровневой(*multimaster*)репликацииданных.

Совместимость с предыдущимиверсиями ОС**WindowsNT**.Взаимодействие с сетями**NetWare**.

*ActiveDirectory*позволяетуправлятьсодногорабочегоместавсемизаявленнымиресурсами(файлами,периферийнымиустройствами,базамиданных,подключениямик серверам,доступомкWeb,пользователями,другимиобъектами,сервисамиит.д.).В качествеидентификационнойслужбывнейиспользуетсядоменнаясистемаимен(***DNS***),применяемаявИнтернете,объектывдоменахстроятсявиерархиюорганизационныхединиц(***OE***),адоменымогутбытьобъединенывдревовиднуюструктуру.Администрированиестановитсяещепроще,таккакв*ActiveDirectory*отсутствуетпонятиеглавногоконтроллерадоменов(***ГКД***)ирезервногоконтроллерадоменов(***РКД***).

В*ActiveDirectory*существуюттолькоконтроллерыдомена(***КД***),ивсеониравнымеждусобой.Администраторможетсделатьизмененияналюбом***КД***,иэтиизменениябудутскопированы на всехостальных***КД***.

*ActiveDirectory*отделяет логическуюструктуруиерархии доменов**Windows2003**от физическойструктурысети.*Объекты:*ресурсыхранятся в виде объектов.

Схема*ActiveDirectory*:

- Домены:базоваяорганизационнаяструктура.
- Деревья:несколькодоменовобъединяются в иерархическуюструктуру.Леса:группа из
- нескольких деревьев домена.

*Организационные единицы:*позволяютделитьдомен назоны и делегировать нанихправа.

Логическаяструктура*ActiveDirectory*небазируетсянафизическомместонахождениисерверовилисетевыхсоединенияхвпределахдомена.Этопозволяетструктурироватьдомены,оттал киваясьнеоттребованийфизическойсети,аотадминистративныхи организационныхтребований.

Объектыхранятсяв*ActiveDirectory*ввидеиерархическойструктурыконтейнеровиподконтейнеров,упрощающейпоиск,доступиуправление,онавомногомпохожанафайловую систему**Windows**с файлами в папками.

Классыобъектов.Объектнасамомделепредставляетсобойпростонаборатрибутов.Например,объектпользователя(*userobject*)состоитизтакихатрибутов,какимя,пароль,телефонныйномер,сведенияочленствевгруппахит.д.Атрибуты,образующиеобъект,определяютсяклассом объекта.

Классыиатрибуты,определяемыеими,собирательноназываются*ActiveDirectorySchema*

—втерминологиибазданныхсхема(*schema*)— этоструктураблициполей,атакжеихвзаимосвязи.*ActiveDirectorySchema*можносчитатьнабором данных(классовобъектов),определяющимто,какорганизованаихранитсяреальнаяинформация(атрибутыобъекта) вкаталоге.

ActiveDirectory— неперваяслужбакаталогов.Всовременныхсетяхиспользуетсянесколькослужбкаталогов истандартов. Вот лишьнекоторыеизних:

X.500и**DirectoryAccessProtocol(DAP).X.500** — спецификация**InternetStandardsOrganization (ISO)**, определяющая,как должны быть структурированыглобальныекаталоги.**X.500**такжеописываетприменение**DAP**для обеспечения взаимодействия междуклиентами и серверамикаталогов;

LightweightDirectoryAccessProtocol (LDAP).LDAPбыларазработанав ответ накритические замечания по**DAP**,котораяоказалась слишком сложнойдля применения вбольшинствеслучаев.**LDAP**быстросталастандартнымпротоколом каталоговв Интернете.

- **NovellDirectoryServices (NDS)**. Службакаталогов для сетей**NovellNetWare**,совместимаясостандартом**X.500**.
- **ActiveDirectory**. Составная частьсетей подуправлением**WindowsServer2000**или**WindowsServer2003**. Соответствуетстандарту**LDAP**.

Порядокработы

Внимательноознакомьтесьскраткимисправочно-информационнымматериаломпотемезанятия.

Задание1. Установите ActiveDirectory.

1. Подготовьте виртуальнуюмашину **VM-2**кустановкеслужбы каталогов:
- подключите к ВМ образустановочного диска***win2003-1.iso***;
2. Откройтедиалоговоеокно**Управлениеданнымсервером** (***Пуск/ Администрирование/Управление ДаннымСервером***).
3. Проверьте наличиеустановленногосервера доменных имен (***DNS***).

*Установкаслужбы каталогов невозможна без**DNS**.*

4. Активизируйте добавление новыхролей для сервера (***Добавить илиудалитьроль***).
5. Выберите пункт**Контроллердомена(ActiveDirectory).** Перейдитек следующемушагукнопкой***Далее***.
6. Ознакомьтесь с информацией обустанавливаемыхкомпонентах ищелкните***Далее***.
7. Ознакомьтесь с информацией**МастераустановкиActiveDirectory**и щелкните***Далее***.
8. Ознакомьтесь с информаций о совместимости с операционнойсистемой ищелкните***Далее***.
9. Укажите **вариантсозданийконтроллерадомена**-*Контроллер домена вновом домене*и щелкните***Далее***.
10. Укажите **тип создаваемогодомена**-*Новый домен в новом лесу*и щелкните***Далее***.
11. Введите**полноеDNS-имя создаваемого домена**-***example.edu.ru***и щелкните***Далее***.
12. Введите**NetBIOS-имя домена** -*EXAMPLE*и щелкните***Далее***.

*Обычно оно уже указаннопо умолчанию,исходяиз того, какое**DNS**-имя было дано создаваемому домену. Например, при созданиидомена с именем**example.edu.ru**, по умолчанию**NETBIOS-имя**будет **EXAMPLE**.*

13. Укажите местохранениябазданныхи журналов*ActiveDirectory*:

введите в поле **Папкарасположения Баз-*C:\WINDOWS\NTDS\BASE***;введите в поле **Папкарасположенияжурнала-*C:\WINDOWS\JOURNAL***;подтвердите изменениякнопкой***Далее***.

14. Ознакомьтесь с информацией об общей папке и щелкните***Далее***.

*ЕсливашDNS-сервер настроен неправильно,выполучитесообщениеоб ошибке ивозможных путях её устранения(выберите**Проблема будетрешенапозже**).*

15. Установите разрешениядля объектов службыкаталогов-*Разрешения,совместимыетолько cWindows 2000 илиWindowsServer 2003*и щелкните***Далее***.

16. Укажите пароль, дляучётнойзаписиадминистратора режима восстановления:введите в поле **Пароль режимавосстановления**– *123456*;введите в поле **Подтверждение**– *123456*;подтвердите измененияк нопкой***Далее***.

17. Ознакомьтесь с сводной информацией обустановкеслужбы каталогов и запустите еёустановкукнопкой***Далее***.

18. Завершите работумастера кнопкой***Готово***.

19. Перезагрузите виртуальную машинукнопкой***Перезагрузитьсейчас***.

20. Войдите в системупосле перезагрузки и завершитеустановкуслужбы каталоговкнопкой***Готово***.

Задание2. Работа с ActiveDirectoryManager

- Откройтедиалоговоеокно**Пользователи и компьютеры(*Пуск/Администрирование/ActiveDirectory–пользователи и компьютеры*)**.
- Ознакомьтесь с структуройсозданногоранее домена:• развернитеузел**example.edu.ru**;

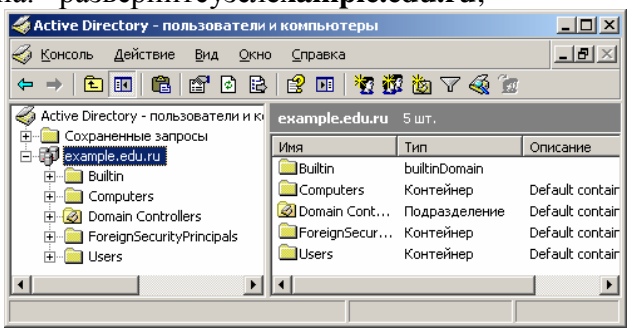


Рисунок 1. Пользователии компьютерыдомена.

- просмотрите стандартныхпользователейдомена (**Builtin**);
- просмотрите контроллеры домена (**DomainControllers**).

Создайте новыйкаталог(подразделение/контейнер) в корне сервера:активизируйтеузел**example.edu.ru**;

- щелкните покнопке***Создание новогоподразделения втекущемконтейнере*** напанелиинструментов;
- в появившемся диалоговомокне введите**имя создаваемогоподразделения**-*Students*(***OK***);

Будетсозданновыйконтейнер дляподразделенияи выделение автоматически переместитьсяна него.

- Создайте новуюучетнуюзаписьпользователя в контейнере**Students**:
- откройте диалоговоеокно**Новый объект– Пользователь** кнопкой***Создание нового пользователя втекущемконтейнере*** ;
- введите данныео пользователе:
  - **Полноеимя пользователя** – *ПростоПользователь*;
  - **Имя входа пользователя(логин)**– *JustUser*;
  - Подтвердите введенныеданныекнопкой***Далее***.

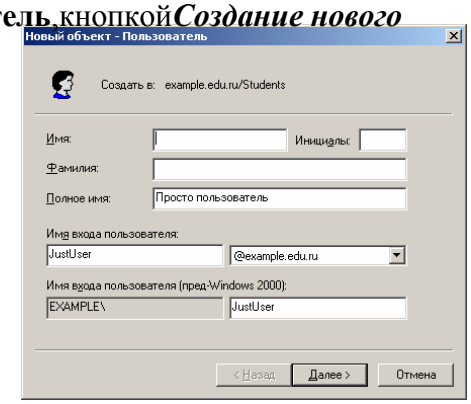


Рисунок 2. Ввод данныхновогопользователя.

установите пароль для пользователя:

- введите в поле **Пароль** – *User1234*;
- введите в поле **Подтверждение**– *User1234*;
- установите флажок*Срок действияпаролянеограничен*;
- завершите ввод пароля кнопкой***Далее***.

В правойобласти отобразитьсязапись,соответствующаясозданномупользователю.

- Введите болееполнуюинформацию о пользователе:
  - откройте диалоговоеокно**свойствпользователя** (двойнойщелчокпо надписи***Простопользователь***);
  - введите в поле **Описание**– *это тестовый пользователь*;
  - введите в поле **Комната** -*316* (номеркабинета, в котором проходитзанятие);
  - введите в поле **Телефон**– <*номер_телефона*>;
  - укажите *адресные данные*на вкладке**Адрес**;
  - укажите несколькодополнительныхтелефоновпользователя навкладке **Телефоны**;
  - завершите изменение данных пользователякнопкой***ОК***.Создайте группу**group1**в контейнере**Students**:
    - откройте диалоговоеокно**создания групп(*контекстное меню/Создать/Группа*)**;
    - введите **имя группы**– *group1*;
    - завершите создание группыкнопкой***ОК***.

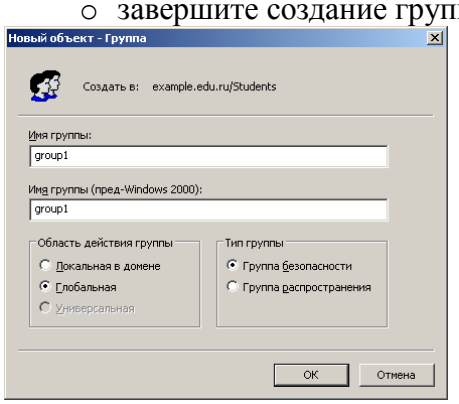


Рисунок 3. Создание группы.

- Задайте дополнительнуюинформацию для группы**group1**:
  - откройте диалоговоеокно**свойствгруппы**(двойнойщелчокпо надписи**group1**);
  - введите в поле **Описание**– *Этотестоваягруппа*;
  - завершите изменение данныхгруппыкнопкой***ОК***.
  - Включите созданногоранее пользователя**Простопользователь(*JustUser*)** в группу**group1**:
  - откройте диалоговоеокно**свойствпользователя**(двойнойщелчокпо записипользователя);
  - перейдите навкладку**Член групп**;
  - откройте диалоговоеокно выбора группыкнопкой***Добавить***;
  - введите **название группы**– *group1*;
  - завершите добавлениепользователя в группукнопкой***ОК***.
  - закройте диалоговоеокносвойствпользователякнопкой***ОК***.
- Выполните редактирование политикибезопасностидомена,созданную автоматически:
  - откройте диалоговоеокно свойствдомена**example.edu.ru** (***контекстное меню/Свойства***);
  - перейдите навкладку**Групповая политика**:

*В списке будетрасположена политика доменапо умолчанию**DefaultDomainPolicy**.*

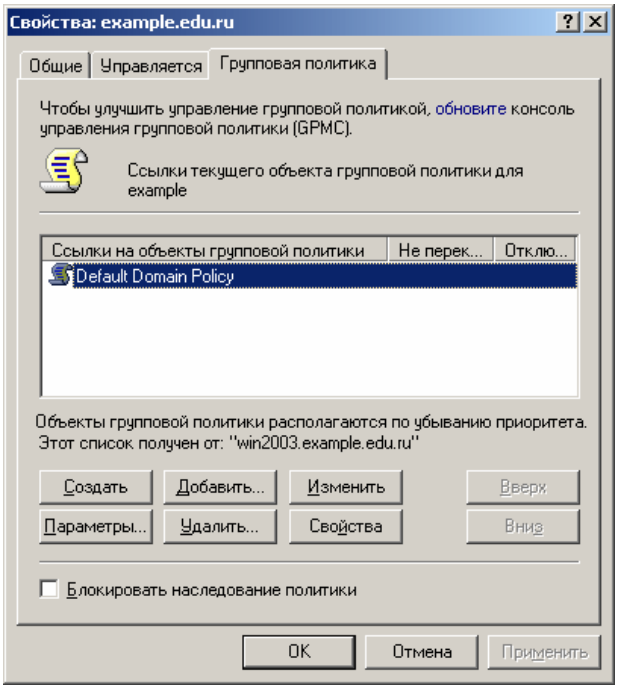


Рисунок 4. Свойства домена

- откройте диалоговое окно (**Редактор объектов групповой политики**) изменения политики***Default Domain Policy*** (двойной щелчок по политике);

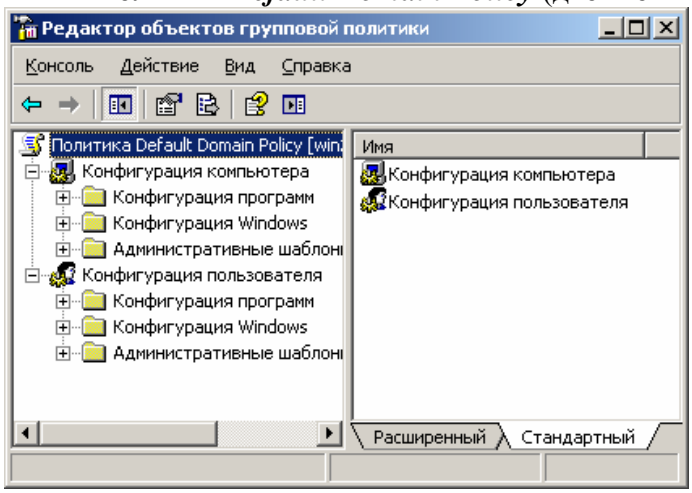


Рисунок 5. Редактор объектовгрупповой политики

- внесите в изменения вполитикупаролей:
- перейдите в раздел**Политикапаролей(*Конфигурациякомпьютера/КонфигурацияWindows /Параметры безопасности/Политикиучётныхзаписей/Политики паролей*)**;

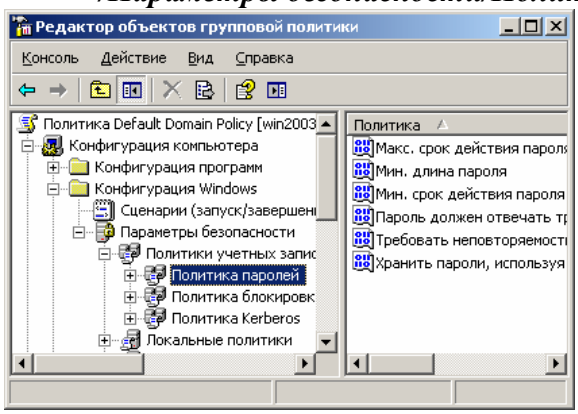


Рисунок 6. Политика паролей.

установите минимальную длину пароля:
1. откройте окно **изменения параметров пароля** (двойной щелчок по надписи ***Мин. длинна пароля***);
2. введите в поле **Длина пароля не менее** – *5*;
3. подтвердите изменения кнопкой ***ОК***;
отключите соответствие пароля требованиям сложности:
1. откройте диалоговое окно **свойств требования сложности** (двойной щелок по надписи ***Пароль должен отвечать требованиям сложности***);
2. установите радиокнопку *Отключить*;
3. подтвердите изменения кнопкой ***ОК***;
закройте **Редактор объектов групповой политики (*Консоль/Выход*)**;
закройте диалоговое окно свойств домена кнопкой ***ОК***.
Выполните выход из системы с повторным входом для активации изменений в политике безопасности. *Изменения в политике паролей вступят в силу только после выхода из системы и повторного входа в неё.*

- Измените пароль созданного ранее пользователя:
- активизируйте раздел **Students**;
- задайте новый, более простой пароль пользователю **Просто пользователь**:
- откройте диалоговое окно **задания пароль (*контекстное меню/Смена пароля*)**;
- введите в поле **Пароль** – *123*;
- введите в пол **Подтверждение пароля** – *123*;
- *Обратите внимание что сообщений о слишком простом пароле не было.*
- Исключите созданного ранее пользователя из группы **group1**:
- откройте диалоговое окно **свойств группы**;
- перейдите на вкладку **Члены группы**;
- выделите в списке удаляемого пользователя и щелкните по кнопке ***Удалить***;
- подтвердите удаление кнопкой ***Да***;
- закройте диалоговое окно свойств группы кнопкой ***ОК***.
- Включите созданного ранее пользователя в администраторы домена:
- откройте диалоговое окно **свойств пользователя Просто пользователь**;
- перейдите на вкладку **Член групп** и щелкните ***Добавить***;
- введите в поле Администраторы домена;
- завершите добавление в группу кнопкой ***ОК***;
- закройте окно свойств пользователя кнопкой ***ОК***.

Задание 3. Присоединение компьютеров под управлением Windows XP к домену.
1. Запустите виртуальную машину **VM-3** и загрузите в ней ОС **Windows XP**.
2. Откройте диалоговое окно **Свойства системы (*Пуск/Панель управления/Система*)** и перейдите на вкладку **Имя компьютера** (***Далее***).
3. Откройте диалоговое окно **Изменение имени** кнопкой ***Изменить***.
4. Укажите в разделе **Является членом** – *домена*.

5. Введите в поле левую часть имени созданного ранее домена, например,**example**.

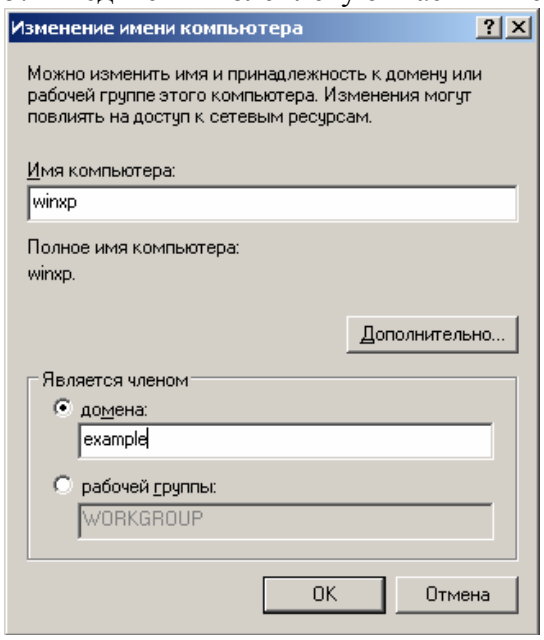


Рисунок 7. Изменение имени компьютера.

6. Подтвердите изменения кнопкой ***ОК***. *Через некоторое время домен к которому подклю-чается компьютер запросит имя и пароль администратора домена.*
7. Введите **имя/пароль** администратора в созданном ранее домене (*JustUser/123*).
8. Ознакомьтесь с сообщением от домена *«Добро пожаловать в домен»* и щелкните ***ОК***.
9. Ознакомьтесь с информацией о необходимости перезагрузки компьютера и закройте окно кнопкой ***ОК***.
10. Закройте диалоговое окно **Свойства системы** кнопкой ***ОК***.
11. В появившемся диалоговом окне согласитесь с перезагрузкой кнопкой ***Да***. *После этого компьютер начнет перезагружаться.*
12. Войдите в систему с использованием любой из созданных вами учетных записей.
13. Проверьте действие сделанных вами ограничений в домене.
14. Выключите ВМ **VM-1**.

Контрольные вопросы

1. Опишите различия между рабочей группой и доменом.
2. Каково основное различие между ОС Windows XP и Windows Server 2003?
3. Возможно ли создать домен в сети, где все компьютеры сети работают под управлением ОС Windows XP?
4. Дайте определение контроллера домена.
5. Перечислите известные Вам встроенные учетные записи пользователей и групп пользователей домена и опишите их назначение.
6. Что означает термин «изолированный» сервер?
7. Опишите различия между рабочей группой и доменом.
8. Почему встроенная учетная запись Guest (Гость), как правило, бывает отключена?

Лабораторная работа

Тема: Установка и настройка сетевой операционной системы: IP -адресация

Цель занятия: Научиться определять адрес подсети и адрес хоста по маске подсети; научиться определять количество и диапазон адресов возможных узлов в подсетях; научиться структурировать сети с использованием масок

Продолжительность занятия: 4 часа

Краткие теоретические и справочно-информационные материалы по теме занятия.

Связь с проектом

Для успешного решения задач администрирования необходимо хорошо разбираться в системе IP-адресации. Знание принципов использования масок и структуризации сетей поможет грамотно решать многие вопросы настройки локальной сети.

Задание 1. Определить, находятся ли два узла А и В в одной подсети или в разных подсетях, если адреса компьютера А и компьютера В соответственно равны: 26.219.123.6 и 26.218.102.31, маска подсети 255.192.0.0.

Указания к выполнению

1. Переведите адреса компьютеров и маску в двоичный вид.
2. Для получения двоичного представления номеров подсетей обоих узлов выполните операцию логического умножения AND над IP-адресом и маской каждого компьютера.
3. Двоичный результат переведите в десятичный вид.
4. Сделайте вывод.

Процесс решения можно записать следующим образом:

Компьютер А:

IP-адрес: 26.219.123.6 = 00011010. 11011011. 01111011. 00000110

Маска подсети: 255.192.0.0 = 11111111. 11000000. 00000000. 00000000

Компьютер В:

IP-адрес: 26.218.102.31 = 00011010. 11011010. 01100110. 00011111

Маска подсети: 255.192.0.0 = 11111111. 11000000. 00000000. 00000000

Получаем номер подсети, выполняя операцию AND над IP-адресом и маской подсети.

Компьютер А: AND	00011010. 11011011. 01111011. 00000110 11111111. 11000000. 00000000. 00000000 00011010. 11000000. 00000000. 00000000 26 192 0 0

Компьютер В: AND	00011010. 11011010. 01100110. 00011111 11111111. 11000000. 00000000. 00000000 00011010. 11000000. 00000000. 00000000 26 192 0 0

Ответ: номера подсетей двух IP-адресов совпадают, значит компьютеры А и В находятся в одной подсети. Следовательно, между ними возможно установить прямое соединение без применения шлюзов.

Задание 2. Определить количество и диапазон IP-адресов в подсети, если известны номер подсети и маска подсети.

Номер подсети – 26.219.128.0, маска подсети – 255.255.192.0.

Указания к выполнению

1. Переведите номер и маску подсети в двоичный вид.

Номер подсети: 26.219.128.0 = 00011010. 11011011. 10000000. 00000000

Маска подсети: 255.255.192.0 = 11111111. 11111111. 11000000. 00000000

2. По маске определите количество бит, предназначенных для адресации узлов (их значение равно нулю). Обозначим их буквой К.
3. Общее количество адресов равно 2К. Но из этого числа следует исключить комбинации, состоящие из всех нулей или всех единиц, так как данные адреса являются особыми. Следовательно, общее количество узлов подсети будет равно 2К – 2.

В рассматриваемом примере К = 14, 2К – 2 = 16 382 адресов.

4. Чтобы найти диапазон IP-адресов нужно найти начальный и конечный IP-адреса подсети. Для этого выделите в номере подсети те биты, которые в маске подсети равны единице.
Это разряды, отвечающие за номер подсети. Они будут совпадать для всех узлов данной подсети, включая начальный и конечный:
Номер подсети: 26.219.128.0 = **00011010. 11011011. 10**000000. 00000000
Маска подсети: 255.255.192.0 = **11111111. 11111111. 11**000000. 00000000
5. Чтобы получить начальный IP-адрес подсети нужно невыделенные биты в номере подсети заполнить *нулями*, за исключением крайнего правого бита, который должен быть равен единице. Полученный адрес будет первым из допустимых адресов данной подсети:
Начальный адрес: 26.219.128.1 = **00011010. 11011011. 10**000000. 00000001
Маска подсети: 255.255.192.0 = **11111111. 11111111. 11**000000. 00000000
6. Чтобы получить конечный IP-адрес подсети нужно невыделенные биты в номере подсети заполнить *единицами*, за исключением крайнего правого бита, который должен быть равен нулю. Полученный адрес будет последним из допустимых адресов данной подсети:
Конечный адрес: 26.219.191.254 = **00011010. 11011011. 10**111111. 11111110
Маска подсети: 255.255.192.0 = **11111111. 11111111. 11**000000. 00000000
Ответ: Для подсети 26.219.128.0 с маской 255.255.192.0: количество возможных адресов: 16 382,
диапазон возможных адресов: 26.219.128.1 – 26.219.191.254.
Задание 3. Организации выделена сеть класса С: 212.100.54.0/24.
Требуется разделить данную сеть на 4 подсети с количеством узлов в каждой не менее 50. Определить маски и количество возможных адресов новых подсетей.
Указания к выполнению
1. В сетях класса С (маска содержит 24 единицы – 255.255.255.0) под номер узла отводится 8 бит, т. е. сеть может включать 28 – 2 = 254 узла.
2. Требование деления на 4 подсети по 50 узлов в каждой может быть выполнено: 4·50 = 200 < 254. Однако число узлов в подсети должно быть кратно степени двойки. Относительно 50 ближайшая б*о*льшая степень – 26 = 64. Следовательно, для номера узла нужно отвести 6 бит, вместо 8, а маску расширить на 2 бита – до 26 бит (см. рис. 3).
3. В этом случае вместо одной сети с маской 255.255.255.0 образуется 4 подсети с маской 255.255.255.192 и количеством возможных адресов в каждой – 62 (не забывайте про два особых адреса).
4. Номера новых подсетей отличаются друг от друга значениями двух битов, отведенных под номер подсети. Эти биты равны 00, 01, 10, 11.
Ответ: маска подсети – 255.255.255.192, количество возможных адресов – 62.

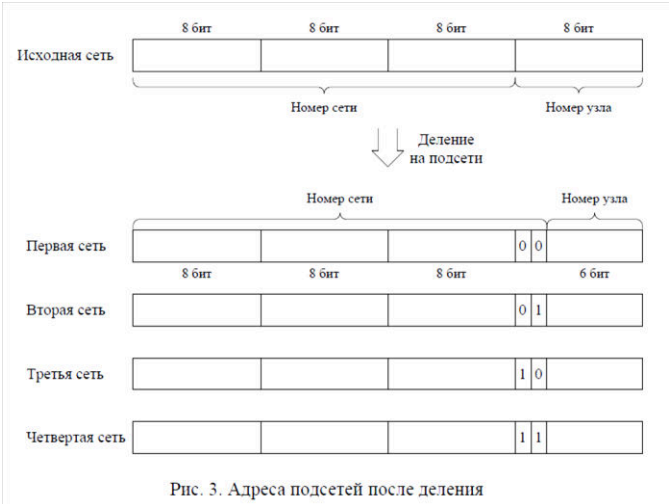


Рис. 3. Адреса подсетей после деления

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

Самостоятельная работа

Задание 1. Определить, находятся ли два узла А и В в одной подсети или в разных подсетях.

1. IP-адрес компьютера А: 94.235.16.59;
IP-адрес компьютера В: 94.235.23.240;
Маска подсети: 255.255.240.0.
2. IP-адрес компьютера А: 131.189.15.6;
IP-адрес компьютера В: 131.173.216.56;
Маска подсети: 255.248.0.0.
3. IP-адрес компьютера А: 215.125.159.36;
IP-адрес компьютера В: 215.125.153.56;
Маска подсети: 255.255.224.0.

Задание 2. Определить количество и диапазон адресов узлов в подсети, если известны номер подсети и маска подсети.

1. Номер подсети: 192.168.1.0, маска подсети: 255.255.255.0.
2. Номер подсети: 110.56.0.0, маска подсети: 255.248.0.0.
3. Номер подсети: 88.217.0.0, маска подсети: 255.255.128.0.

Задание 3. Определить маску подсети, соответствующую указанному диапазону IP-адресов.

1. 119.38.0.1 – 119.38.255.254.
2. 75.96.0.1 – 75.103.255.254.
3. 48.192.0.1 – 48.255.255.254.

Задание 4. Организации выделена сеть класса В: 185.210.0.0/16.

Определить маски и количество возможных адресов новых подсетей в каждом из следующих вариантов разделения на подсети:

1. Число подсетей – 256, число узлов – не менее 250.
2. Число подсетей – 16, число узлов – не менее 4000.
3. Число подсетей – 5, число узлов – не менее 4000. В этом варианте укажите не менее двух способов решения.

Контрольные вопросы

1. Может ли быть IP-адрес узла таким? Укажите неверные варианты IP-адрес. Ответ обоснуйте.

• 192.168.255.0
• 167.234.56.13
• 224.0.5.3
• 172.34.267.34
• 230.0.0.7
• 160.54.255.255

2. Может ли маска подсети быть такой? Укажите неверные варианты. Ответ обоснуйте.

• 255.254.128.0
• 255.255.252.0
• 240.0.0.0
• 255.255.194.0
• 255.255.128.0
• 255.255.255.244
• 255.255.255.255

3. Можно ли следующие подсети разделить на N подсетей. Если это возможно, то укажите варианты разбиения с максимально возможным количеством подсетей или узлов в каждой подсети. Ответ обоснуйте.

• 165.45.67.0, маска 255.255.255.224, N=3
• 235.162.56.0, маска 255.255.255.224, N=6
• 234.49.32.0, маска 255.255.255.192, N=3

Лабораторная работа
Установка и настройка ОС семейства Linux

Цель: научиться устанавливать ОС семейства Linux.

Средства для выполнения работы:

- аппаратные: компьютер с установленной ОС Windows XP.
- программные: приложение ВМ (VirtualBox); виртуальные машина VM-2; установочный образ ОС openSUSE.iso.

Теоретические сведения

Linux (Линукс) — UNIX-совместимое ядро операционной системы, разработка которого была начата финским студентом Линусом Торвальдсом в 1991 году.

Как таковое ядро ОС ***Linux*** способно управлять аппаратным обеспечением и не предоставляет инструментов пользователю для решения его задач. Поэтому ОС ***Linux*** распространяются в виде дистрибутивов.

Дистрибутив операционной системы — это форма распространения системного программного обеспечения. Наличие дистрибутивов вызвано тем, что форма программного обеспечения, используемая для его распространения, почти никогда не совпадает с формой программного обеспечения работающей системы.

Дистрибутив обычно содержит программы для начальной инициализации системы (инициализация аппаратной части, загрузка урезанной версии системы и запуск программы-установщика), программу-установщик (для выбора режимов и параметров установки) и набор специальных файлов, содержащих отдельные части системы (так называемые *пакеты*). Программа установки позволяет также произвести первичную настройку системы.

На сегодняшний день существует большое количество различных дистрибутивов ОС ***Linux*** (более 100), ориентированных на различных пользователей. К наиболее популярным относятся такие дистрибутивы, как: ***PCLinuxOS***, ***Ubuntu***, ***openSUSE***, ***Fedora***, ***Mint***, ***Sabayon***, ***Mandriva***, ***Debian***, ***MEPIS***, ***Damn Small1*** .

Характеристики ОС семейства Linux — многозадачность, многопользовательский доступ, свопирование оперативной памяти на диск, загрузка выполняемых модулей по требованию, совместное использование выполняемых программ, общие библиотеки, динамическое кэширование диска, возможность запуска исполняемых файлов других ОС, поддержка различных форматов файловых систем, работа на различных аппаратных платформах и т.д.

OpenSUSE — дистрибутив рассчитан, в первую очередь, на настольные системы и ориентирован на широкий круг пользователей от новичков до профессионалов, - любопытствующих, мигрирующих с других ОС и давних приверженцев ***Linux*** и свободного программного обеспечения. Удобный и дружественный интерфейс, родная языковая среда наряду с самыми свежими версиями пользовательских и системных программ и пакетов призваны окончательно развеять миф о недоступности и неудобстве ***Linux*** в повседневной работе.

Разрабатывается французской компанией. Дистрибутив основан на *Red Hat Linux*, с большим количеством дополнений. Содержит большое множество программного обеспечения. Включает в себя новую и интуитивно понятную программу установки с графическим интерфейсом, переведенную на большое количество языков; фирменные средства настройки системы; поддержку автоматического монтирования/демонтирования носителей информации.

Установка ***OpenSUSE*** на компьютер отличается простотой и включает в себя следующие этапы: загрузка компьютера с установочного диска, принятие лицензионного соглашения, выбор языка, установка параметров безопасности, подготовка жесткого диска, выбор пакетов для установки, ввод данных пользователя и его пароля.

К одной из самых сложных частей процесса установки относится подготовка жесткого диска, которая в случае неправильных действий пользователя может привести к потере данных. Установщик ОС ***OpenSSE*** может автоматически использовать все свободное пространство на жестком диске, весь диск целиком или позволяет пользователю самому выполнить подготовку диска к установке.

Подготовка жесткого диска к установке сводится к выделению места для устанавливаемой ОС, созданию разделов в выделенном пространстве и их форматированию. Специалисты по ОС семейства ***Linux*** рекомендуют создавать отдельные разделы для размещения ядра ОС и файлов загрузчика ОС, файлов пользователей, файла подкачки.

Как правило в случае выбора автоматического режима подготовки диска, установщик самостоятельно создает перечисленные выше разделы.

Выполнение работы

Задание 1. Установите ОС OpenSUSE в ВМ VirtualBox.

1. Запустите приложение виртуальных машин ***VirtualBox***.
2. Запустите созданную ранее виртуальную машину VM-2 кнопкой ***Запустить*** и перейдите в окно ВМ, активизировав его щелчком мыши.
3. Выберите язык установки *русский* (см. Рисунок 3):
   - откройте список поддерживаемых языков (клавиша **F2**);
   - выберите в списке нужный язык (*русский*) с помощью клавиш управления курсором;
   - подтвердите выбор клавишей ***ENTER***.

Рисунок 3. Выбор языка установки

4. Запустите **Мастер установки ОС** - пункт меню ***Установка***;
5. Пропустите проверку носителя информации с которого происходит установка ОС кнопкой ***Далее***.
6. Ознакомьтесь с лицензионным соглашением и примите его - радиокнопка **Да, я согласен с условиями лицензионного соглашения** (***Далее***).
7. Выберите в качестве рабочего стола **KDE** (***Далее***).
8. Подготовьте жесткий диск для установки ОС:
   - запустите **Мастер разбивки жестких дисков** - надпись ***Разметка***;

- ознакомьтесь с предложением разметки;
- укажите **способ разметки** – *Принять предложение* (***Далее***);
- ознакомьтесь и примите предложение мастера разметки - ***Принять***;
- завершите работу мастера кнопкой ***Принять***;

9. Ознакомьтесь с лицензионным соглашением пакета agfa-fonts и согласитесь кнопкой ***Я согласен***.
10. Ознакомьтесь с лицензионным соглашением пакета flash-player и согласитесь кнопкой ***Я согласен***.
11. Ознакомьтесь с лицензионным соглашением пакета java-1_5_0-sun и согласитесь кнопкой ***Я согласен***.
12. Ознакомьтесь с лицензионным соглашением пакета java-1_5_0-sun-plugins и согласитесь кнопкой ***Я согласен***.
13. Подтвердите установку кнопкой ***Установить***. *Дождитесь окончания установки ОС в конце которой будет произведена перезагрузка.*
14. Введите пароль для пользователя *root - 123456*. Подтвердите кнопкой ***Далее***.
15. Ознакомьтесь с информацией о небезопасном пароле и щелкните ***Да***.
16. Ознакомьтесь с информацией о том, что пароль содержит только цифры, и щелкните ***Да***.
17. Задайте **имя компьютера**:
    - введите в поле **Имя узла** – *linux*;
    - введите в поле **Имя домена** – *example.edu.ru*;
    - подтвердите введенные данные кнопкой ***Далее***.
18. Ознакомьтесь с предлагаемыми **сетевыми настройками** и примите их (***Далее***).
19. Укажите **способ регистрации** – *Локальный (/etc/passwd)* (***Далее***).
20. Введите **данные пользователя**:
    - введите в поле **Полное имя пользователя** – *Просто Пользователь*;
    - введите в поле **Имя пользователя** – *JustUser*;
    - введите в поле **Пароль** – *123*;
    - введите в поле **Подтверждение пароля** – *123*;
    - завершите ввод данных пользователя кнопкой ***Далее***.
    - ознакомьтесь с информацией о слишком простом пароле и согласитесь с его использованием кнопкой ***Да***.
21. Ознакомьтесь с **Примечаниями к выпуску** и щелкните ***Далее***.
22. Ознакомьтесь с предлагаемыми настройками оборудования и щелкните ***Далее***.
23. Завершите настройку кнопкой ***Завершить***.
24. Создайте и сохраните в своей папке *снимок экрана* с работающей ВМ с загруженной ОС.
25. Завершите работу виртуальной машины (***Меню KDE()/Выйти/Остановить компьютер/Подтвердить***).

Лабораторная работа
Совместная работа различных ОС

Цель: научиться организовывать совместную работу различных ОС.

Средства для выполнения работы:

- аппаратные: компьютер с установленной ОС Windows XP.

- программные: приложение ВМ (VirtualBox); виртуальная машина VM-1; установочный образ ОС openSUSE.iso, драйвер для файловой системы Ext2 - Ext2 Installable File System For Windows.

Теоретические сведения

Одно из первых понятий, с которым сталкивается любой пользователь компьютера - это *понятие файловой системы*. При этом пользователь видит только одну сторону файловой системы, а именно - иерархическую структуру (или дерево) каталогов и файлов. Фактически все каталоги тоже являются файлами, и, с точки зрения механизма хранения файлов на диске, все файлы (включая каталоги) организованы одинаково. Но для человека работать с "линейным" списком, содержащим тысячи файлов, было бы крайне неудобно, поэтому и было изобретено понятие "каталога", исключительно логического образования, позволяющего дать каждому файлу понятное для человека "полное имя", определяющее некий "путь" к файлу в единой структуре каталогов.

Файловая система

Файловая система (англ. file system) — регламент, определяющий способ организации, хранения и именования данных на носителях информации. Она определяет формат физического хранения информации, которую принято группировать в виде файлов. Конкретная файловая система определяет размер имени файла, максимальный возможный размер файла, набор атрибутов файла. Некоторые файловые системы предоставляют сервисные возможности, например, разграничение доступа или шифрование файлов.

Сегодня существует большое количество различных файловых систем исопльзуемые для различных целей и операционных систем. Различные ОС используют разнообразные файорвые системы, например ***Windows - FAT и NTFS***, а ***ОС Linux*** традиционно используют ***ext3, XFS*** и множество других.

NTFS (*от англ. New Technology File System — «файловая система новой технологии»*) — стандартная файловая система для семейства операционных систем **Microsoft Windows NT**. **NTFS** заменила использовавшуюся в MS-DOS и Microsoft Windows файловую систему **FAT**. **NTFS** поддерживает систему метаданных и использует специализированные структуры данных для хранения информации о файлах для улучшения производительности, надёжности и эффективности использования дискового пространства. **NTFS** имеет встроенные возможности разграничивать доступ к данным для различных пользователей и групп пользователей, а также назначать квоты (ограничения на максимальный объём дискового пространства, занимаемый теми или иными пользователями). **NTFS** использует систему журналирования для повышения надёжности файловой системы.

EXT3 или *3-я расширенная файловая система* — журналируемая файловая система, используемая в операционных системах на ядре **Linux**, является файловой системой по умолчанию во многих дистрибутивах. Основана на ФС **ext2**. Основное отличие от **ext2fs** состоит в том, что **ext3** *журналируема*, то есть в ней предусмотрена запись некоторых данных, позволяющих восстановить файловую систему при сбоях в работе компьютера.

XFS — высокопроизводительная журналируемая файловая система, созданная компанией ***Silicon Graphics*** для их операционной системы **IRIX**. 1 мая 2001 года ***Silicon Graphics*** выпустила **XFS** под **GNU General Public License**. Поддержка **XFS** была включена в ядро Linux версий 2.4 (начиная с 2.4.25, когда Марсело Тосатти (Marcelo Tosatti) посчитал её достаточно стабильной) и 2.6, и, таким образом, она стала довольно универсальной для Linux-систем. Инсталляторы дистрибутивов ***SuSE, Gentoo, Mandriva, Slackware, Ubuntu, Fedora и Debian*** предлагают **XFS** как вариант файловой системы для установки. **FreeBSD** стала поддерживать **XFS** в режиме чтения в декабре 2005 года.

*Более полное представление о существующих файловых системах можно найти на страницах электронной энциклопедии **Wikipedia**.*

Операционные системы **Windows** стандартными средствами способны работать только с "родными" файловыми системами - **FAT** и **NTFS**. Для поддержки других файловых систем необходимо использовать дополнительные драйвера или программное обеспечение. Для доступа к файловой системе **ext2** или **ext3** можно воспользоваться:

- драйвером Ext2 Installable File System For Windows;
- утилитой Explore2fs .

Драйвер **Ext2 Installable File System For Windows** позволяет получить доступ на чтение и запись к разделам с файловыми системами **ext2/ext3**. После установки раздел с неродной для ОС Windows файловой системой появляется как еще один дополнительный диск. В процессе установки пользователю будет предложено указать желаемую букву диска подключаемого раздела **Linux** (см. Рисунок 1).

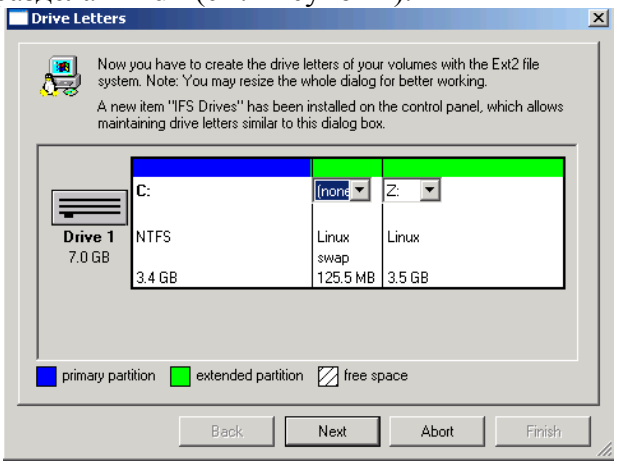


Рисунок 1. Выбор буквы диска

Утилита **Explore2fs** - программа для ОС **Windows**, предназначенная для доступа к разделам с файловыми системами **ext2/ext3** в режиме чтения (см. Рисунок 2).

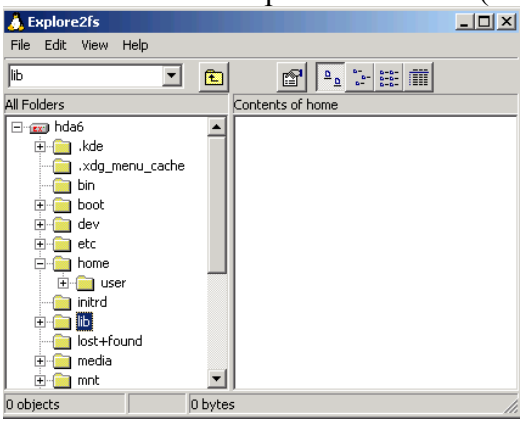


Рисунок 2. Интерфейс программы Explore2fs

Иерархия каталогов

Практически всегда файлы на дисках объединяются в *каталоги*.

В простейшем случае все файлы на данном диске хранятся в одном каталоге. Такая одноуровневая схема использовалась в **CP/M** и первых версиях **MS-DOS**. Сегодня её можно встретить, например, в некоторых цифровых фотоаппаратах: все сделанные фотографии складываются в один каталог. Иерархическая файловая система со вложенными друг в друга каталогами впервые появилась в **UNIX**.

```
Wiki.txt
Tornado.jpg
Notepad.exe
```

(Одноуровневая файловая система)

Каталоги на разных дисках могут образовывать несколько отдельных деревьев, как в **DOS/Windows**, или же объединяться в одно дерево, общее для всех дисков, как в **UNIX**-подобных системах.

```
C:
 \Program files
    \CDEx
        \CDEx.exe
        \CDEx.hlp
        \mppenc.exe
 \Мои документы
    \Wiki.txt
    \Tornado.jpg
D:
 \Music
    \ABBA
        \1974 Waterloo
        \1976 Arrival
           \Money, Money, Money.ogg
        \1977 The Album
```

(Иерархическая файловая система Windows/DOS)

В **UNIX** существует только один корневой каталог, а все остальные файлы и каталоги вложены в него. Чтобы получить доступ к файлам и каталогам на каком-нибудь диске, необходимо примонтировать этот диск командой mount. Например, чтобы открыть файлы на CD, нужно, говоря простым языком, сказать операционной системе: «возьми файловую систему на этом компакт-диске и покажи её в каталоге /mnt/cdrom». Все файлы и каталоги, находящиеся на CD, появятся в этом каталоге /mnt/cdrom, который называется точкой монтирования (англ. mount point). В большинстве UNIX-подобных систем съёмные диски (дискеты и CD), флэш-накопители и другие внешние устройства хранения данных монтируют в каталог ***/mnt, /mount или /media***. **UNIX** также позволяет автоматически монтировать диски при загрузке операционной системы.

```
/bin
  /ls
/mnt
  /cdrom
    /Music
       /ABBA
         /1974 Waterloo
         /1976 Arrival
            /Money, Money, Money.ogg
         /1977 The Album
  /floppy
/home
  /peter
    /Wiki.txt
    /tornado.jpg
```

(Иерархическая файловая система UNIX)

Кроме того, следует отметить, что вышеописанная система позволяет монтировать не только файловые системы физических устройств, но и отдельные каталоги (параметр --bind) или, например, образ ISO (опция loop).

Выполнение работы

Задание 1. Установите параллельно с Windows XP другую ОС (OpenSUSE).

1. Подключите к созданной ранее ВМ **VM-1** образ загрузочного диска ОС ***Mandriva Linux*** (***mandriva.iso***).
2. Запустите ВМ.
3. Активизируйте *режим загрузки с оптического привода*.
4. Следуйте указаниям из *задания 1* в *лабораторной работе 1.2* до пункта *8* включительно.
5. Удалите из списка устанавливаемого программного обеспечение Игры, Мультимедийные компоненты, Графические пакеты, Эффекты рабочего стола и Офисное программное обеспечение:
   - откройте диалоговое окно ***Выбор программного обеспечения***, щелкнув по ссылке ***Программное оебспечение***;

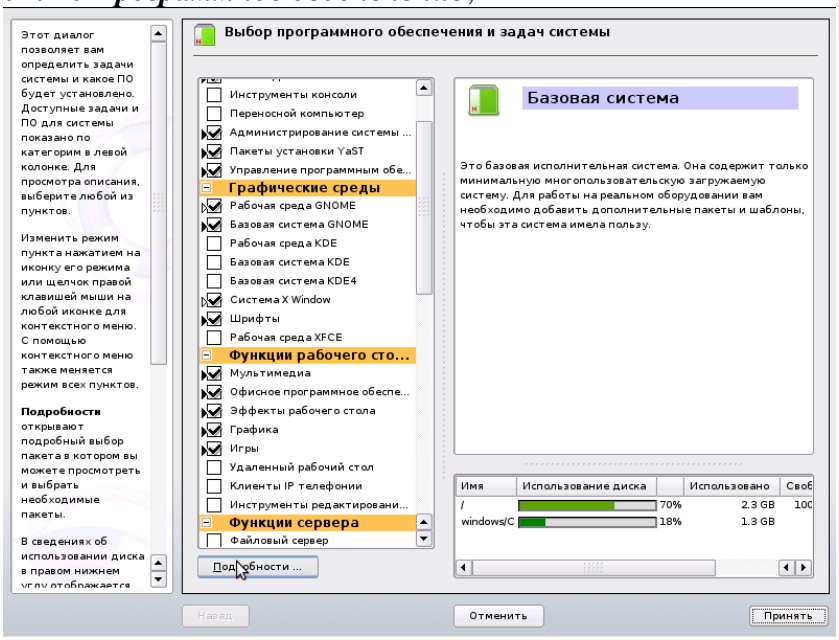


Рисунок 3. Выбор программного обеспечения.

   - сбросьте в списке программного обеспечения следующие флажки: ***Мультимедиа***, ***Офисное программное обеспечение***, ***Эффекты рабочего стола***, ***Графика***, ***Игры***;
   - подтвердите изменения кнопкой ***Принять***;
6. Дале следуйте указаниям из *задания 1* в *лабораторной работе 1.2* с пункта *9* и до конца.

Задание 2. Установите фоновое изображение рабочего стола в OpenSUSE.

Используйте ВМ, запущенную в предыдущем задании.

1. Откройте окно Мой компьютер с помощью ярлыка на рабочем столе.

Рисунок 7. Ярлык Мой компьютер.

2. Перейдите на раздел с файлами ОС **Windows XP** - ***3.4 G Media ntfs*** (Рисунок 8.).

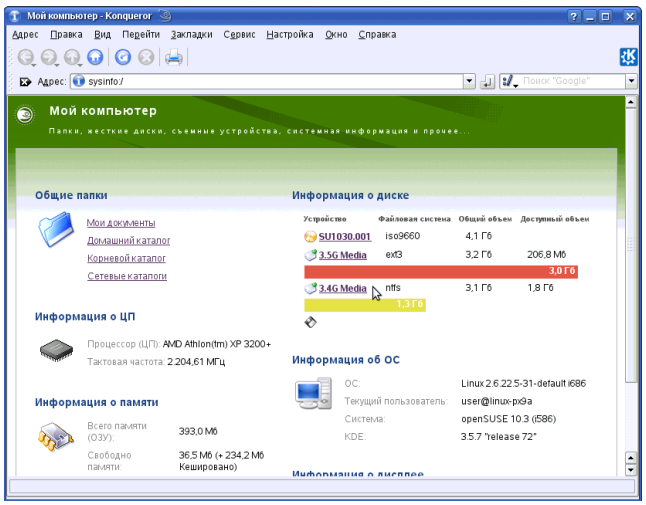


Рисунок 8. Выбор раздела с установленной ОС Windows.

3. Перейдите в папку с образцами рисунков ***(Documents and Settings/All Users/Документы/Мои рисунки/Образцы рисунков)***.

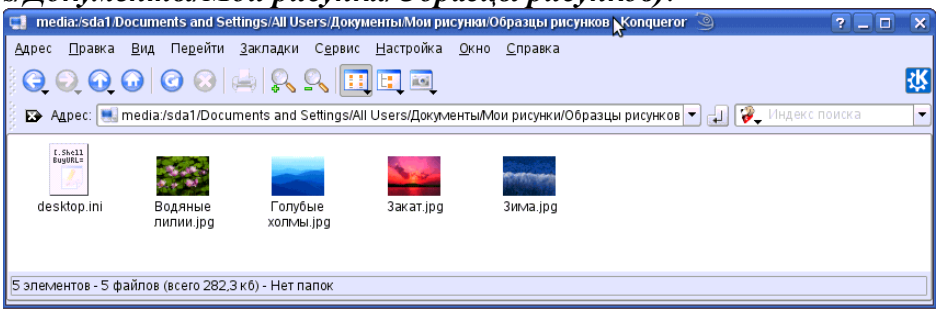


Рисунок 9. Папка с образцами рисунков.

4. Установите рисунок ***Закат.jpg*** в качестве фонового изображения рабочего стола:
   - скопируйте файл в домашний каталог:
     - выполните команду **Копировать** (***Контекстное меню/Копировать***);
     - перейдите в домашний каталог с помощью кнопки **Домой**  на панели инструментов;
     - вставьте скопированное изображение (***Правка/Вставить***);
   - установите скопированный рисунок в качестве фона рабочего стола (***Контекстное меню/Действия/Сделать фоновым рисунком/По центру***).
5. Создайте снимок экрана ВМ с установленным фоном рабочего стола и сохраните в личной папке.
6. Завершите работу виртуальной машины (***Меню KDE/Выйти/Остановить компьютер/Подтвердить***).

Задание 3. Измените фоновое изображение рабочего стола в ОС Windows XP.

1. Установите в ОС ***Windows*** драйвер для работы с файловой системой **ext3**:
   - подключите к ВМ образ диска с программным обеспечением к лабораторным работам;
   - установите драйвер файловых систем **ext2/ext3** (***Ext2IFS_1_10c.exe***).
     *В ходе установки будет предложено указать букву диска (например **Z**), под которой будет доступен раздел ОС **Linux**.*
2. Установите в качестве фона рабочего стола произвольную картику:
   - откройте раздел с **LINUX** (***Мой компьютер\Z:\share\walpapers***);
   - выделите изображение и выполните команду контекстного меню **Сделать фоновым рисунком рабочего стола**.
3. Создайте снимок экрана ВМ с установленным фоном рабочего стола и сохраните в личной папке.

4. Завершите работу виртуальной машины.

Лабораторная работа
Сетевые адаптеры

Цель: научиться определять параметры сетевого адаптера, настраивать и устанавливать его.

Средства для выполнения работы:

- аппаратные: компьютер, подключенный к локальной вычислительной сети (ЛВС), сетевой адаптер, витая пара.
- программные: ОС Windows XP.

Теоретические сведения

Сетевые адаптеры (СА) или *интерфейсные карты (NIC - Network Interface Card)*, служат для подключения компьютеров к локальной вычислительной сети (ЛВС).

Основные функции СА: организация приема/передачи данных из/в компьютер, согласование скорости приема/передачи информации (буферизация), формирование пакета данных, параллельно-последовательное преобразование (конвертирование), кодирование/декодирование данных, проверка правильности передачи, установление соединения с требуемым абонентом сети, организация собственно обмена данными.

Классификации сетевых адаптеров:

По среде передачи данных:

- проводные (витая пара, коаксиальный кабель, оптоволокно);
- беспроводные (инфракрасная связь, Bluetooth, wireless LAN).

По выполняемым функциям СА:

- реализующие функции физического и канального уровней. Такие адаптеры, выполняемые в виде интерфейсных плат, отличаются технической простотой и невысокой стоимостью. Они применяются в сетях с простой топологией, где почти отсутствует необходимость выполнения таких функций, как маршрутизация пакетов, формирование из поступающих пакетов сообщений, согласование протоколов различных сетей и др.
- реализующие функции первых четырех уровней базовой модели взаимодействия открытых систем ***OSI (Open System Interconnection)*** - физического, канального, сетевого и транспортного. Эти адаптеры, кроме функций СА первой группы, могут выполнять функции маршрутизации, ретрансляции данных, формирования пакетов из передаваемого сообщения (при передаче), сборки пакетов в сообщение (при приеме), согласования протоколов передачи данных различных сетей, сокращая таким образом затраты вычислительных ресурсов ЭВМ на организацию сетевого обмена. Технически они могут быть выполнены на базе микропроцессоров.

По топологии ЛВС адаптеры разделяются на группы, поддерживающие различные топологии ЛВС: шинную; кольцевую; звездообразную; древовидную; комбинированную.

По принадлежности к типу компьютера:

- адаптеры для клиентских компьютеров;
- адаптеры для серверов.

В адаптерах для клиентских компьютеров значительная часть работы по приему и передаче сообщений перекладывается на программу, выполняемую в ПК. Такой адаптер проще и дешевле, но он дополнительно загружает центральный процессор компьютера. Адаптеры для серверов снабжаются собственными процессорами, выполняющими всю нужную работу.

Основные характеристики СА:

- установленная микросхема контроллера (микрочип);

- разрядность - имеются 8-, 16-, 32- и 64-битные сетевые карты (определяется микрочипом);
- скорость передачи - от 10 до 1000 Мбит/с (наиболее популярные 100 Мбит/с);
- тип подключаемого кабеля - коаксиальный кабель толстый и тонкий, неэкранированная витая пара, волоконно-оптический кабель;
- поддерживаемые стандарты передачи данных - **Ethernet, IEEE 802.3, Token Ring, FDDI** и т. д.

Микросхема контроллера имеет важнейшее значение, она определяет многие параметры адаптера, в том числе надежность и стабильность работы.

На сетевых картах может быть установлен также чип ПЗУ BootROM, обеспечивающий возможность удаленной загрузки операционной системы с сервера сети, то есть использовать сетевой компьютер без дисковой памяти.

Выполнение работы

Задание 1. Определите тип сетевой карты (тип шины, тип среды для передачи данных).

1. Осмотрите сетевую карту. Определите *тип шины*, к которой она подключается (для этого посмотрите на ту часть сетевой карты, которая имеет контакты):
   - карта подключается к шине **PCI (*Peripheral Component Interconnect* -** соединение периферийных компонент), если длина контактной пластины *менее 10 см*;
   - карта подключается к шине **ISA (*Industry Standard Architecture* -** стандартная промышленная архитектура), если длина контактной пластины *более 10 см*.
2. Определите *тип физической среды*, с которой работает сетевая карта. Посмотрите на металлическую пластину, к которой крепится карта.
   Круглый коннектор свидетельствует о том, что эта карта для коаксиального кабеля; разъем RJ-45 - для работы с витой парой.
3. Визуально определите на карте наличие микросхемы для загрузки компьютера по сети.

Задание 2. Установите сетевой адаптер в компьютер.

1. Выключите компьютер и откройте системный блок.
2. Вставьте сетевую карту в соответствующий разъем на материнской плате и закрепите ее в корпусе.
3. Закройте системный блок и включите компьютер.
   *В процессе загрузки ОС определяет подключенное оборудование. Если сетевая карта соответствует стандарту **Plug and Play**, то она будет найдена ОС и автоматически настроена. Если ОС не сможет определить установленную сетевую карту, то потребуется вручную установить ее драйвера.*
4. Проверьте установку сетевой карты:
   - откройте диалоговое окно **Диспетчер устройств** (***Пуск/Панель управления/Система/Оборудование/Диспетчер устройств***);
   - раскройте список ***Сетевые платы***
   - Если в этом списке есть название адаптера, то установка прошла успешно.

Задание 3. Изучите параметры сетевого адаптера.

1. Откройте окно параметров сетевого адаптера (воспользуйтесь ***Диспетчером устройств***);
2. Определите *физический* (***MAC, Medium Access Control*** - управление доступом к носителю) адрес сетевой карты помощью команды ***ipconfig***:
   - запустите *консоль* (командную строку) любым способом (например, ***Пуск/Программы/Стандартные/Командная строка***);
   - введите команду ***ipconfig*** с параметром **all**;
   - в полученном списке найдите строку *Физический адрес*.

- Физический адрес и будет являтся ***MAC-адресом*** сетевого адаптера.

Например, выведенный системой список может выглядеть так:

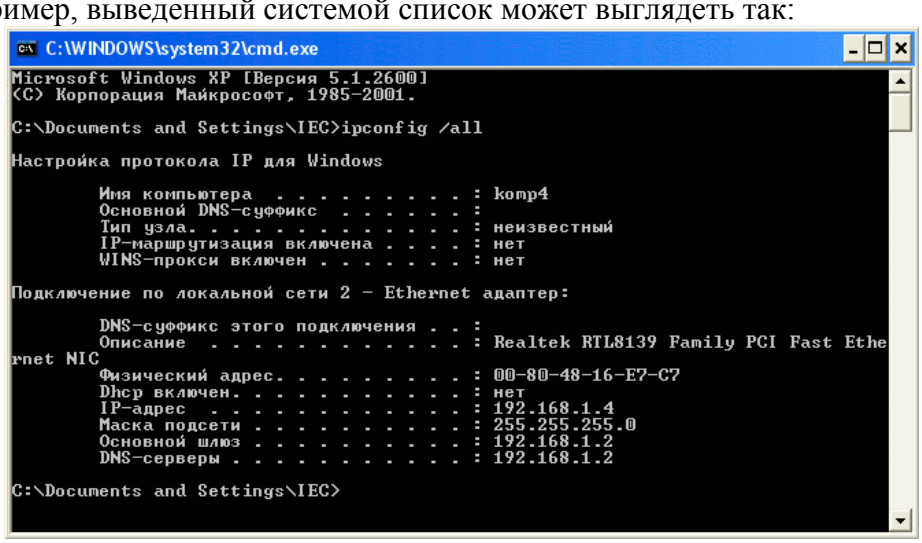


Рисунок 1. Результат работы команды ***ipconfig /all***

Лабораторная работа
Тема: Конфигурирование DHCP Server

Цели работы:

- научиться устанавливать и удалять DHCP-сервер;
- научиться настраивать область действия DHCP-сервера;
- научиться выполнять резервирование адресов.

Примечание. Если виртуальная машина подключена к сетевому адаптеру на физическом компьютере (не Microsoft Loopback Adapter), т. е. имеет выход в реальную сеть, перед выполнением работы необходимо отключить физический компьютер от сети, потому что установка DHCP-сервера на виртуальной машине может вызвать ошибки в работе реальной сети.

Целью данной лабораторной работы является установка DHCP-сервера для локальной сети факультета. Значение адреса узла, на котором будет работать DHCP-сервер, равно 192.168.1.1 и зарезервировано, а диапазон динамически выдаваемых адресов 192.168.1.11 - 192.168.1.100.

План

Задание 1. Назначить серверу сетевые параметры.

Указания к выполнению

1. Запустите виртуальную машину с Microsoft Windows Server 2003. Будем называть эту машину сервером сети.

2. Назначьте виртуальной машине IP-адрес 192.168.1.1, маска подсети 255.255.255.0.

3. Проверьте с помощью утилиты IPconfig правильность настройки сетевых параметров.

4. На физическом компьютере проверьте доступность виртуальной машины с помощью утилиты ping.

Задание 2. Установите DHCP-сервер на виртуальной машине.

Указания к выполнению

1. Для установки DHCP-сервера проделайте следующие действия1:

- Откройте Control Panel (Панель управления), затем Add/Remove Programs (Установка и удаление программ).
- На вкладке Add/Remove Windows Components (Установка компонентов Windows)

найдите Networking Services (Сетевые службы) и нажмите Details (Состав).

- Поставьте галочку около Dynamic Host Configuration Protocol (Протокол Динамической конфигурации хостов) и подтвердите свой выбор.
- Дождитесь завершения установки сервера.

2. Проверьте, что после установки сервера в меню Administrative Tools (Администрирование) добавилась новая оснастка - DHCP. Эта оснастка используется для настройки DHCP-сервера. Если в оснастке DHCP нет вашего сервера, то в меню нужно выбирать команду Add server (Добавить сервер), а затем указать имя DHCP-сервера или найти его с помощью клавиши Browse (Обзор).

3. Запуск и остановка DHCP-сервера производятся при помощи пункта контекстного меню DHCP-сервера All tasks (Все задачи).

4. Заметьте, что перед использованием DHCP-сервера в сети с установленной службой каталога Active Directory, его нужно авторизовать1.

Задание 3. Создать область действия DHCP-сервера со следующим диапазоном IP-адресов: 192.168.1.11 - 192.168.1.100.

Указания к выполнению

1. Запустите оснастку DHCP.
2. В контекстном меню конфигурируемого DHCP-сервера выберите пункт New Scope (Создать область).
3. В окне Scope Name (Имя области) определите имя для создаваемой области действия и дайте ей краткое описание. Используйте понятные имена, которые позволяют легко определить область действия в том случае, если на DHCP-сервере хранится несколько областей.
4. В окна мастера IP Address Range (Диапазон адресов) определите пул IP-адресов, для которых создается область действия. Пул задается путем указания начального (192.168.1.10) и конечного адреса (192.168.1.100) диапазона. Также указывается маска подсети (255.255.255.0).
5. В окне Add Exclusions (Добавление исключений) можно определить исключения из только что определенного диапазона, при этом можно исключать как отдельные адреса, так и целые диапазоны. Для исключения одиночного IP-адреса необходимо указать его в поле Start IP address (Начальный IP-адрес). Поле End IP address (Конечный IP-адрес) необходимо оставить в этом случае пустым. После нажатия кнопки Add (Добавить) введенный адрес будет добавлен в список исключенных из диапазона адресов.
6. В окне Lease Duration (Время аренды) определяется время аренды IP-адресов (по умолчанию - 8 дней).
7. На следующей странице мастера будет задан вопрос - требуется ли определить опции DHCP для создаваемой области действия непосредственно в ходе работы мастера или это будет сделано администратором впоследствии. Определите опции сразу же:
   - IP address of router (Адрес шлюза по умолчанию) - поставьте адрес сервера (нажмите клавишу Add, чтобы он появился в списке);
   - DNS server (DNS сервер) - добавьте адрес сервера;
   - WINS server - добавьте адрес сервера или оставьте пустым, если служба WINS в сети не работает.
8. В конце работы мастера необходимо выбрать Yes, activate scope now (Активизировать область действия сейчас).
9. Если служба DHCP-сервера функционирует нормально, на значке сервера должна появиться зеленая стрелка. Красная стрелка указывает, что служба не работает, в этом случае следует обновить информацию о сервере (контекстное меню сервера - Refresh) или перезапустить службу (контекстное меню сервера - All Tasks - Restart).

Задание 4. Проверить работу DHCP-сервера.

Указания к выполнению

1. Запустите виртуальную машину с Microsoft Windows XP. Эта машина будет являться DHCP-клиентом, будем называть её рабочей станцией.

2. Настройте рабочую станцию на автоматическое получение IP-адреса и имени DNS-сервера.

- Откройте окно свойств Подключение по локальной сети и выберите Протокол Интернета (TCP/IP).
- Установите переключатель в положение Получить IP-адрес автоматически.

3. Выполните утилиту IPconfig с ключом /renew, а затем с ключом /all, и убедитесь в том, что рабочая станция получила сетевые параметры от DHCP-сервера.

Задание 5. Зарезервируйте для рабочей станции постоянный IP-адрес 192.168.1.20.

Указания к выполнению

1. Запустите оснастку DHCP.

2. Для просмотра текущих аренд откройте раздел Address Leases (Аренды адресов) и найдите аренду для рабочей станции.

3. Определите MAC-адрес станции (столбец Unique ID) и запишите его.

4. В контекстном меню раздела Reservations (Резервирования) выбираем New reservation… и вводим параметры - имя резервирования, необходимый IP-адрес (192.168.1.20), MAC-адрес станции.

5. На рабочей станции выполните утилиту IPconfig с ключом /renew, а затем с ключом /all, и убедитесь в том, что рабочая станция получила зарезервированный IP-адрес от DHCP-сервера.

Задание 6. Зарезервируйте для рабочей станции адрес вне текущей области действия DHCP-сервера.

Указания к выполнению

1. Выполните резервирование для рабочей станции IP-адреса вне области действия DHCP-сервера, например, 192.168.1.200.

2. Проверьте на рабочей станции, получила ли она новые параметры.

Задание 7. Настройте мониторинг DHCP-сервера.

Указания к выполнению

1. Служба DHCP-сервера ведет мониторинг своих действий, записывая их в журнал (audit logging). Этот журнал можно использовать при решении проблем с DHCP-сервером.

2. Чтобы включить журнал, откройте окно свойств DHCP-сервера (контекстное меню сервера - Properties). На вкладке General (Общие) выберите пункт Enable DHCP audit logging (Разрешить мониторинг DHCP).

3. Файлы журнала находится в следующем каталоге: C:\Windows\system32\dhcp. Файлы создаются ежедневно и называются по следующему принципу: к постоянному имени DhcpSrvLog добавляется
обозначение дня недели, например, журнал понедельника называется DhcpSrvl_og-Mon.log.

4. Просмотрите файл журнала за текущий день. В начале журнала приводятся значения кодов событий. Затем указывается точное время и краткое описание события.

5. Найдите в журнале записи, соответствующие вашим действиям в этой лабораторной работе.

Контрольные вопросы

Установите диапазон адресов для DHCP-сервера 172.16.0.1 -172.16.0.10, маска подсети 255.240.0.0. Проверьте работу DHCP-сервера.

Установите зарезервированный за рабочей станцией IP-адрес 172.16.0.20. Проверьте получение станцией адреса.

Используйте вкладку альтернативной конфигурации рабочей станции на случай отключения службы DHCP. Протестируйте полученные настройки.

Что такое автоматические частные адреса? Протестируйте их получение и работу сети в случае, если DHCP-сервер оказывается недоступным.

Лабораторная работа.
Тема: Настройка параметров DHCP Server

Цель работы. Изучить процесс установки, авторизации сервера DHCP, создания области и настройки параметров области

План

Исходная конфигурация компьютера

Компьютеры с операционной системой Windows 2003 Server с созданными контроллерами домена.

Результат

Сервер с установленной и настроенной службой DHCP

Краткие сведения

Общие сведения о службе DHCP.
Описание последовательности выполняемых действий.
Последовательность выполняемых действий
Установка службы DHCP
Авторизация сервера DHCP в Active Directory
Создание области и настройка параметров сервера DHCP

Лабораторная работа
Тема: Конфигурирование службы DNS Server

Цель работы. *Цель данной работы – научиться конфигурировать и тестировать службу имен для корпоративной сети на основе сервера DNS bind.*

Краткие теоретические сведения

Служба имен в Интернете

Служба доменных имён DNS является важнейшей системной службой в TCP/IP сетях. Назначение DNS – преобразование символьных имен в IP адреса и наоборот, а так же предоставление дополнительной информации о хостах и группах хостов (доменах), такой как адреса почтовых обменников, публичные ключи служб и т.п. В сети Интернет служба DNS оперирует распределённой иерархической базой данных в виде дерева имен, находящейся на множестве различных хостов. Ответственность за корректность базы данных в каждом узле дерева возлагается на администратора соответствующего домена. В сети Интернет корнем дерева является домен ".". Полное - абсолютное или полностью определенное, fully qualified domain name - доменное имя заканчивается точкой, обозначающей корень доменного дерева, но часто эта завершающая точка опускается. Анализ имени производится справа налево. Самая правая секция имени характеризует страну (для каждой страны мира выделен свой домен с двух символьным именем в соответствии со стандартом ISO, например, ua – Украина, ru – Россия, uk – Англия и т.п.) или характер организации (образовательная, коммерческая, правительственная и т.п.). Таим образом, домены верхнего уровня (Top Level Domains, TLD) - это хорошо известные

всем домены, такие как org (бесприбыльная организация), com (коммерческая организация), gov (государственное учреждение), mil (военное предприятие или организация), edu (учебное заведение), int (международная организация), net (большая сеть) и т.д. Ответственность за TLD лежит на международной бесприбыльной организации Internet Corporation for Assigned Names and Numbers (ICANN, www.icann.org). Ниже по дереву имен расположены домены второго и последующих уровней. В некоторых странах существуют домены, подобные исторически первым TLD, например, org.ua, gov.ua, edu.ua и т.п. В Украине для каждой области выделены двухбуквенные домены, такие как cn.ua – Чернигов, dp.ua – Днепропетровск, и т.д., хотя исторически сложившиеся домены, такие как kiev.ua, kharkov.ua, chernigov.ua, тоже поддерживаются. Маленький фрагмент интернетовской иерархии имен показан на рисунке 1. Число уровней реально больше, но обычно не превышает 5.
Таким образом, в службе DNS каждый сервер отвечает за определенную зону (зона ответственности) - т.е. свою часть дерева доменных имен, хранит соответствующие базы данных и отвечает на запросы. При этом вышестоящие по дереву серверы имеют информацию об адресах нижестоящих серверов, что обеспечивает связность дерева. Говорят, что вышестоящий сервер делегирует нижестоящему серверу полномочия по обслуживанию определенной зоны. Важно понимать различие между доменом и зоной. Домен - это поддерево дерева доменных имен. Зона - это часть дерева, за которую отвечает тот или иной DNS-сервер.

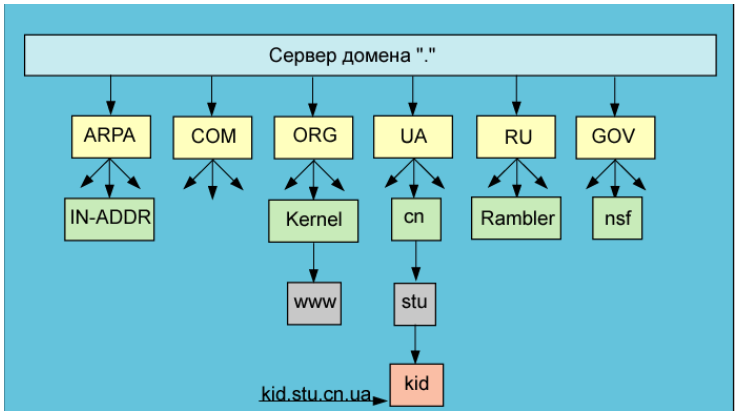


Рисунок 1 – Фрагмент иерархии имен в Интернет

За каждую зону DNS отвечает не менее двух серверов. Один из них является первичным, primary, или, в новой терминологии — master. остальные - вторичными, secondary, или slave. Первичный сервер содержит оригинальные файлы с базой данных DNS для своей зоны. Вторичные серверы получают эти данные по сети от первичного сервера и периодически запрашивают первичный сервер на предмет обновления данных. Признаком обновления данных служит увеличение серийного номера в записи SOA – см ниже. В случае, если данные на первичном сервере обновлены, вторичный сервер запрашивает "передачу зоны" ("zone transfer")- т.е. базы данных требуемой зоны. Передача зоны происходит с помощью протокола TCP, порт 53, в отличие от запросов, которые направляются на UDP/53.
Изменения в базу данных DNS могут быть внесены только на первичном сервере. С точки зрения обслуживания клиентских запросов первичные и вторичные серверы идентичны. Рекомендуется, чтобы первичный и вторичные серверы находились в разных сетях - для увеличения надежности обработки запросов на случай, если сеть одного из серверов становится недоступной. Серверы DNS не обязаны находиться в том домене, за который они отвечают.

Вторичный сервер необязательно получает данные непосредственно с первичного сервера; источником данных может служить и другой вторичный сервер. В любом случае сервер-источник данных для данного вторичного сервера называется "главным" ("master").
У каждого домена есть свои “писаные правила”, именуемые “полиси”, в соответствии с которыми можно получить имя хоста или субдомена (чаще говорят “зоны”) в данном домене. Самым простым примером таких правил могут служить полиси домена com. Если данное имя не зарегистрировано или не находится в процессе регистрации, то по уплате определенной суммы любое физическое или юридическое лицо может получить это имя от регистратора домена com.
Процесс получения собственного домена называется “делегирование”, что, собственно, и отражает суть действий: субдомен передается в полное управление его администратору. Для получения субдомена в каком-то домене необходимо в соответствии с полиси обратится к регистратору, выполнить формальные процедуры, а так же ряд технических действий по настройке сервера DNS, которые, собственно и являются предметом данной лабораторной работы.
Различают 3 режима работы сервера DNS:
master (primary). Данный режим используется администратором зоны, файлы баз данных ведутся вручную на этом сервере. Данный сервер является абсолютным авторитетным источником информации для данной зоны;
slave (secondary). Данный режим используется по просьбе администратора зоны, которая автоматически регулярно копируется с master сервера. Данный сервер является авторитетным источником информации для данной зоны;
hint (caching). Режим кэширования всех запросов, попадающих в определённую зону, обычно “.”, т.е. кэшируются все запросы. Такой сервер обычно используется для ускорения работы с сетью.

Для каждой зоны, обслуживаемой данным сервером, может быть выбран тот или иной режим. Обычно для зоны “.” все сервера конфигурируются по типу hint, что позволяет кешировать все запросы пользовательских рабочих станций на время жизни конкретной записи DNS. Это значительно ускоряет обработку локальных запросов.
База данных DNS для каждого домена в простейшем случае представляет собой набор текстовых файлов, которые системный администратор ведет на главном сервере имен этого домена. В этих файлах содержатся директивы синтаксического анализатора ($ORIGN, $TTL) и записи о ресурсах.

Записи ресурсов в базе данных домена

Файл любой зоны начинается с записи Start Of Authority, ***SOA***. Эта запись является заголовочной и содержит информацию о размещении зоны, о почтовом адресе ответственного лица и о базовых временных параметрах записей данной зоны.
Файл прямой зоны содержит стандартные записи ресурсов базы данных DNS для преобразования доменных имен хостов в данной зоне в IP-адреса, определения авторитарных DNS-серверов данной зоны, определения хостов-обработчиков почты для доменных имен в данной зоне и др.
Файлы баз данных DNS состоят из стандартных записей ресурсов. В общем виде стандартная запись ресурса связывает данные определенного типа с некоторым именем и формируется по шаблону:
имя [время_жизни_записи] IN тип_записи данные
Именем является некоторое доменное имя (необязательно имя физически существующих хоста или домена). Если поле "имя" пусто, то значение этого поля берется из предыдущей записи. Данными может быть, например, IP-адрес хоста, если имя относится к хосту, или DNS-сервер домена, если имя относится к домену, и т.п.

Время жизни записи определяет время хранения информации этой записи в кэше запросившего запись сервера в секундах и указывается, только если оно отличается от времени жизни, определенного для всей зоны в записи SOA.
Основные типы записей:
SOA (Start Of Authority) - заголовок зоны;
NS (Name Server) - сервер DNS;
A (Address) - IP-адрес для хоста;
MX (Mail Exchanger) - почтовый обменник;
CNAME (Canonical Name) - каноническое имя, псевдоним хоста;
PTR (Pointer) - указатель по обратной зоне, фактически — имя хоста;
Прямая зона DNS.
Рассмотрим примеры файлов базы данных DNS. Первой рассмотрим прямую зону для приватной части корпоративной сети, домен “stu.”, файл db.stu.

```
$ORIGIN .
stu 28800 IN SOA ns.stu. dnsmaster.stu. (
                                2005033100 ; Serial
                                28800 ; Refresh
                                7200 ; Retry
                                604800 ; Expire
                                86400 ; Time To Live)
; authoritative name servers for zone
28800 IN NS ns.stu.
28800 IN NS ns1.stu.
; mail exchangers for entire zone
28800 IN MX 10 stalker.stu.
28800 IN MX 20 cs.stu.
$ORIGIN stu.
; name servers glue records
ns IN A 192.168.0.10
ns1 IN A 192.168.0.14
;servers
dragon IN A 192.168.0.17
auth IN CNAME dragon.stu.
cs IN A 192.168.0.14
stalker IN A 192.168.0.10
www IN CNAME stalker.stu.
mail IN CNAME stalker.stu.
ftp IN CNAME stalker.stu.
www.docs IN CNAME cs.stu.
kid IN A 192.168.0.12
; workstations
ie-21-7 IN A 192.168.3.40
ie-21-8 IN A 192.168.3.41
ie-21-9 IN A 192.168.3.42
vc-105-1 IN A 192.168.66.2
```

Первая строка – это макрос, говорящий, что все имена далее следуют непосредственно за доменом “точка”. Таким образом, для приватной сети мы используем имена в нашем приватном дереве относительно нашего собственного корня “.”. Следует помнить, что для сервера, разрешающего одновременно и имена в корпоративной сети, и имена в интернете, имя зоны следует выбирать из 3-х символов, не совпадающих с именами TLD.

Первой записью всегда идет ***SOA*** (Start of Authority), в которой указывается имя зоны (“stu.”, или макрос @), TTL, т.е. время жизни этой записи, дальше – ключевые слова IN (Internet records) и ***SOA***. Далее идут параметры зоны: имя основного сервера DNS, почтовый адрес администратора зоны, однако вместо символа “@” там стоит точка, поскольку @ - это ссылка на имя зоны. Сразу за открывающейся скобкой находится серийный номер данного файла, обычно в формате ггггммддNN. Серийный номер необходимо увеличивать при каждом изменении файла, что бы ведомые сервера идентифицировали изменения и обновили файлы баз данных с главного сервера. Далее следуют стандартные времена в секундах для данной зоны:
Refresh – время, по истечении которого вторичные сервера должны обновить данные с первичных серверов (zone transfer);
Retry – время, через которое вторичные сервера должны совершить повторную попытку обновления, если предыдущая попытка не удалась;
Expire – время, через которое вторичные сервера должны выбросить запись о зоне и считать ее недоступной, если обновления не удались.
TTL – стандартное время жизни записей из данной зоны для кеширующих серверов.
Следующая группа записей является так же обязательной и указывает на авторитетные сервера имен для данной зоны - записи типа ***NS***. Авторитетным является сервер, на котором информация соответствует реальному состоянию зоны, т.е. регулярно обновляется (см. выше). Крайне желательно, чтобы имена, указанные в этой секции, имели соответствующие адресные ***IN A*** записи в этой же базе данных.
Ниже следует секция почтовых обменников, т.е. записи типа ***MX*** (Mail Exchanger). Они указывают на сервера электронной почты, способные принимать почту для всего домена по протоколу SMTP. Чем меньше цифра перед именем, тем больший приоритет имеет данный почтовый сервер. Как правило, запись с наивысшим приоритетом относится к серверу, на котором почта заканчивает свой путь, а другие записи относятся к серверам-релеям, на которых почта может сохраняться некоторое время, пока основной почтовый сервер для зоны не доступен. Естественно, записи ***MX*** на релеи нельзя расставлять произвольно, поскольку релей обязательно должен быть сконфигурирован для приёма почты данного домена. При отсутствии записи MX для какого-либо доменного имени, почта, адресованная с этим доменным именем, будет доставляться непосредственно на хост, имеющий такое имя. Однако, такого хоста может не быть, в этом случае почта вернется отправителю с сообщением об ошибке.
Ниже, после макроса “$ORIGIN stu.”, задающего суффикс для всех записей ниже, следуют записи типа ***IN A***, предназначенные для задания соответствия между именем хоста в зоне и его IP адресом.
Для задания псевдонимов хостам используется запись ***CNAME*** (Canonical Name). Псевдонимы удобны для указания на стандартные сервисы, такие как www, mail, ftp, а так же для задания псевдонимов, используемых для создания виртуальных серверов (см. www, docs).
Рассмотрим теперь файл зоны stu.cn.ua. Данная зона мало чем отличается от предыдущей зоны внешне.

```
$ORIGIN .
stu.cn.ua 28800 IN SOA ns.stu.cn.ua. nsmaster.stu.cn.ua(
                                    2005033100 ; Serial
                                    28800 ; Refresh
                                    7200 ; Retry
                                    604800 ; Expire
                                    86400 ; Time To Live
                                    )
```

```
; authoritative name servers for zone
IN NS ns.stu.cn.ua.
IN NS ns1.stu.cn.ua.
IN NS ns.cn.ua.
; mail exchangers for entire zone
IN MX 10 stalker.stu.cn.ua.
IN MX 15 cs.stu.cn.ua.
IN MX 20 relay1.cn.ua
; name servers glue records
ns.cn.ua IN A 212.86.96.10
$ORIGIN stu.cn.ua.
ns IN A 195.69.76.130
ns1 IN A 195.69.76.134
;servers
dragon IN A 195.69.76.137
auth IN CNAME dragon.stu.cn.ua.
cs IN A 195.69.76.134
stalker IN A 195.69.76.130
www IN CNAME stalker.stu.cn.ua.
mail IN CNAME stalker.stu.cn.ua.
ftp IN CNAME stalker.stu.cn.ua.
www.docs IN CNAME cs.stu.cn.ua.
; workstations
admin IN A 195.69.76.139
```

Конфигурация данной зоны практически повторяет предыдущую зону, однако отличие в том, что данная зона является субдоменом домена cn.ua. Значит, она должна быть делегирована в соответствующей зоне cn.ua примерно так, как показано в следующем фрагменте:

```
$ORIGIN cn.ua.
stu IN NS ns.stu.cn.ua.
IN NS ns1.stu.cn.ua.
IN NS ns.cn.ua.
$ORIGIN .
ns.stu.cn.ua IN A 195.69.76.130
ns1.stu.cn.ua IN A 195.69.76.134
```

Как видно из приведенного фрагмента, в “материнской” зоне cn.ua. находятся только записи о серверах имен для делегированной зоны stu.cn.ua. Управление остальной информационной базой зону передается на сервера ns.stu.cn.ua и ns1.stu.cn.ua.

Обратная зона DNS

Теперь рассмотрим файлы обратных зон, предназначенные для проведения обратного DNS-преобразования, т.е. "IP-адрес в доменное имя".

Для приватных блоков адресов, таких как 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16 никаких проблем с делегированием, в общем-то, нет, поскольку эти адреса не маршрутизируются в Интернете и нужны только внутри приватной сети.

```
$ORIGIN .
0.168.192.IN-ADDR.ARPA. 86400 IN SOA ns.stu. dnsmaster.stu. (
                                2006060200
```

86400
14400
3600000
345600
)
86400 IN NS ns.stu.
86400 IN NS ns1.stu.
$ORIGIN 0.168.192.IN-ADDR.ARPA.
10 IN PTR stalker.stu.
14 IN PTR cs.stu.
17 IN PTR dragon.stu.
12 IN PTR kid.stu.

Стоит обратить внимание, что имя зоны состоит из развёрнутых по отношению к записи адреса цифр. Для адресного блока 192.168.0.0/24 имя зоны 0.168.192.IN-ADDR.ARPA. IN-ADDR.ARPA. - это специальный домен верхнего уровня, отведенный для делегирования обратных зон. В файле обратной зоны присутствует, конечно же, запись ***SOA***, как минимум пара записей типа ***NS*** об официальных авторитетных серверах и записи типа ***PTR*** (Pointer), ставящие в соответствие адреса и имена. Обратная зона для публичных адресов 195.69.76.0/24 приведена ниже:

$ORIGIN .
76.69.195.IN-ADDR.ARPA. 86400 IN SOA ns.stu.cn.ua dnsmaster.stu.cn.ua (2004060200
86400 14400 3600000 345600)

IN NS ns.stu.cn.ua.
IN NS ns1.stu.cn.ua.
$ORIGIN 0.168.192.IN-ADDR.ARPA.
10 IN PTR stalker.stu.cn.ua.
14 IN PTR cs.stu.cn.ua.
17 IN PTR dragon.stu.cn.ua.
12 IN PTR kid.stu.cn.ua.

Отличие данной зоны от предыдущей опять же только в том, что она является публичной и должна делегироваться в соответствии с правилами выдачи и регистрации IP адресов. Вкратце необходимо отметить следующее. Выдача блоков адресов потребителям производится локальными Интернет регистратурами (LIR), которые, в свою очередь, получают их от региональных регистратур. В Европе это – бесприбыльная организация RIPE (http://www.ripe.net/), финансируемая провайдерами. Основные функции региональных регистратур – координация использования IP адресов и, соответственно, маршрутизации в регионе. Для получения своего блока публичных адресов необходимо заполнить соответствующие формы RIPE и направить их вашему LIR.

Особенности размещения и конфигурирования серверов для корпоративной сети

Поскольку сервис DNS является критическим для функционирования сети, то в сети должно быть как минимум 2 сервера. Обычно размещают их так, как показано на рисунке 2. Для внутренней сети доступны оба сервера, а для внешней – только внешний сервер. Внутренний сервер является первичным для внутренних доменов и использует внешний в качестве форварда (forwarding server), поскольку напрямую не видит домен “.” . Внешний сервер в общем случае не должен отвечать на рекурсивные запросы извне, поскольку он может быть использован как платформа для DDoS атак на другие сервера.

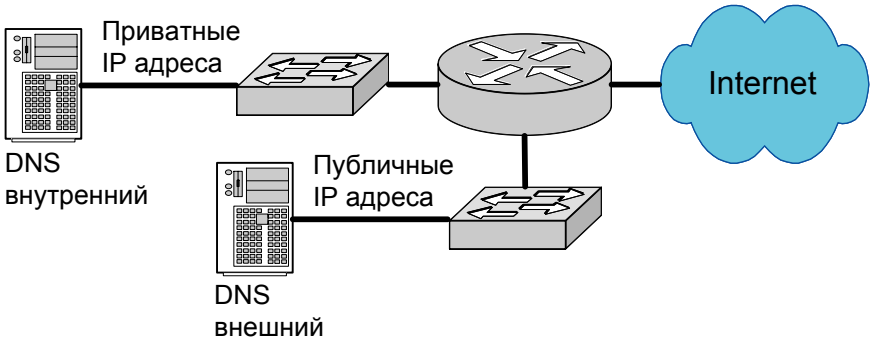


Рисунок 2 – Расположение серверов имен в сети

Установка ПО сервера DNS

Наиболее популярным ПО, реализующим сервис DNS, является сервер ***bind*** (Berkeley Internet Name Daemon), поддерживаемый Internet Software Consortium (http://www.isc.org). Существуют лёгкие реализации, предназначеные для работы в качестве кеширующих серверов, есть реализации, специфичные для конкретних коммерческих ОС, однако на практике лучше использовать bind, поскольку он распространяестя под лицензией GPL, т.е. вместе с исходным кодом, что гарантирует отсутсвие давно не исправляемых уязвимостей и прочих неприязностей закритого кода.

Пакет bind поставляется практически со всеми дистрибутивами Linux и xBSD.

Для работы сервера в ОС Fedora Linux не обходимо установить следующие пакеты: bind-utils – утилиты для работы с DNS и тестирования сервера, bind – собственно сервер, bind-chroot – файлы, необходимые для запуска сервера в индивидульном окружении в режиме chroot. Запуск сервера в этом режиме минимизирует потери при взломе системы через работающий сервис.

Проверить, утсновлены ли пакеты, можно командой

rpm –qa | grep bind

Если пакету не установлены, установите их командой

yum install bind-utils bind bind-chroot

При установке сервера автоматически создается конфигурация для кеширующего сервера зоны «.» и для первичных серверов локальних зон.

Для небольшого сервера на несколько мелких зон конфигурации зон обычно хранятся в текстових вайлах. В нашем случае – это **/var/named/chroot/var/named/*** . Для больших зон, содержащих миллионы записей, используются специальные модули хранения, которые могут сохранять данные зон в реляционных БД (PostgreSQL) либо на сервере LDAP.

Конфигурирование сервера DNS

Рассмотрим подробнее пример файла конфигурации для такого случая: наш сервер является основным для внутренней корпоративной сети 192.168.0.0 и внутреннего домена “stu.”, и кэширующим для домена “.”. Все пути, приведенные ниже, в случае работы сервера в окружении chroot, нужно понищать как относительные к **/var/named/chroot.**

Файл конфигурации **/etc/named.conf** приведен ниже:

```
options {
  directory "/etc/namedb";
  forward first;
  forwarders {
   195.69.76.130;
```

```
  };
};

// caching server for root domain
zone "." {
  type hint;
  file "named.root";
};

// it's not neccesary but good to resolve localhost
zone "0.0.127.IN-ADDR.ARPA" {
  type master;
  file "localhost.rev";
};
// private zone for our network
zone "stu" {
  type master;
  file "db.stu.private";
  allow-transfer{
    195.69.76.130;
  };
  allow-query{
    192.168.0.0/16;
  };
};
// Inverse zone for private zone stu
zone "0.168.192.IN-ADDR.ARPA" {
  type master;
  file "db.192.168.0";
  allow-transfer{
   195.69.76.130;
  };
  allow-query{
   192.168.0.0/16;
  };
};
```

В приведенном выше файле конфигурации все интуитивно понятно, однако стоит особо отметить, что сервер в DNS с адресом 195.69.76.130 используется как форвард и как вторичный сервер для внутренних доменов. Предложение ***allow-transfer*** используется для ограничения полной перекачки зоны только на вторичный сервер. Предложение ***allow-query*** указывает серверу, что отвечать на запросы по данным зонам можно только хостам из приведенного блока адресов.
Ниже приведена конфигурация второго сервера. Кроме того, он является первичным для публичных зон stu.cn.ua и 76.69.195.IN-ADDR.ARPA.

```
options {
  directory "/etc/namedb";
  forward first;
  forwarders {
    212.86.96.10;
```

```
  };
};

// caching server for root domain
zone "." {
  type hint;
  file "named.root";
};

// it's not neccesary but good to resolve localhost
zone "0.0.127.IN-ADDR.ARPA" {
  type master;
  file "localhost.rev";
};
// private zone for our network
zone "stu" {
  type slave;
  file "db.stu.private";
  master {
    192.168.0.10;
  };
  allow-query{
    192.168.0.0;
  };
};
// Inverse zone for private zone stu
zone "0.168.192.IN-ADDR.ARPA" {
  type slave;
  file "db.192.168.0";
  masters {
   192.168.0.10;
  };
  allow-query{
    192.168.0.0;
  };
};

// public zone for our network
zone "stu.cn.ua." {
  type master;
  file "db.stu.cn.ua";
  allow-transfer{
    212.86.96.10;
  };
};
// Inverse zone for public zone stu.cn.ua.
zone "76.69.195.IN-ADDR.ARPA" {
  type master;
  file "db.195.69.76";
  allow-transfer{
    212.86.96.10.
```

```
  };
};
```

Заметим, что здесь появилось предложение ***allow-query***, необходимое для того, чтобы данный сервер мог отвечать на запросы о внутренних зонах только во внутреннюю сеть. Предложение allow-transfer используется так же, как и в предыдущем случае и ограничивает полную перекачку всей зоны только серверу с адресом 212.86.96.10, который является вторичным для данной зоны. Этот же сервер используется и как форвард. Строго говоря, такой необходимости нет, но в ситуации, когда почему-то пол-Интернета не видно, а этот форвард находится в пределах досягаемости и видит весь Интернет, использование форварда оказывается оправданным.
Естественно, многие вопросы остались за пределами этого короткого обзора. Например, конфигурирование мощной системы логов сервера bind, специальные ресурсные записи и т.д.

Тестирование работы сервера имён
Тестирование работы сервера производится командой dig, которая позволяет производить произвольные запросы к указанному в командной строке серверу. Ниже приведен пример запроса к DNS серверу, расположенному на локальном компьютере на предмет записи SOA для зоны stu.

```
al@stalker$>dig @127.0.0.1 SOA stu
; <<>> DiG 8.3 <<>> @127.0.0.1 SOA stu
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12648
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2,
;; ADDITIONAL: 2
;; QUERY SECTION:
;; stu, type = SOA, class = IN
;; ANSWER SECTION:
stu. 8H IN SOA ns.stu. dnsmaster.stu. (
2005033100 ; serial
8H ; refresh
2H ; retry
1W ; expiry
1D ) ; minimum
;; AUTHORITY SECTION:
stu. 8H IN NS ns.stu.
stu. 8H IN NS ns1.stu.
;; ADDITIONAL SECTION:
ns.stu. 8H IN A 192.168.0.10
ns1.stu. 8H IN A 192.168.0.14
;; Total query time: 19 msec
;; FROM: stalker.stu.cn.ua to SERVER: 127.0.0.1
;; WHEN: Wed Sep 14 14:37:22 2005
;; MSG SIZE sent: 21 rcvd: 134
```

Разберём вывод команды. Следует отметить, что вывод содержит собственно ответ на заданный вопрос и дополнительные сведения, отмеченные как комментарии знаками “;;” в начале строки. Поскольку мы запрашивали запись SOA, то она и показана в секции

ответов. Далее следует секция авторитетности, в которой указываются авторитетные сервера для данной зоны, и, наконец, дополнительная секция, где обычно указываются IP адреса (записи IN A) для авторитетных серверов данной зоны. Ниже приведен еще один пример запроса типа A.

```
al@stalker$dig @127.0.0.1 A stalker.stu
; <<>> DiG 8.3 <<>> @127.0.0.1 A stalker.stu
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14417
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2,
;; ADDITIONAL: 2
;; QUERY SECTION:
;; stalker.stu, type = A, class = IN
;; ANSWER SECTION:
stalker.stu. 8H IN A 192.168.0.10
;; AUTHORITY SECTION:
stu. 8H IN NS ns.stu.
stu. 8H IN NS ns1.stu.
;; ADDITIONAL SECTION:
ns.stu. 8H IN A 192.168.0.10
ns1.stu. 8H IN A 192.168.0.14
;; Total query time: 3 msec
;; FROM: stalker.stu.cn.ua to SERVER: 127.0.0.1
;; WHEN: Wed Sep 14 14:47:33 2005
;; MSG SIZE sent: 29 rcvd: 112
```

Как видно из примера, кроме затребованной записи A, выданы опять же две секции об авторитетных серверах, т.е. тех серверах, где информация о данной зоне наиболее достоверна.
Если запрос попадает к кэширующему серверу, то информация о зоне в нём может быть устаревшей. Запросы для проверки обратной зоны нужно давать в форме полного имени записи PTR. См. пример ниже:

```
alukin@stalker$dig @127.0.0.1 SOA 1.1.168.192.IN-ADDR.ARPA
; <<>> DiG 8.3 <<>> @127.0.0.1 SOA 1.1.168.192.IN-ADDR.ARPA
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 22408
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1,
;;ADDITIONAL: 0
;; QUERY SECTION:
;; 1.1.168.192.IN-ADDR.ARPA, type = SOA, class = IN
;; AUTHORITY SECTION:
1.168.192.IN-ADDR.ARPA. 4D IN SOA ns.stu. dnsmaster.stu. (
2001101800 ; serial
1D ; refresh
4H ; retry
5w6d16h ; expiry
4D ) ; minimum
```

;; Total query time: 8 msec
;; FROM: stalker.stu.cn.ua to SERVER: 127.0.0.1
;; WHEN: Wed Sep 14 14:54:58 2005
;; MSG SIZE sent: 42 rcvd: 94

Ход работы

Выполнение данной лабораторной работы состоит из следующих шагов:
1. Создайте файлы зон для прямой и обратной приватной зоны. Возьмите блок адресов 172.16.X.0, где X – номер машины в классе. Сконфигурируйте первичный сервер DNS для этих зон на локальном компьютере и запустите его. Не забудьте, что все сообщения выводятся не на консоль, а в системный журнал. Сообщения удобнее всего просматривать в отдельном терминале командой:

tail -f /var/log/messages

2. Проведите тестирование созданных прямой и обратной зон при помощи команды ***dig***.
3. Проведите тестирование разрешения внешних имён вашим сервером. Запросите, например информацию о зоне slashdot.org.
4. Сконфигурируйте ваш сервер как вторичный для зон, которые создал ваш сосед по лаборатории. Произведите корректировку и проверку записей зон на предмет записей типа NS. Произведите проверку командой ***dig***, обращая особое внимание на секцию "AUTHORITY SECTION".

Содержание отчета

Отчет должен содержать файлы зон, файл конфигурации сервера и результаты проверок. Наличие комментариев и выводов необходимо.

Контрольные вопросы

Почему для корпоративных зон удобнее использовать 3-х буквенные имена?
В каком случае сервер имён считается авторитетным?
Какие параметры отвечают за время обновления зоны вторичным сервером?
Как обеспечить защиту зоны от скачивания и от просмотра?
Какая запись RR применяется при создании виртуальных серверов?
Какая запись RR задаёт почтовый обменник для всей зоны?
Кокой файл содержит адреса корневых серверов имен, необходимых для инициализации кеша и рекурсивних запросив?
Что такое рекурсивный запрос?
Как производится установка ведомого сервера для конкретной зоны?

Лабораторная работа
Тема: Настройка параметров DNS Server

Цели работы:

- научиться устанавливать службу DNS;
- научиться конфигурировать зоны DNS;
- научиться тестировать службу DNS;
- научиться применять файл HOSTS.

Дополнительные библиотеки для работы DNS сервера (требуются при его включении) лежат в \\Epam-server\teachers \net\win2003.iso это образ переписываем на диск с виртуальной машины, распаковываем. В нем находятся необходимые библиотеки.

Связь с проектом

Служба DNS предназначена для преобразования символьных доменных имен в IP-адреса и обратно. В сети, где работает служба DNS, пользователи могут без труда

обращаться к различным сетевым ресурсам по доменным именам, а не по IP-адресам. Также, устанавливая эту службу, мы готовим платформу для установки Active Directory.

Требования к отчету

Отчет должен включать скриншоты каждого шага выполнения установки и проверки работоспособности DNS-сервера.

Задание 1. Установите сервер DNS на виртуальную машину с Windows Server 2003.

Указания к выполнению

1. Выполните предварительную конфигурацию компьютера, на котором будет установлен сервер DNS: проверьте, что серверу DNS назначен статический IP-адрес (например, 192.168.1.1).

2. Для установки сервера DNS воспользуйтесь одним из двух способов.

1-й способ.

- Откройте Control Panel (Панель управления), затем Add/Remove Programs (Установка/удаление программ).
- На вкладке Add/Remove Windows Components (Установка/удаление компонентов Windows) найдите Networking Services (Сетевые службы) и нажмите Details (Подробно).
- Выберите компонент Domain Name System (DNS) и подтвердите свой выбор.
- Дождитесь завершения установки сервера.

2-й способ.

- Откройте Control Panel - Administrative Tools (Панель управления - Администрирование).
- Запустите Manage Your Server (Управление сервером).
- Выберите Add or remove a role (Добавить или удалить роль) и выберите DNS Server.
- Дождитесь завершения установки сервера.

3. Для дальнейшей настройки DNS-сервера используется оснастка главного системного меню Administrative Tools (Администрирование) – DNS.

Задание 2. Создайте зону прямого просмотра myzone.ru.

Указания к выполнению

1. Откройте оснастку DNS.
2. Разверните узел DNS, далее разверните узел <Имя компьютера>.
3. Для создания нового домена щелкните правой кнопкой по Forward Lookup Zones (Зоны прямого просмотра) и выберите пункт New zone (Новая зона).
4. В окне Zone Type (Тип зоны) укажите Primary Zone (Основная зона) и нажмите Next (Далее).
5. В окне Zone Name (Имя зоны) укажите имя зоны – myzone.ru и нажмите Next.
6. В окне Zone File (Файл зоны) убедитесь, что выбран переключатель Create A New File With This File Name (Создать новый файл с этим именем) и имя создаваемого файла – myzone.ru.dns.
7. Просмотрите сводку выбранных параметров и щелкните кнопку Finish (Готово).
8. Убедитесь, что в Forward Lookup Zones появился новый узел myzone.ru и сгенерированы записи Start of Authority (SOA) (Начальная запись зоны), Name Server (NS) (Сервер имен) и Host (A) (Хост).
9. Для добавления нового узла (хоста) в созданную зону, щелкните правой кнопкой по узлу myzone.ru и выберите New Host (Новый хост). В поле Name (Имя) введите имя узла – server. Поле IP Address установите равным IP-адресу вашего компьютера. Нажмите Add Host (Добавить хост).

Задание 3. Протестируйте работу службы DNS.

Указания к выполнению

1. Запустите виртуальную машину с Windows XP. Выполните в ней команду ping server.myzone.ru.

2. Убедитесь, что такой узел был найден, и отображается его IP-адрес. Если ping не проходит, нужно исправить настройки.

3. Для преобразования IP-адреса в доменное имя выполните утилиту nslookup с параметром, равным IP-адресу виртуальной машины. Объясните, почему появилась ошибка.

Задание 4. Создайте зону обратного просмотра (для преобразования IP-адреса в доменное имя).

Указания к выполнению

1. В узле Reverse Lookup Zones (Зоны обратного просмотра) щелкните правой кнопкой мыши и выберите New zone (Мастер создания новой зоны).

2. В окне Zone Type (Тип зоны) укажите Primary Zone (Основная зона) и нажмите Next.

3. Убедитесь, что выбран переключатель Network ID (Номер сети). В поле под ним введите адрес вашей сети (например, 192.168.1). Поле Reverse Lookup Zone Name (Имя зоны обратного просмотра) внизу окна должно выглядеть так: 1.168.192.in-addr.arpa.

4. Завершите работу мастера, оставив все настройки по умолчанию.

5. Щелкните правой кнопкой мыши по новому узлу в Reverse Lookup Zones (например, 192.168.1.x Subnet) и выберите New Pointer (Новый указатель). Последнее число установите равным последнему числу в IP-адресе. В поле Host name (Имя хоста) запишите полное имя узла, например server.myzone.ru.

Задание 5. Создайте псевдоним для узла server.myzone.ru.

Указания к выполнению

Щелкните правой кнопкой мыши по узлу myzone.ru и выберите New Alias (Новый псевдоним). В поле Alias name (Имя псевдонима) укажите псевдоним узла (например, MyServer). В поле Fully qualified domain name (Полное доменное имя) впишите полное имя server.myzone.ru

Задание 6. Протестируйте работу службы DNS.

Указания к выполнению

Используйте утилиты ping, nslookup.

В дереве консоли откройте свойства узла через команду контекстного меню Properties (Свойства).

Перейдите на вкладку Monitoring (Наблюдение).

В группе Select A Test Type (Выберите тип теста) пометьте флажки A Simple Query Against This DNS Server (Простой запрос к этому DNS-серверу) и Recursive Query To Other DNS Servers (Рекурсивный запрос к другим DNS-серверам). Щелкните кнопку Test Now (Тестировать).

В списке Test Results (Результаты теста) против обеих записей вы увидите PASS (тест пройден). Если вы работаете на автономном сервере, напротив Recursive Query (Рекурсивный запрос) вы увидите FAIL (ошибка).

Задание 7. Сконфигурируйте клиента для использования службы DNS.

Указания к выполнению

1. На клиенте откройте диалоговое окно его свойств TCP/IP. Настройте систему для автоматического получения адреса DNS (это обеспечивает сервер DHCP) или вручную укажите IP-адреса предпочтительного и дополнительного серверов DNS.

2. Для настройки дополнительных параметров DNS щелкните кнопку Advanced (Дополнительно). Чтобы задать параметры DNS, в диалоговом окне Advanced TCP/IP Settings (Дополнительные параметры TCP/IP) перейдите на вкладку DNS. Здесь можно сконфигурировать и параметры, обеспечивающие разрешение имен узлов, для которых не было указано полное доменное имя, и настроить параметры регистрации DNS.

Задание 8. Задайте разрешение имен с использованием файла HOSTS для случаев отказа службы DNS и для возможности использования коротких имен при доступе к удаленным узлам.

Указания к выполнению

1. На сервере найдите системный файл HOSTS и откройте его в текстовом редакторе.
2. Какая запись уже присутствует в файле по умолчанию и что эта запись означает? Что это за адрес и для чего он используется?
3. Выясните IP-адрес узла www.microsoft.com.
4. Внесите запись в файл, указав полученный IP-адрес и имя -www.microsoft.com. Сохраните изменения.
5. Проверьте через браузер доступность узла www.microsoft.com.
6. Внесите в файл IP-адрес своего сервера и имя в формате computer.domain. Сохраните изменения.
7. Остановите службу DNS через утилиту Services.
8. Проверьте, доступно ли это имя в формате computer.domain через утилиту ping.

Самостоятельная работа

Установите DNS-сервер для домена faculty.ru. Настройте прямую и обратную зоны, протестируйте сервер с помощью оснастки DNS, командной строки и виртуальной машины с Windows XP.

Зафиксируйте все шаги установки, настройки и тестирования DNS-сервера с помощью скриншотов в отчете.

Лабораторные работы на темы:
1.Конфигурирование информационной системы домена
2.Настройка параметров информационной системы домена

Цель работы: познакомиться с основными характеристиками Windows Server 2003 и средствами администрирования программно-аппаратной части информационно вычислительной системы. Изучить задачи администратора и инструментарий, применяемый для их решения. Получение навыков по применению механизмов резервного копирования и восстановления.

Теоретический материал

Введение в Windows Server 2003

Система Windows Server 2003 - это развитие системы Windows 2000. Для администраторов, работающих с сетями Windows 2000, развертывание этой новой версии Windows не станет сложной задачей, поскольку основы изменились не слишком сильно. Для администраторов, работающих с сетями Windows NT, эта превосходно настроенная версия корпоративной операционной системы Microsoft содержит столько инструментов администрирования и средств управления, что у них не найдется причин для того, чтобы продолжать работать с NT.

Версии Windows Server 2003

Windows Server 2003 поставляется в виде следующих четырех версий (изданий):

- Windows Server 2003, Standard Edition, разработана для предоставления служб и ресурсов другим системам в сети. Она сменила Windows NT 4.0 Server и Windows 2000 Server. Эта ОС обладает богатым набором функций и конфигурационных параметров. Windows Server 2003 поддерживает до двух центральных процессоров и до 4 Гбайт оперативной памяти.

- Windows Server 2003, Enterprise Edition, расширяет возможности Windows Server 2003, Standard Edition, обеспечивая поддержку служб кластеров, служб метакаталогов и служб для Macintosh. В ней также поддержи каются 64-разрядные процессоры Intel Itanium, оперативная память с возможностью ≪горячей≫ замены и неоднородный доступ к памяти (nonuniform memory access, NUMA). Эта версия поддерживает до 32 Гбайт оперативной памяти на процессорах x86, до 64 Гбайт оперативной памяти на процессорах Itanium и до 8 центральных процессоров.
- Windows Server 2003, Datacenter Edition, — самый надежный Windows-сервер. Эта версия поддерживает более сложную кластеризацию и способна работать с большими объемами оперативной памяти — до 64 Гбайт на процессорах x86 и до 128 Гбайт на процессорах Itanium. Минимальное количество процессоров для работы Datacenter Edition — 8, максимальное — 32.
- Windows Server 2003, Web Edition, предназначена для запуска служб Web при развертывании Web-узлов и Web-приложений. Для решения этих задач в данную версиювключены Microsoft .NET Framework, Microsoft Internet Information Sendees (IIS), AS P.NET и функции для равномерного распределения нагрузки на сеть, Многие другие функции, в частности Active Directory, в ней отсутствуют. Строго говоря, из стандартных компонентой Windows в этой версии предусмотрены лишь распределенная файловая система DFS, шифрованная файловая система EFS и удаленный рабочий стол. Версия Windows Server 2003, Web Edition, поддерживает до 2 Гбайт оперативной памяти и до двух центральных процессоров.

Все версии поддерживают одни и те же базовые функции и средства администрирования. Т. е. методики, описанные в этой книге, можно применять независимо от того, какой версией Windows Server 2003 вы пользуетесь. Помните, что в версии Web Edition нет Active Directory, поэтому сервер, работающий под управлением этой версии, нельзя сделать контроллером домена. Он, тем не менее, может быть частью домена Active Directory.

Различия в администрировании

Сети Microsoft Windows поддерживают две модели служб каталогов: рабочую группу (workgroup) и домен (domain).

- Рабочие группы — это свободные объединения компьютеров, в которых каждый компьютер управляется независимо.
- Домены — это объединения компьютеров, коллективно управляемых с помощью контроллеров домена, т. е. систем Windows Server 2003, регулирующих доступ к сети, базе данных каталога и общим ресурсам.

Для организаций, внедряющих Windows Server 2003, модель домена наиболее предпочтительна. Модель домена характеризуется единым каталогом ресурсов предприятия — Active Directory, — которому доверяют все системы безопасности, принадлежащие домену. Поэтому такие системы способны работать с субъектами безопасности (учетными записями пользователей, групп и компьютеров) в каталоге, чтобы обеспечить защиту ресурсов. Служба Active Directory, таким образом, играет роль идентификационного хранилища и сообщает «кто есть кто» в этом домене.

Впрочем, Active Directory — не просто база данных. Это коллекция файлов, включая журналы транзакций и системный том (Sysvol), содержащий сценарии входа в систему и сведения о групповой политике. Это службы, поддерживающие и использующие БД, включая протокол LDAP (Lightweight Directory Access Protocol), протокол безопасности Kerberos, процессы репликации и службу FRS (File Replication Service). БД и ее службы устанавливаются на один или несколько контроллеров домена. Контроллер домена назначается Мастером установки Active Directory, который можно запустить с помощью Мастера настройки сервера или командой DCPROMO из командной строки. После того как сервер становится контроллером домена, на нем хранится копия (реплика) Active

Directory, и изменения БД на любом контроллере реплицируются на все остальные контроллеры домена.

Домены, деревья и леса

Active Directory не может существовать без домена и наоборот. Домен — это основная административная единица службы каталогов. Однако предприятие может включить в свой каталог Active Directory более одного домена. Когда несколько моделей доменов совместно используют непрерывное пространство имен DNS, они образуют логические структуры, называемые деревьями (tree). Например, домены contoso.com, us.contoso.com и europe.contoso.com совместно используют непрерывное пространство имен DNS и, следовательно, составляют дерево.

Домены Active Directory с разными корневыми доменами образуют несколько деревьев. Они объединяются в самую большую структуру Active Directory — лес (forest). Лес Active Directory содержит все домены в рамках службы каталогов. Лес может состоять из нескольких доменов в нескольких деревьях или только из одного домена. Когда доменов несколько, приобретает важность компонент Active Directory, называемый глобальным каталогом (global catalog): он предоставляет информацию об объектах, расположенных в других доменах леса.

Групповая политика

Организационные подразделения (ОП) также используются для объединения одинаково настроенных объектов — компьютеров и пользователей. Групповая политика Active Directory позволяет централизованно управлять практически любыми конфигурационными изменениями системы. С ее помощью можно указать настройки безопасности, развернуть ПО и настроить поведение ОС и приложений, даже не прикасаясь к компьютерам пользователей. Вы просто реализуете свою конфигурацию в рамках одного объекта групповой политики (ОГП).

ОГП состоят из сотен возможных конфигурационных параметров: от прав и привилегий пользователя до ПО, которое разрешено запускать на системе. ОГП подключается к контейнеру внутри Active Directory (обычно к ОП, но может и к доменам или даже сайтам), и после этого его настройки распространяются на всех пользователей и компьютеры внутри этого контейнера.

Любой сервер может поддерживать одну или более следующих ролей.

- Контроллер домена (Domain controller) — сервер, на котором работают службы каталогов и располагается хранилище данных каталога. Контроллеры домена также отвечают за вход в сеть и поиск в каталоге. При выборе этой роли на сервере будут установлены DNS и Active Directory. Почтовый сервер (POPS, SMTP) [Mail server (POP3, SMTP)] - сервер, на котором работают основные почтовые службы POP3 (Post Office Protocol 3) и SMTP (Simple Mail Transfer Protocol), благодаря чему почтовые POP3-клиенты домена могут отправлять и получать электронную почту. Выбрав эту роль, вы определяете домен по умолчанию для обмена почтой и создаете почтовые ящики. Эти службы удобны в небольших компаниях или при удаленном соединении, когда электронная почта необходима, но вполне может обойтись без функциональности Microsoft Exchange Server.
- Сервер печати (Print, server) — сервер, организующий доступ к сетевым принтерам и управляющий очередями печати и драйверами принтеров. Выбор этой роли позволит вам быстро настроить параметры принтеров и драйверов.
- Сервер потоков мультимедиа (Streaming media server) — сервер, предоставляющий мультимедийные потоки другим системам сети или Интернета. Выбор этой роли приводит к установке служб Windows Media. Эта роль поддерживается только в версиях Standard Edition и Enterprise Edition.
- Сервер приложений (Application server) — сервер, на котором выполняются Web-службы XML, Web-приложения и распределенные приложения. При назначении серверу этой роли на нем автоматически устанавливаются IIS, COM+ и Microsoft .NET Framework.

При желании вы можете добавить к ним серверные расширения Microsoft FrontPage, а также включить или выключить ASP.NET.

- Сервер терминалов (Terminal Server) — сервер, выполняющий задачи для клиентских компьютеров, которые работают в режиме терминальной службы. Выбор этой роли приводит к установке Terminal Server. Для удаленного управления сервером устанавливать Terminal Server не нужно. Необходимый для этого удаленный рабочий стол (Remote Desktop) устанавливается автоматически вместе с ОС.
- Сервер удаленного доступа или VPN-сервер (Remote access/VPN server) — сервер, осуществляющий маршрутизацию сетевого трафика и управляющий телефонными соединениями и соединениями через виртуальные частные сети (virtual private network, VPN). Выбрав эту роль, вы запустите Мастер настройки сервера маршрутизации и удаленного доступа (Routing and Remote Access Server Setup Wizard). С помощью параметров маршрутизации и удаленного доступа вы можете разрешить только исходящие подключения, входящие и исходящие подключения или полностью запретить доступ извне.
- Узел кластера серверов (Server cluster node) — сервер, действующий в составе группы серверов, объединенных в кластер. Выбор этой роли приводит к запуску Мастера создания кластера (New Server Cluster Wizard), позволяющего создать новую кластерную группу, или Мастера добавления узлов (Add Nodes Wizard), который поможет добавить сервер к существующему кластеру. Эта роль поддерживается только в версиях Enterprise Edition и Datacenter Edition.
- Файл-сервер (File server) — сервер, предоставляющий доступ к файлам и управляющий им. Выбор этой роли позволит вам быстро настроить параметры квотирования и индексирования. Вы также можете установить Web-приложен и для администрирования файлов. В этом случае будет установлен IIS и включены страницы ASP (Active Server Pages).
- DHCP-сервер (DHCP Server) — сервер, на котором запущен DHCP (Dynamic Hose Configuration Protocol), позволяющий автоматизировать назначение IP-адресов клиентам сети. При выборе этой роли на сервере будет установлен DHCP и запущен Мастер создания области (New Scope Wizard).
- DNS-сервер (DNS Server) — сервер, на котором запущена служба DNS, разрешающая имена компьютеров в IP-адреса и наоборот. При выборе этой роли на сервере будет установлена DNS и запущен Мастер настройки DNS-сервера (Configure DNS Server Wizard).
- WINS-сервер (WINS server) — сервер, на котором запущена служба WINS (Windows Internet Name Service), разрешающая имена NetBIOS в IP-адреса и наоборот. Выбор этой роли приводит к установкеWINS.

Управление выбранными ролями сервера осуществляется с помощью программы Управление данным сервером (Manage Your Server), в окне которой сосредоточены все основные инструменты для управления Windows Server 2003. В частности, здесь перечислены текущие роли сервера (рис.1). Чтобы открыть это окно, воспользуйтесь меню Администрирование (Administrative Tools).

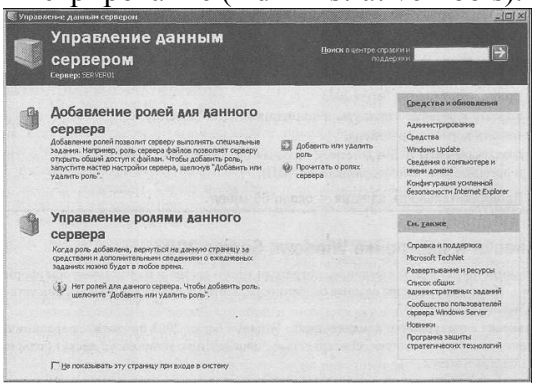


Рисунок 1. Страница Управление данным сервером

Таблица 1. Краткий справочник основных средств администрирования Windows Server 2003

Средство администрирования	Назначение
Active Directory — домены и доверие (Active Directory Domains and Trusts)	Управление доверительными отношениями между доменами
Active Directory — пользователи и компьютеры (Active Directory Users and Computers)	Управление пользователями, группами, компьютерами и другими объектами Active Directory
Active Directory — сайты и службы (Active Directory Sites and Service)	Создание сайтов для управления репликацией Active Directory
DHCP	Конфигурация и управление службой DHCP
DNS	Управление службой системы доменных имен (DNS)
WINS	Управление службой WINS, преобразующей имена NetBIOS в IP-адреса
Администратор кластеров (Cluster Administrator)	Управление службой Cluster
Администратор серверных расширений (Server Extensions Administrator)	Управление серверными расширениями, например FrontPage
Внешнее хранилище (Remote Storage)	Управление службой Remote Storage
Диспетчер служб Интернета (Internet Information Services Manager)	Управление Web-, FTP- и SMTP-серверами
Диспетчер служб терминалов (Terminal Services Manager)	Управление пользователей, сеансов и процессов Terminal Service
Источники данных (ODBC) [Data Sources (ODBC)]	Добавление, удаление и настройка источников данных и драйверов ODBC (Open Database Connectivity)
Контроль допуска QpS (QoS Admission Control)	Управление службой Quality of Service (QpS) Admissions Control для регулировки пропускной способности сети
Лицензирование (Licensing)	Управление лицензированием доступа клиентов к серверным продуктам
Маршрутизация и удаленный доступ к сети (Routing and Remote Access)	Конфигурация и управление службой Routing and Remote Access, контролирующей интерфейсы маршрутизации, динамическую IP-маршрутизацию и удаленный доступ
Настройка сервера (Configure Your Server)	Добавление, удаление и конфигурация служб Windows для сети
Настройка служб терминалов (Terminal Services Configuration)	Управление настройкой протокола Terminal Service и параметрами сервера
Пакет администрирования диспетчера подключений (Connection Manager Administration Kit)	Конфигурирование и настройка диспетчера подключений
Политика безопасности домена (Domain Security Policy)	Просмотр и редактирование политики безопасности в домене
Политика безопасности контроллера домена (Domain Controller Security Policy)	Просмотр и редактирование политики безопасности для организационного полразделения контроллера домена
Производительность (Performance)	Отображение графиков производительности системы и настройка журналов и сигналов оповещения
Просмотр событий (Event Viewer)	Управление событиями и журналами
Распределенная файловая система DIFS (Distributed File System)	Создание и управление распределенными файловыми системами, объединяющими общие папки из разных компьютеров
Сетевой монитор (Microsoft Network Monitor)	Мониторинг сетевого трафика и устранение неисправностей в сети
Службы (Services)	Управление запуском и настройка служб Windows
Службы компонентов (Component Services)	Конфигурация и управление приложениями COM-, управление событиями и службами
Удаленные рабочие столы (Remote Desktop)	Настройка удаленных подключений и просмотр сеансов удаленных подключений
Управление компьютером(Computer Management)	Запуск и остановка служб, управление дисками и доступ к другим средствами управления системой
Центр сертификации (Certification Authority)	Управление сертификационными службами

Регистрация пользователя в системе

Защиту ресурсов реализуют несколько процессов на разных уровнях операционной системы. Первый из них — механизм регистрации — обеспечивает защиту доступа к домену или компьютеру.

Чтобы получить доступ к ресурсам, пользователям необходимо сначала зарегистрироваться — идентифицировать себя в домене или на компьютере.

При регистрации пользователя, в зависимости от выбранного способа регистрации в системе, появляется диалоговое окно «Операционная система Windows» с текстом «Нажмите Ctrl+Alt+Delete».

Рисунок 2. Диалоговое окно "Операционная система Windows"

Рисунок 3. Диалоговое окно "Вход в Windows"

Параметры диалогового окна «Вход в Windows» описаны в таблице 2.

Таблица 2. Параметры диалогового окна "Вход в Windows"

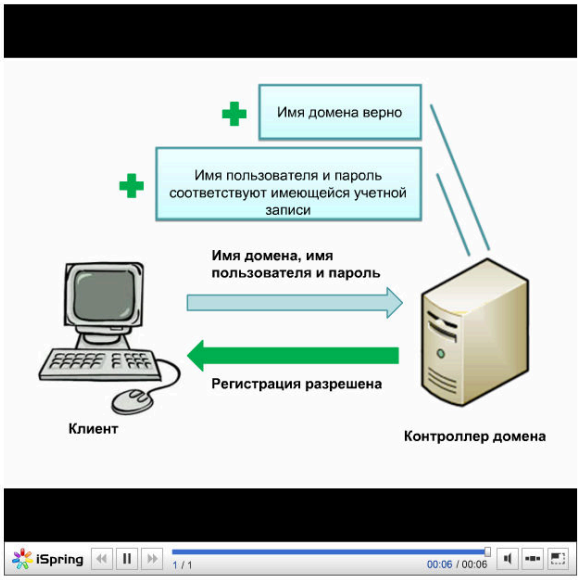
Параметры	Описание
User Name (Имя)	Введите уникальную учетную запись пользователя, присвоенную Вам администратором. Эта учетная запись должна присутствовать в базе данных каталогов на контроллерах домена, чтобы обеспечивать регистрацию в домене, и в базе данных каталогов локального компьютера — для регистрации на локальном компьютере
Password (Пароль)	Введите пароль, присвоенный указанному Вами имени пользователя, учитывая регистр символов. Чтобы пароль не стал достоянием посторонних, при его вводе символы на экране заменяются звездочками (*)
Domain (Домен)	Чтобы зарегистрироваться в домене, укажите его имя. При попытке регистрации пользователя в домене база данных контроллера домена проверяется на наличие соответствующего элемента. Регистрация по указанной учетной записи разрешается, если введенное имя пользователя, пароль и имя домена соответствуют данным в базе данных контроллера домена. Чтобы зарегистрироваться на локальном компьютере, укажите его имя.

	Локальный компьютер проверит наличие информации о Вас в локальной базе данных каталогов. Регистрация по указанной учетной записи разрешается, если введенное имя пользователя, пароль и имя компьютера соответствуют данным в локальной базе данных каталогов. Пользователь может зарегистрироваться на локальном компьютере, только указав имя пользователя, имеющееся в локальной базе данных каталогов. Серверы и компьютеры под управлением Windows 2003 содержат встроенные локальные учетные записи Administrator (Администратор) и Guest (Гость).

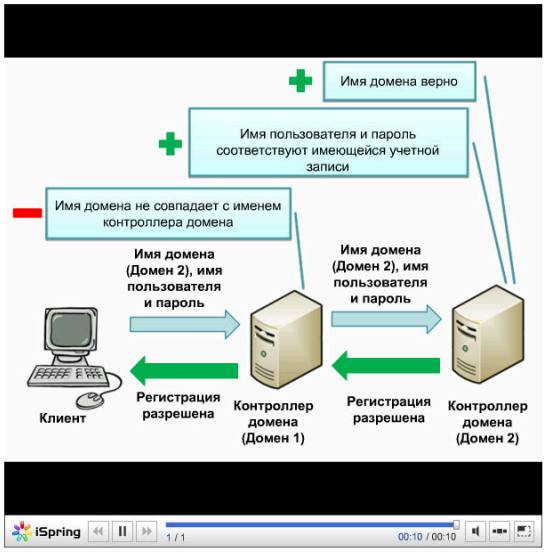
Проверка глобальной учетной записи

Когда пользователь щелкнет кнопку ОК, компьютер передает имя домена, имя пользователя и пароль контроллеру домена. Последний сначала проверяет имя домена, а затем ищет имя пользователя и пароль в базе данных домена. Далее события могут разворачиваться по одному из трех сценариев.

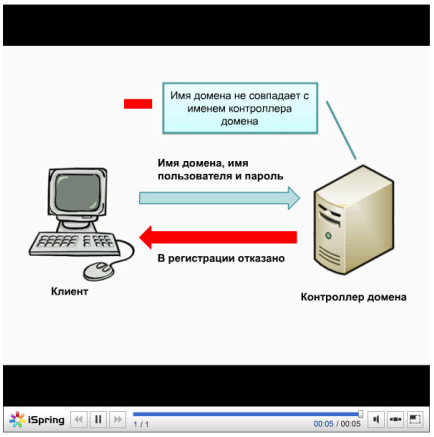
1. Если имя домена указано верно, а имя пользователя и пароль соответствуют имеющейся учетной записи, сервер уведомляет компьютер, что регистрация разрешена.



2. Если пользователь указал имя домена, не совпадающее с именем домена контроллера, но контроллер распознает его как имя доверяемого домена, то он передает информацию контроллеру этого домена. Последний выполняет аутентификацию и возвращает соответствующую информацию.



3. Если имя домена не совпадает с именем контроллера домена и тот не распознает указанный домен, то контроллер запрещает доступ к домену.



Проверка локальной учетной записи

Когда пользователь щелкает кнопку ОК, компьютер сначала проверяет указанное имя компьютера, а затем ищет имя пользователя и пароль в локальной базе данных каталогов. Если имена совпадают, регистрация разрешается и пользователь получает доступ к локальным ресурсам. Если же нет, пользователь не получает доступ к компьютеру.

Функции администратора Windows 2003

Администрирование Windows NT подразумевает выполнение как специальных операций после установки системы, так и рутинных каждодневных действий.

Функции администратора можно разделить на пять категорий.

Таблица 3. Функции администратора

Категория	Характерные задачи
Администрирование учетных записей пользователей и групп	Планирование, создание и ведение учетных записей пользователей и групп для обеспечения каждому пользователю возможности регистрации в сети и доступа к необходимым ресурсам
Администрирование защиты	Планирование и реализация стратегии безопасности для защиты данных и общих сетевых ресурсов, в том числе папок, файлов и принтеров
Администрирование принтеров	Настройка локальных и сетевых принтеров для обеспечения пользователям доступа к ресурсам печати. Устранение обычных проблем печати
Мониторинг событий и ресурсов сети	Планирование и реализация стратегии аудита событий в сети с целью обнаружения нарушений защиты. Управление ресурсами и контроль их использования
Резервное копирование и восстановление данных	Планирование и выполнение регулярных операций резервного копирования для обеспечения быстрого восстановления важных данных

Средства администратора Windows 2003

Средства администрирования входят в состав Windows 2003 и могут применяться или для администрирования любого компьютера домена, или для администрирования локального компьютера.

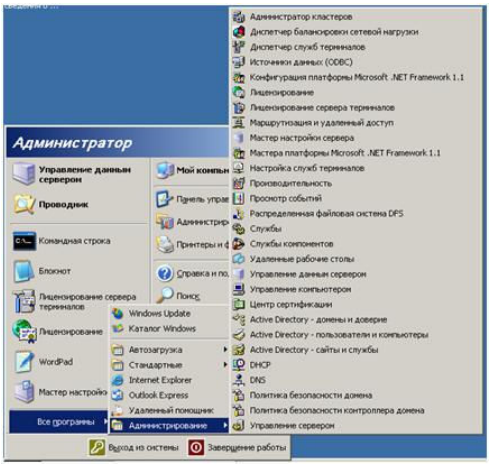


Рисунок 4. Средства администрирования

Таблица 4. Средства администрирования

Средство	Назначение
Администратор кластеров	Администратор кластеров - это основное средство администрирования и конфигурирования объектов кластера серверов, таких как узлы, группы и другие ресурсы. Это позволяет вам управлять кластером серверов без необходимости физического присутствия в одном из узлов.
Диспетчер балансировки сетевой нагрузки	Обеспечивает балансирование IP-трафика между несколькими серверами. Не обеспечивает переход по отказу (failover) для приложений и данных.
Диспетчер служб терминалов	Позволяет управлять конфигурацией сервера служб терминалов
Конфигурация платформы Microsoft .NET Framework 1.1	Позволяет настраивать среду .NET Framework
Лицензирование	Утилита, позволяющая управлять клиентскими лицензиями в масштабах предприятия
Лицензирование сервера терминалов	Утилита, позволяющая управлять клиентскими лицензиями для служб терминалов (Terminal Services), работающих в режиме выполнения приложений
Маршрутизация и удалённый доступ	Служит для управления маршрутизацией и удаленным доступом
Мастер настройки сервера	Мастер, позволяющий администратору настроить сервер в соответствии с выбранными ролями (файловый сервер, сервер служб Интернета и т. д.)
Производительность	Каждый компьютер с Windows Server 2003 содержит компоненты, мониторинг которых можно выполнять с помощью оснастки Performance (Производительность). Это могут быть аппаратные или программные компоненты, которые выполняют задачи или поддерживают рабочую нагрузку. Многие из этих компонентов имеют показатели, отражающие определенные аспекты их функционирования, которые можно точно измерить как скорость выполнения задач.
Просмотр событий	Служит для просмотра и управления системным журналом, журналами безопасности и приложений
Распределенная файловая система DFS	Создает и управляет распределенными файловыми системами, объединяющими совместно используемые папки на различных компьютерах
Службы	Запускает, останавливает и конфигурирует службы (сервисы) Windows
Службы компонентов	Конфигурирует и управляет службами компонентов COM+
Удалённые рабочие столы	Позволяет управлять многочисленными сессиями терминального доступа к удаленным компьютерам
Управление данным сервером	Мастер, представляющий собой информационный центр для управления различными ролями сервера, обращения к службам поддержки и вспомогательным инструментам, а также позволяющий быстро находить информацию об обновлениях, способах решения проблем и т. п.

Управление компьютером	Предоставляет функции администрирования системы. Содержит в своем составе ряд изолированных оснасток и оснасток расширения
Центр сертификации	Позволяет работать с центрами сертификации, развернутыми в корпоративной сети
Active Directory - домены и доверие	Служит для управления доменами и доверительными отношениями
Active Directory — сайты и службы	Определяет топологию и расписание репликации Active Directory. Обеспечивает изменение служб корпоративного уровня
Политика безопасности домена	Служит для управления параметрами безопасности (представленными в узле Security Settings объекта групповой политики, привязанного к объекту домена) для всего домена
Политика безопасности контроллера домена	Служит для управления параметрами безопасности (представленными в узле Security Settingsобъекта групповой политики, привязанного к подразделению Domain Controllers) на контроллерах домена

Мониторинг ресурсов

Сведения о системе

Утилита System Information (Сведения о системе) (Winmsd.exe) представляет исчерпывающую информацию об аппаратном обеспечении компьютера, системных компонентах и программной среде. Системная информация разделена на категории, которым в окне структуры соответствуют следующие узлы (Рисунок 5): System Summary (Сведения о системе),Hardware Resources (Ресурсы аппаратуры), Components (Компоненты), Software Environment (Программная среда) и Internet Settings (Параметры Интернета).

- Узел System Summary отображает общую информацию о компьютере и операционной системе: версию ОС и номер сборки, тип процессора, объем ОЗУ, версию BIOS, региональные установки, а также информацию об объеме физической и виртуальной памяти на компьютере.
- Узел Hardware Resources отображает информацию об аппаратных установках, таких как каналы DMA, номера прерываний (IRQ), адреса ввода/вывода (I/O) и адреса памяти. Узел Conflicts/Sharing (Конфликты/ Совместное использование) идентифицирует устройства, которые совместно используют ресурсы или конфликтуют с другими ресурсами. Такая информация помогает выявлять проблемы, возникающие с аппаратными устройствами.
- Узел Components отображает информацию о конфигурации Windows и используется для определения статуса драйверов устройств, сетевых устройств и программного обеспечения мультимедийных устройств. Кроме того, данный узел содержит обширную информацию об истории драйверов с записью всех изменений, которые производились с компонентами.
- Узел Software Environment отображает "снимок" программного обеспечения, загруженного в память компьютера. Данная информация может быть использована для просмотра списка выполняющихся задач или для выяснения номера версии продукта.
- Узел Internet Settings содержит, в частности, информацию о настройках программы Internet Explorer.

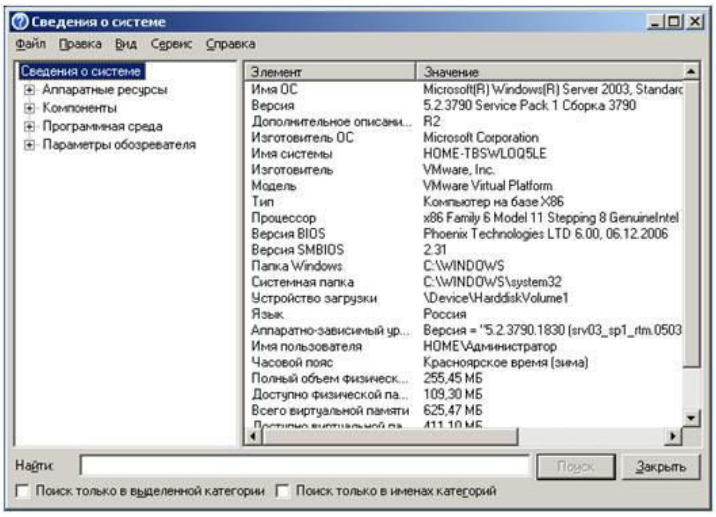


Рисунок 5. Внешний вид утилиты "Сведения о системе"

Составление и печать сводки

- Информация, предоставляемая программой System Information (Сведения о системе), нужна не только организации, осуществляющей поддержку, — напечатанная сводка может пригодиться службе инвентаризации. Из сводки можно быстро узнать объем оперативной памяти и дискового пространства на конкретном компьютере, а также, какие устройства на нем установлены.
- Распечатать постранично или всё целиком можно из меню Файл->Печать. Сохранить общий отчёт можно из меню Файл->Экспорт.

Управление компьютером

Инструмент (и одноименная оснастка) Computer Management (Управление компьютером) (Рисунок 6) является одним из основных средств системного администратора для конфигурирования компьютера. Данную оснастку можно использовать для администрирования, как локальной системы, так и удаленных компьютеров (в том числе систем Windows 2000 и — с некоторыми ограничениями — компьютеров с Windows NT 4.0). Это позволяет администратору со своего рабочего места устранять проблемы и конфигурировать любой компьютер в сети, на котором установлена Windows Server 2003.

Для запуска оснастки Computer Management можно пользоваться двумя способами: выбрать соответствующую команду в меню Start | Administrative Tools или щелкнуть правой кнопкой мыши на команде My Computer(Мой компьютер) в меню Startи выбрать в контекстном меню пункт Manage(Управление).

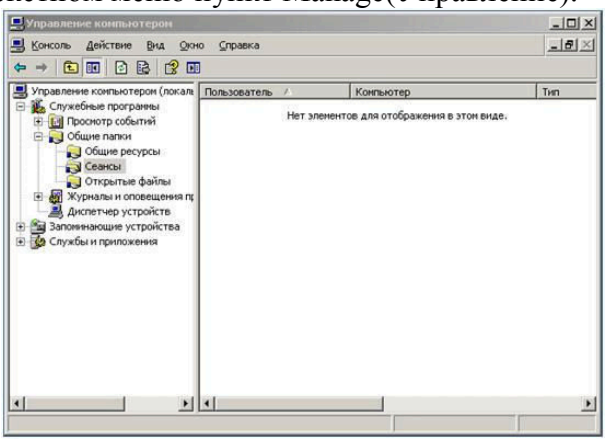


Рисунок 6. Оснастка "Управление компьютером"

Просмотр пользовательских сеансов

Оснастка Shared Folders(Общие папки) позволяет просматривать информацию о соединениях и использовании ресурсов локального или удаленного компьютеров. Данная оснастка используется вместо программы Server в Control Panel системы Windows NT 4.0.

Оснастка Shared Folders содержит три узла: Shares (Ресурсы), Sessions (Сеансы) и Open Files (Открытые файлы). При выборе данных узлов в панели результатов отображается содержание соответствующего узла.

С помощью оснастки можно выполнять следующие задачи:

- создавать, просматривать, изменять свойства и удалять общие ресурсы на локальном или удаленном компьютерах (Windows NT 4.0/2000/XP и Windows Server 2003) и устанавливать разрешения на доступ к ним. Кроме того, можно управлять режимом кэширования общих папок (в случае их использования в качестве изолированных папок). В системах Windows XP и Windows Server 2003 появилась очень удобная новая возможность управления процессом публикации общей папки в каталоге Active Directory (рис. 6.12) — можно сразу после создания общей папки опубликовать ее в каталоге, не прибегая к помощи оснастки Active Directory Users and Computers. Все необходимые действия достаточно очевидны из содержания приведенного примера: в данном случае публикуется общая папка службы факсов, содержащая клиентское программное обеспечение для систем, не имеющих его (например, Windows 9x);
- просматривать список удаленных пользователей, подключенных к компьютеру, и отключать их;
- просматривать список файлов, открытых удаленными пользователями, и закрывать открытые файлы.

Windows 2003 Backup

Регулярное резервное копирование информации с серверов и локальных жестких дисков предотвращает утрату и повреждение данных из-за поломки жесткого диска, отключения питания, воздействия вирусов и т.д. Резервное копирование при грамотном планировании и наличии надежного оборудования позволяет безболезненно справиться с последствиями катастрофы.

Графическое инструментальное средство Windows 2003 Backup предназначено для автоматического и ручного резервного копирования и восстановления файлов, расположенных на разделах файловых систем FAT и NTFS.

Выбор стратегии резервного копирования

Перед тем как приступать к резервному копированию файлов, нужно разработать стратегию, отвечающую потребностям Вашей организации и гарантирующую восстановление утраченных данных. Эффективное архивирование и восстановление информации — одна из самых важных задач администратора.

Отбор файлов для резервного копирования

По степени важности (а следовательно, и по частоте создания резервных копий) папки и файлы можно разделить на три категории:

- важные — их резервные копии создаются всегда;
- полезные — их резервные копии создаются изредка;
- малозначимые — их резервные копии не создаются никогда.

Отбирая файлы для резервного копирования, учитывайте следующие правила:

- всегда создавайте резервные копии файлов, жизненно важных для работы Вашей организации; реестров всех главных и резервных контроллеров домена (каждый контроллер домена имеет свою копию базы данных каталогов; резервное копирование реестра контроллера домена предотвращает потерю информации об учетных записях пользователей и защите).
- резервные копии файлов, изменяемых редко или не представляющих особой ценности, следует создавать лишь время от времени.
- не сохраняйте временные файлы, так как они постоянно изменяются, и вряд ли могут быть использованы для восстановления данных.

Выбор типа резервного копирования

Windows 2003 Программа архивации (Backup Utility) предлагает пять вариантов резервного копирования: обычное (normal), копирующее (copy), инкрементальное (incremental), разностное (differential) и ежедневное (daily). Выбор стратегии резервного копирования определяется тем, сколько времени отводится на сохранение данных и каковы требования к скоростям поиска резервных копий и восстановления файлов.

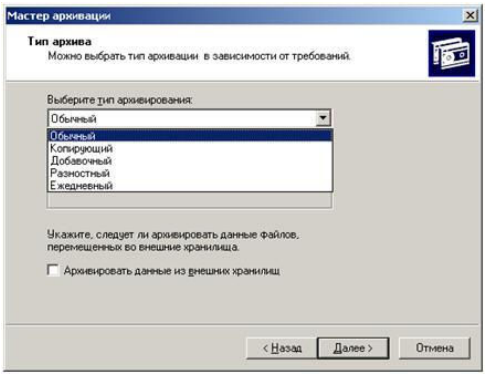


Рисунок 7. Выбор типа архивации

Краткая характеристика перечисленных выше типов резервного копирования приведена в таблице.

Таблица 5. Варианты резервного копирования

Варианты резервного копирования	Характеристика
Обычное или полное	Архивирует выбранные файлы и помечает их как сохраненные. Обычное резервное копирование позволяет быстро восстанавливать файлы, так как наиболее свежие файлы находятся на последней ленте. Для создания первой резервной копии всегда следует применять обычное резервное копирование всех файлов
Инкрементальное или добавочное	Архивирует только файлы, созданные или измененные с момента выполнения последнего обычного или инкрементального резервного копирования. Эти файлы помечаются флажком архивации. Если Вы сочетаете обычное и инкрементальное резервное копирование, то воссоздание информации начинается с восстановления последней обычной резервной копии, а затем последовательно восстанавливаются файлы инкрементальных копий
Разностное	Архивирует файлы, созданные или измененные со времени последнего обычного (или инкрементального) резервного копирования. Файлы при этом не помечаются флажком архивации. При комбинации обычного и разностного резервного копирования для восстановления данных требуются лишь 2 ленты: с последней обычной и с последней разностной копиями
Копирующее	Архивирует выбранные файлы, не помечая их флажком архивации. Тем самым не оказывает влияния на операции обычного и инкрементального резервного копирования и может применяться для промежуточного сохранения данных
Ежедневное копирование	Архивирует выбранные, файлы, которые были изменены во время ежедневного копирования. Файлы не помечаются флажком архивации. Эта операция полезна, например, когда Вы берете работу на дом и хотите быстро выбрать файлы, над которыми сегодня работали

Журналы резервного копирования

Журнал резервного копирования (backup log) — это текстовый файл, в котором регистрируются операции резервного копирования (рис. 8). Он полезен при восстановлении данных. Его можно либо распечатать, либо посмотреть в любом текстовом редакторе. Журнал хранится на диске, поэтому в случае повреждения каталога архива на ленте обратитесь к нему, чтобы найти нужный файл.

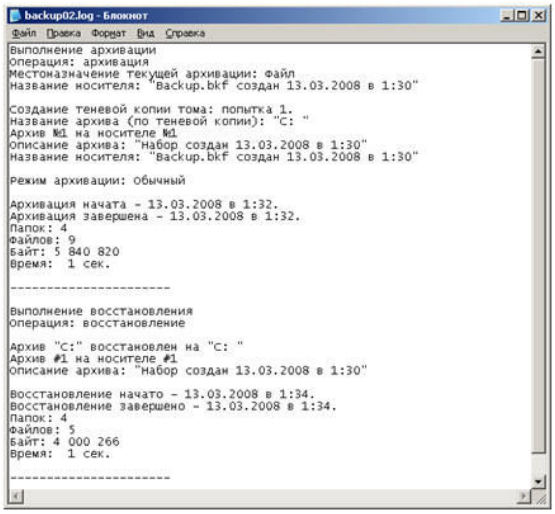


Рисунок 8. Журнал резервного копирования

Журнал резервного копирования содержит следующую информацию:

- дату создания архива;
- название варианта резервного копирования;

местонахождение накопителя.

Шаблон плана резервного копирования

Местонахождение накопителя __ Местонахождение лент_____

Путь к архивируемым файлам и папкам	Ежедневное резервное копирование	Еженедельное резервное копирование (укажите день)

Недельное расписание резервного копирования

Понедельник	Вторник	Среда	Четверг	Пятница
Тип копирования	Тип копирования	Тип копирования	Тип копирования	Тип копирования
Лента	Лента	Лента	Лента	Лента
Архив: Да Нет	Архив: Да Нет	Архив: Да Нет	Архив: Да Нет	Архив: Да Нет

Типы резервного копирования:

О = Обычное, Д = Инкрементальное, Р = Разностное, К = Копирующее, ЕК = Ежедневное копирование

Резервное копирование файлов

Программа резервного копирования Windows 2003 выглядит следующим образом. (рис. 9)

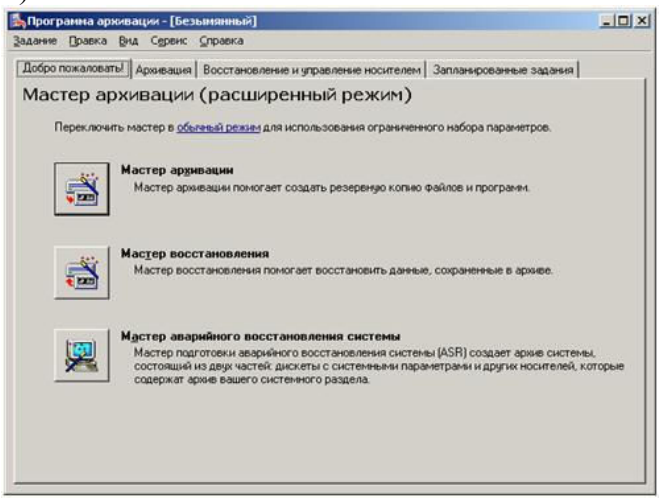


Рисунок 9. Окно мастеров архивации

Чтобы запустить программу, в меню Start (Пуск) выберите пункты Programs (Программы), Accessories (Стандартные), System Tools (Служебные), Backup (Архивация данных).

На рис. 10 представлены мастера архивации. Здесь можно выбрать 3 мастера: мастер архивации, мастер восстановления и мастер аварийного восстановления системы.

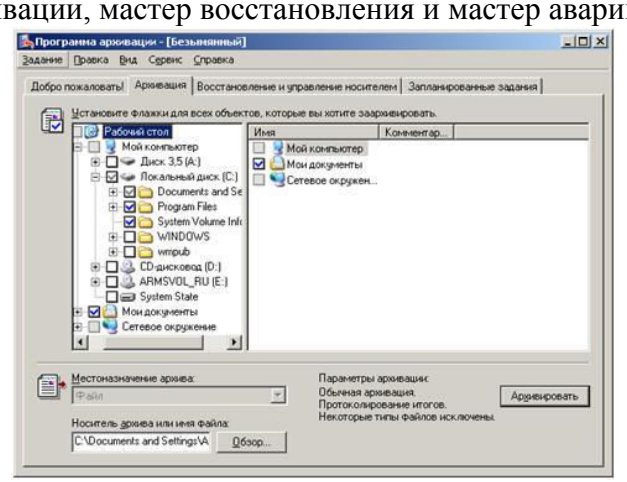


Рисунок 10. Окно "Архивация"

На рисунке 10 представлено окно архивации. Здесь можно выбрать параметры архивации: объекты архивации и назначение архивации. Можно также выбрать дополнительные параметры архивации (рисунок 11).

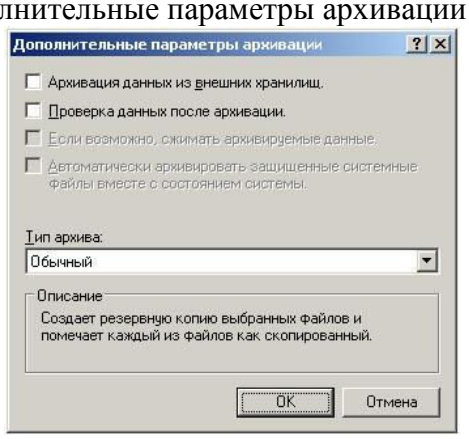


Рисунок 11. Окно "Дополнительные параметры архивации"

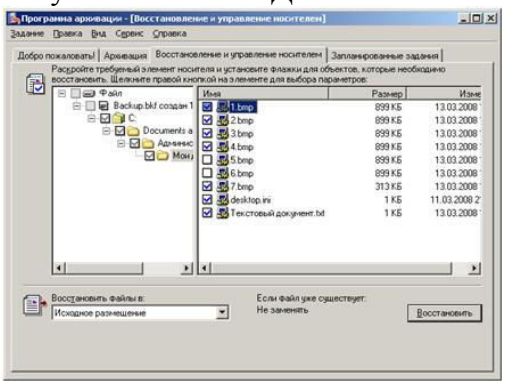


Рисунок 12. Окно "Восстановление и удаление носителем"

На рисунок 12 представлено окно восстановления управления носителем. Здесь можно выбрать необходимые для восстановления объекты.

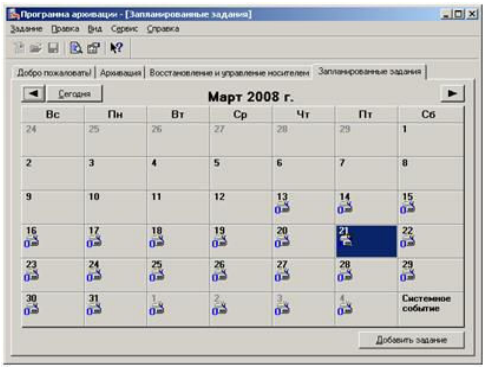


Рисунок 13. Окно "Запланированные задания"

На рисунок 13 представлено окно планировщика заданий. Здесь можно создать задание архивации, путем вызова мастера архивации (рисунок 14).

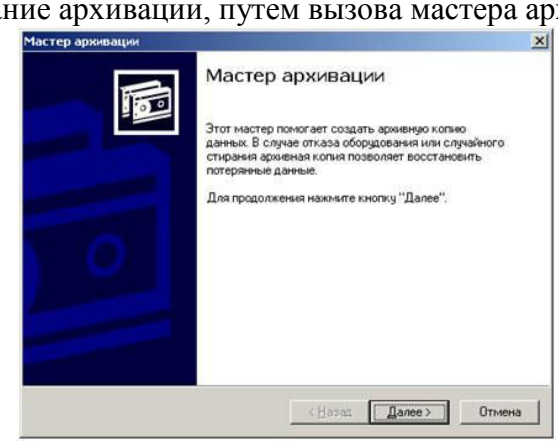


Рисунок 14. Мастер архивации

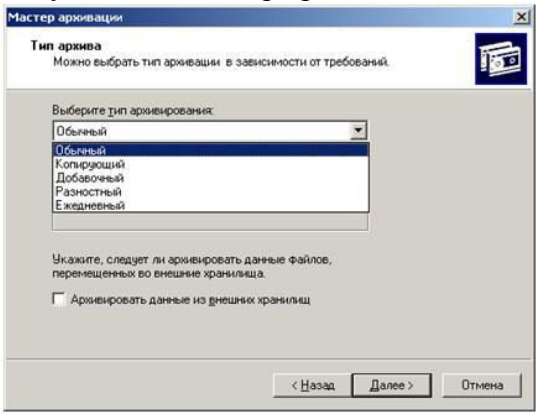


Рисунок 15. Окно "Мастер архивации". Выбор типа архивации.

На рисунок 15 представлены типы архивации: обычный, копирующий, добавочный, разностный, ежедневный. Далее предлагается выбрать время выполнения задания (рисунок 16) и параметры задания (рисунок 17).

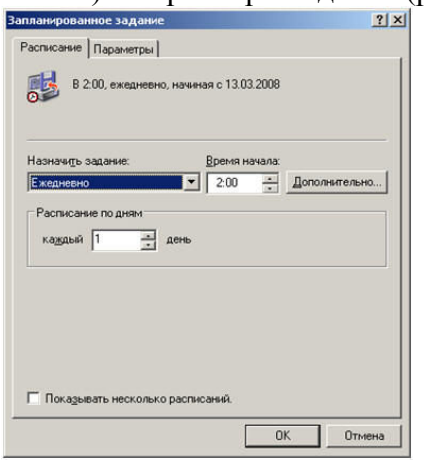


Рисунок 16. Окно "Расписание"

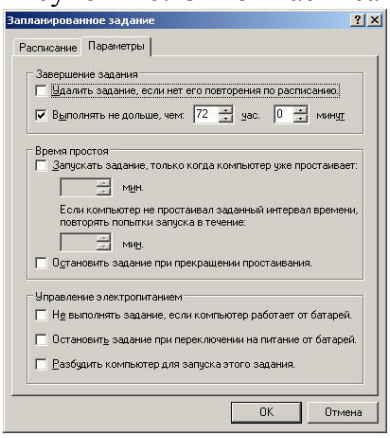


Рисунок 17. Окно "Параметры архивации"

Порядок выполнения работы

1. Изучить предлагаемый теоретический материал.
2. Получить следующую информацию с помощью утилиты System Information (Сведения о системе):
   - свойства компьютера
   - пользовательские сеансы
   - список ресурсов, открытых на сервере
4. Построить отчет с максимальным объемом данных о компьютере (системе).
5. Создать план резервного копирования
6. Выполнить резервное копирование различного типа с помощью программы Backup Utility (Start (Пуск) - Programs (Программы) - Accessories (Стандартные) - System Tools (Служебные) - Backup (Архивация данных)):
   - Полное
   - Инкрементное
   - Ежедневное
7. Проанализировать журнал резервного копирования. Сделать выводы на основании анализа.

Лабораторные работы на темы:
1. Конфигурирование групповых политик домена
2. Настройка параметров групповой политики домена

Цели работы:

• изучить способы задания групповых политик;
• изучить виды параметров групповых политик;
• изучить объекты групповых политик;
• научиться задавать групповые политики для разных объектов.

Групповые политики позволяют реализовать гибкое управление членами доменами – пользователями и компьютерами. В данной работе вам предстоит научиться использовать групповые политики и применять их для управления членами домена **faculty.ru** в соответствии с требованиями проекта.

Задание 1. Задайте в домене политику, в соответствии с которой на уровне всего домена при установке пароля пользователя требовалось бы следующее:

• длина пароля – не менее 8 символов;
• пользователь не может установить ни один из трех предыдущих паролей;
• пароль должен отвечать требованиям сложности;

• максимальный возраст пароля – 60 дней.

Указания к выполнению

1. Для запуска консоли управления MMC выполните команду Start – Run – mmc.

2. Для управления объектами групповой политики на уровне домена в консоли MMC добавьте оснастку Group Policy Object Editor командой File (Консоль) – Add (Добавить) – Remove Snap-in… (Добавить или удалить оснастку) – Add… (Добавить) и выберите из списка соответствующую оснастку.

3. Для определения объекта действия политики нажмите Browse… (Обзор…)

4. Изучите окно и перечислите объекты групповых политик.

5. Выберите Default Domain Policy. Нажмите Finish (Готово). В левом окне консоли должна появиться оснастка Default Domain Policy <имя контроллера домена> Policy.

6. Разверните оснастку и выберите Computer Configuration (Конфигурация компьютера) – Windows Settings (Конфигурация Windows) – Security Settings (Параметры безопасности) – Account Policies (Политики учетных записей) – Password Policy (Политика паролей).

7. Изучите политики паролей и установите настройки в соответствии с требованием задания.

8. Создайте нового пользователя и проверьте правильность настроек.

Запишите в отчет объекты групповых политик.

Внесите в отчет скриншот окна, отражающего установленные параметры политики.

Задание 2. Задайте политику u1085 на уровне всего домена, выполняющую блокировку учетных записей на 5 минут в том случае, если подряд было сделано не менее трех ошибок входа в систему.

Указания к выполнению

1. Соответствующая политика находится в следующем разделе:

Computer Configuration (Конфигурация компьютера) – Windows Settings (Конфигурация Windows) – Security Settings (Параметры безопасности) – Account Policies (Политики учетных записей) – Account Lockout Policy (Политика блокировки учетной записи).

2. Проверьте правильность настроек политики путем нескольких попыток ввести неверный пароль пользователя на рабочей станции.

3. Зайдите на контроллер домена и разблокируйте учетную запись пользователя.

Внесите в отчет скриншоты окна, сообщающего о блокировке учетной записи на рабочей станции, и окно снятия блокировки.

Задание 3. Создайте организационное подразделение StudentSecurity.

Указания к выполнению

1. Выполните команду Start – Programs – Administrative Tools – Active Directory Users and Computers (Пуск – Программы – Администрирование – Пользователи и компьютеры Active Directory).

2. Раскройте папку faculty.ru в левой панели окна.

3. В меню Action выберите команду New – Organization Unit (Создать – Организационное подразделение).

4. В окне New Object – Organization Unit (Новый объект – Подразделение) в поле Name наберите StudentSecurity.

5. Поместите в организационное подразделение учетную запись студента.

6. Правой кнопкой щелкните по новому объекту, выберите Properties

(Свойства) – Security (Безопасность).

7. Просмотрите список групп, обладающих правом доступа к подразделению StudentSecurity.

Внесите в отчет скриншоты окна свойств организационного подразделения.

Задание 4. Задайте политику на уровне организационного подразделения StudentSecurity, запрещающую менять картинку рабочего стола и загружающую общую для всех картинку.

Указания к выполнению

1. Откройте окно StudentSecurity.

2. Выполните команду User Configuration (Конфигурация пользователя) – Administrative Templates (Административные шаблоны) – Desktop (Рабочий стол) – ActiveDesktop, выберите параметр, запрещающий изменение картинки и задайте общую картинку рабочего стола для всего подразделения.

3. Убедитесь в правильности настройки.

Самостоятельная работа

Сохраняйте в отчет скриншоты основных u1096 шагов.

Задание 1. Задайте на уровне организационного подразделения StudentSecurity следующие политики:

• политика пароля, отличная от политики всего домена: длина пароля – не менее 0 символов, пароль не должен отвечать требованиям сложности, срок действия пароля не ограничен;

• запретить менять пароль при помощи окна, вызываемого при помощи Ctrl-Alt-Del;

• убирать пункт меню Properties (Свойства) из контекстных меню My Computer и My Documents;

• из меню Start (Пуск) уберите пункт Run и Help.

Задание 2. Создайте организационное подразделение TeachersSecurity. Разрешите подразделению добавлять рабочие станции, но запретите менять дополнительные параметры стека TCP/IP.

Задание 3. На уровне домена запретить доступ к папке Network Connections (Сетевые подключения).

Лабораторные работы на темы:
1.Конфигурирование безопасной передачи информации
2. Настройка протоколов безопасной передачи информации

Цель работы: Получение навыков настройки портов коммутатора, изучение технологии зеркалирования портов (Port Mirroring) и принципов работы со статической таблицей перенаправления коммутатора.

Применяемое оборудование:

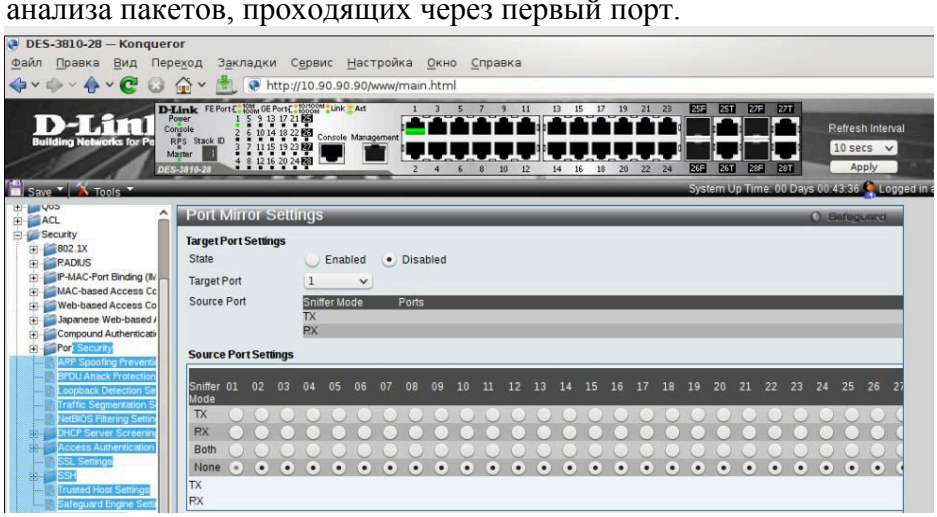
1. Четыре ПК.
2. Два коммутатора третьего уровня D-Link DES-3810-28.
3. Два управляемых коммутатора второго уровня D-Link DES-3200-10.

Теоретические сведения:

Раздел Port Mirror:

Сегодня анализаторы сетевых протоколов эффективно используются ИТ-отделами и отделами информационной безопасности для решения широкого круга задач. С их помощью можно быстро определить причину медленной работы ИТ-сервиса или бизнес-приложения. Они позволяют документировать сетевую активность пользователей и использовать полученные данные, например, для определения источника утечки информации. Единственной «ложкой дегтя» является неудобство их использования в коммутируемых сетях. Дело в том, что анализатор протоколов должен «видеть» весь анализируемый трафик, в то время как в коммутируемой сети трафик между двумя портами коммутатора

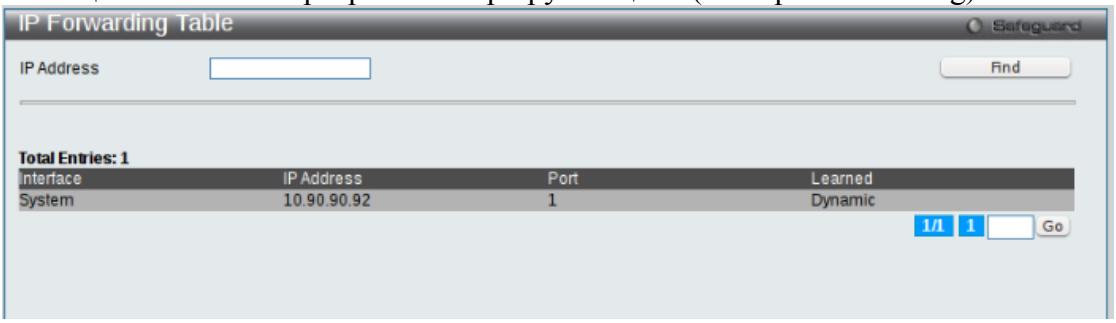
«невиден» на других его портах. Одним из способов решения данной проблемы является технология зеркалирования портов (Port Mirroring), которая поддерживается многими коммутаторами класса High End.
Зеркалирование позволяет копировать пакеты, получаемые и передаваемые с одного порта, на другой зеркальный порт (mirrored port). К зеркальному порту можно подключить устройство мониторинга (например, сетевой сниффер) для детального анализа пакетов, проходящих через первый порт.



Позволяет управлять функцией зеркалирования портов

- Mirror Port State – активность функции
- Target Port – выходной порт
- Source Port – прослушиваемые порты
- Sniffer Mode – настройка прослушиваемых портов
- Tx – только исходящий трафик
- Rx – только входящий трафик
- Both – оба направления
- None – не прослушивать

Раздел Forwarding & Filtering:
Коммутатор принимает все пакеты с присоединенных сегментов. Для каждого получаемого пакета устройство считывает адрес получателя из заголовка протокола Ethernet, и если этот пакет предназначен для системы, расположенный в другом сегменте, передает пакет в этот сегмент и только в этот сегмент. Если пакет послан системе в локальном сегменте, коммутатор отбрасывает его, поскольку данные уже достигли своего места назначения. Чтобы эффективно выполнять перенаправление получаемых пакетов, мост должен знать, какие системы в каком сегменте находятся. Мост хранит эту информацию во внутренней адресной таблице перенаправления (Forwarding Table). Механизм заполнения данной таблицы называется прозрачной маршрутизацией (Transparent Routing).

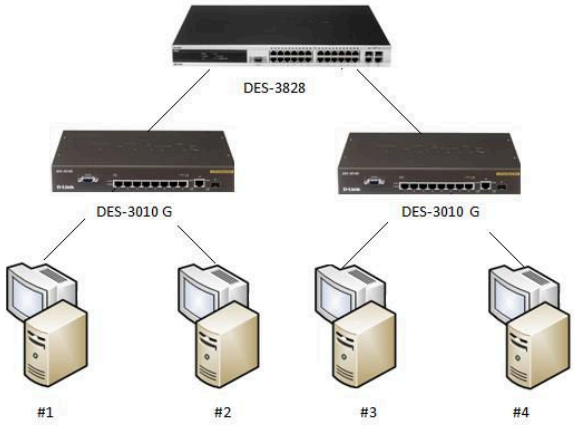


Позволяет управлять статическими записями таблицы коммутации

- Vlan ID - Vlan, в котором действительна запись

- MAC Address – MAC –адрес узла
- Port- порт , на котором находится узел

Порядок выполнения работы



1. Изучите раздел 2.2 «Administration» (меню «Port Configuration»).
2. Постройте топологию сети, показанную на рисунке 4.
3. Выключите один из портов коммутатора, к которому подключен один из компьютеров.
4. Попробуйте осуществить взаимодействие компьютеров. Сделайте выводы на основе полученного результата.
5. Изучите раздел 2.2 «Administration» (меню «Port Mirroring»).
6. Настройте на коммутаторе зеркало для любого из портов, к которому подключен один из компьютеров.
7. Запустите на машинах, подключенных к порту-источнику и порту-приемнику (зеркалу), утилиту tcpdump. Активизируйте сетевую активность. Сравните результаты работы утилит на обеих машинах.
8. Силами двух бригад соберите топологию сети, представленную на рисунке 5. Все линия связи должны быть подключены к портам с пропускной способностью 100 Мбит/с. Обязательно соблюдайте нумерацию портов.
9. Установите пропускную способность портов коммутатора DES-3010G, к которому подключены машины 3 и 4, равной 10 Мбит/с.
10. Настройте зеркало на коммутаторе DES-3010G, к которому подключены машины 1 и

следующим образом: машина 1 - приёмник, машина 2 - источник.

11. «Пингуйте» (утилита ping) одновременно машину 2 с машин 3 и 4.
12. Запустите на машинах 1 и 2 утилиту tcpdump. Сравните результаты работы утилит на обеих машинах.
13. Проделайте действия пунктов 8-12 в обратную сторону.
14. Изучите раздел 2.2 «Administration» (меню «Forward and Filtering»).
15. Создайте в статической таблице перенаправления коммутатора DES-3010G, к которому подключены машины 1 и 2, следующую некорректную запись: машина #4 подключена к порту 3. Вторая бригада должна сделать то же самое на своём коммутаторе - создать следующую некорректную запись: машина #1 подключена к порту 2.
16. Удалите из таблицы перенаправления все записи, полученные коммутатором в режиме самообучения.
17. «Пингуйте» машину #4 с машины #1 и машину #1 с машины #4.

Лабораторная работа
МЕХАНИЗМ АДРЕСАЦИИ В IP-СЕТЯХ

Цель работы – изучить адресацию, общую классификацию адресов в стеке TCP/IP, принцип назначения IP-адресов узлам отдельных подсетей.

Типы адресов стека TCP/IP

В стеке **TCP/IP** используются **три типа адресов**:

1. **локальные** (называемые также аппаратными)
2. **IP-адреса**
3. **символьные доменные имена**

Локальные адреса

Локальный адрес в терминологии **TCP/IP** - это такой тип адреса, который используется средствами **базовой технологии** для доставки данных в пределах **подсети**, которая сама является элементом **составной интерсети**.

В разных подсетях допустимы разные сетевые технологии, разные стеки протоколов, поэтому при создании стека **TCP/IP** уже заранее предполагалось наличие **разных типов локальных адресов**.

Если подсетью интерсети является локальная сеть, то **локальный адрес - это MAC - адрес**.

MAC - адрес назначается сетевым адаптерам и сетевым интерфейсам маршрутизаторов.

MAC - адреса назначаются производителями оборудования и являются уникальными, так как управляются централизованно.

Для всех существующих технологий локальных сетей **MAC - адрес имеет формат 6 байт**, например **11-AO-17-3D-BC-01**.

Надо отметить, что поскольку **протокол IP** может работать и над протоколами **более высокого уровня**. В этом случае **локальными адресами** для **протокола IP** соответственно будут **адреса соответствующих протоколов более высокого уровня**.

Следует учесть, что компьютер в локальной сети может иметь несколько **локальных адресов** даже при одном сетевом адаптере. И наоборот, некоторые сетевые устройства вообще не имеют **локальных адресов**. Например, к таким устройствам относятся глобальные порты маршрутизаторов, предназначенные для соединений типа **"точка-точка"**.

IP-адреса - основной тип адресов сетевого уровня.

На основании IP-адресов сетевой уровень передает пакеты между сетями.

IP-адреса состоят из **4 байт**.

IP-адрес назначается администратором во время конфигурирования компьютеров и маршрутизаторов.

IP-адрес состоит из двух частей: **номера сети** и **номера узла**.

Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения **Internet (Internet Network Information Center, InterNIC)** , если сеть должна работать как составная часть **Internet**. Обычно поставщики услуг **Internet** получают диапазоны адресов у подразделений **InterNIC**, а затем распределяют их между своими абонентами.

Номер узла в **протоколе IP** назначается **независимо** от **локального адреса** узла!

Маршрутизатор по определению входит сразу в несколько сетей. Поэтому каждый порт маршрутизатора имеет собственный **IP-адрес**.

Конечный узел также может входить в несколько **IP-сетей**. В этом случае компьютер должен иметь несколько **IP-адресов**, по числу сетевых связей.

Таким образом, **IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение**. Напоминаю, что мы поговорим об этом немного позже более подробно.

Символьные имена

Символьные имена имеют символьный вид и в **IP-сетях** называются **доменными**.

Доменные имена строятся по иерархическому признаку. Полное **символьное имя в IP-сетях** состоит из нескольких составляющих, которые разделяются точкой. Они перечисляются в следующем порядке (сдева-направо):

- сначала простое **имя конечного узла**
- затем **имя группы узлов** (например, имя организации)
- затем **имя более крупной группы** (**поддомена**)

И так до имени домена самого высокого уровня (например, домена объединяющего организации по географическому принципу: **UA** - Украина, **RU** - Россия, **UK** - Великобритания, **SU** - США)

Примеров **доменного имени** может служить имя **base2.sales.zil.ru**. Между **доменным именем** и **IP-адресом** узла **нет никакого соответствия**, поэтому необходимо использовать какие-то дополнительные таблицы или службы, чтобы узел интерсети однозначно мог определяться в сети, как по **доменному имени**, так и по **IP-адресу**.

IP адреса. Классы IP адресов

Самое первое, что надо сразу уяснить - **IP-адреса** назначаются не узлам составной сети. **IP адреса** назначаются сетевым интерфейсам узлов составной сети.

Очень многие (если не большинство) компьютеров в **IP сети** имеют единственный сетевой интерфейс (и как следствие один **IP адрес**). Но компьютеры и другие устройства могут иметь несколько (если не больше) сетевых интерфейсов - и каждый интерфейс будет иметь свой собственный **IP адрес**.

Так устройство с 6 активными интерфейсами (например, маршрутизатор) будет иметь **6 IP адресов** - по одному на каждый интерфейс в каждой сети, к которой он подключен.

Итак, **IP адрес** определяет однозначно **сеть** и **узел**, который подключен к данной сети. **IP адрес** имеет длину **4 байта (8 бит)**, это дает в совокупности **32 бита** доступной информации.

Для улучшения читабельности, **IP адрес** записывается в виде четырех чисел, **разделенных точками**:

например, **128.10.2.30** - десятичная форма представления адреса - **4 (десятичных) числа, разделенных (.) точками**, а **10000000 00001010 00000010 00011110** - двоичная форма представления этого же адреса. **4-ре 8-ми разрядных числа (октета)**

*Так как каждое из четырех чисел - это десятичное представление 8-битного байта, то каждое число может принимать значения от **0 до 255** (что дает **256** уникальных значений - помните, ноль - это тоже величина).*

Здесь надо отметить:

Десятичная форма записи **IP-адреса** используется в основном при в операционных системах, как наиболее удобная при настройке.

Кроме двоичной формы, встречается шестнадцатеричная форма записи **IP-адреса: C0.94.1.3**

Для сведения: использование **32-разрядных** двоичных чисел позволяет создавать **4 294 967 296 уникальных IP-адресов** - более чем достаточно для любой частной **интрасети** (хотя сеть **Internet** скоро может начать испытывать нехватку уникальных адресов).

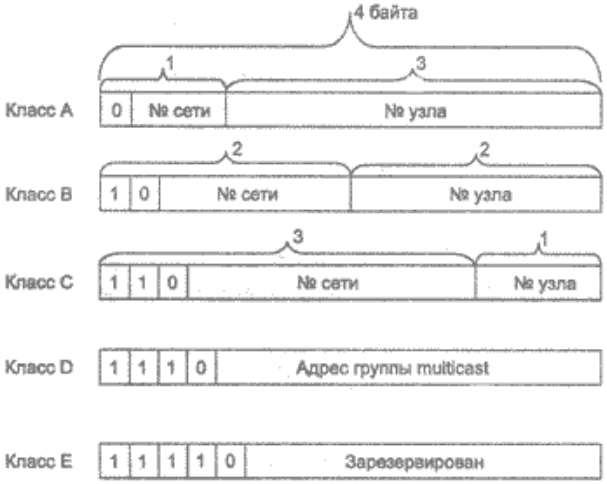
IP адрес состоит из двух логических частей - номера сети и номера узла в сети.

Конечно же, сразу возникает вопрос: а как определить в одном адресе, где **номер сети**, а где **номер узла**? Можно условится использовать, например, первые **8 бит адреса** для **номера сети**, остальные для **номеров узлов** в той сети, или **первые 16 бит**, или **первые 24 бита**. Но в таком случае адресация получается абсолютно не гибкой, мы будем иметь или много маленьких сетей и мало больших, или наоборот.

Для того чтобы более рационально определиться с величиной сети и при том разграничить какая часть **IP-адреса** относится к **номеру сети**, а какая - к **номеру узла** условились использовать **систему классов**. Система классов использует значения **первых бит адреса**.

Но, таким образом, что значения этих **первых бит адреса** являются признаками того, к какому **классу** относится тот или иной **IP-адрес**.

Классы IP-адресов:



Итак, давайте в отдельной таблице приведем диапазоны **номеров сетей** и **максимальное число узлов**, соответствующих каждому **классу сетей**:

Класс	**Первые биты**	**Наименьший адрес сети**	**Наибольший адрес сети**	**Максимальное количество узлов**
A	**0**	1.0.0.0	126.0.0.0	2^{24} (16 777 216-2)
B	**10**	128.0.0.0	191.255.0.0	2^{16} (65536-2)
C	**110**	192.0.1.0	223.255.255.0	2^{8} (256-2)
D	**1110**	224.0.0.0	239.255.255.255	Multicast
E	**11110**	240.0.0.0	247.255.255.255	зарезервирован

Сети класса С являются **наиболее распространенными**.

- Если **адрес** начинается с последовательности **1110**, то он является адресом **класса D** и обозначает **особый, групповой адрес - multicast**.

Если в пакете в качестве **адреса назначения** указан **адрес класса D**, то **такой пакет должны получить все узлы**, которым присвоен **данный адрес**. Но об этом мы еще поговорим ниже.

- Если адрес начинается с последовательности 11110, то это значит, что данный адрес относится к классу Е. Адреса этого класса зарезервированы для будущих применений.

Таким образом, можно однозначно определить, что:

Большие сети получают адреса **класса А**, **средние** - **класса В**, а **маленькие** - **класса С**. В зависимости от того к какому классу (**А В С**) принадлежит адрес, **номер сети** может быть

представлен **первыми 8, 16 или 24 разрядами**, а **номер хоста** - **последними 24, 16 или 8 разрядами**.

Такова традиционная **система классов**, но и она не достаточно гибко определяет границы между **номером сети** и **номером узла**. С использованием классов границы проходят по **границам байтов**. Существует другой метод, который может проводить разделение границы между **номером сети и номером узла** в одном **IP-адресе по границам битов!** Но всему свое время, и прежде чем, познакомится с этим способом, мы должны рассмотреть следующий, очень немаловажный момент, который касается "правил исключений" в **IP - адресации**.

Особые IP-адреса

Существуют некоторые значения **IP-адресов**, которые **зарезервированы заранее**, то есть существуют **IP-адреса**, которые предназначены для **особых целей**. Для каких?

1) Если весь **IP-адрес** состоит **только из двоичных нулей**, то он обозначает **адрес того узла, который сгенерировал этот пакет**;

0 0 0 0 ..... 0 0 0 0

этот режим используется только в некоторых сообщениях **протокола межсетевых управляющих сообщений ICMP**.

2) Если в **поле номера сети** стоят только **нули**, то по умолчанию считается, что **узел назначения принадлежит той же самой сети**, что и **узел, который отправил пакет**.

0 0 0 0 .....0 Номер узла

IP-адрес с **нулевым номером хоста** используется для адресации ко всей сети. Например, в сети **класса C** с номером **199.60.32 IP-адрес 199.60.32.0** обозначает сеть в целом.

3) Если все **двоичные разряды IP-адреса равны 1**, то **пакет с таким адресом назначения должен рассылаться всем узлам**, находящимся в той же сети, что и **источник этого пакета**.

1 1 1 1 .....1 1

Такая рассылка называется **ограниченным широковещательным сообщением (limited broadcast)** .

4) Если в **поле номера узла назначения** стоят **только единицы**, то **пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером сети**. Например, пакет с адресом **192.190.21.255** доставляется всем узлам сети **192.190.21.0**.

Номер сети 1111.....11

Такая рассылка называется широковещательным сообщением (broadcast).

Предположим, например, что один из хостов в сети **класса C** с сетевым адресом **199.60.32.0** собирается направить сообщение всем остальным хостам, находящимся в той же сети. В этом случае сообщение должно быть передано на адрес **199.60.32.255**.

При **адресации** хостов интерсети администратор должен обязательно учитывать все ограничения, которые вносятся **особым назначением некоторых IP-адресов**.

Таким образом, каждый администратор должен знать, что **ни номер сети, ни номер узла не может состоять только из одних двоичных единиц или только из одних двоичных нулей**. Отсюда следует, что **максимальное количество узлов**, приведенное в таблице для сетей каждого класса, **на практике должно быть уменьшено на 2**.

Особый смысл имеет IP-адрес, первый октет которого равен 127. Этот адрес зарезервирован для тестирования программ и взаимодействия процессов в пределах одной машины.

Когда программа посылает данные по **IP-адресу 127.0.0.1**, то образуется как бы "петля". Данные не передаются по сети, а возвращаются модулям верхнего уровня, как только что принятые.

Поэтому **в IP-сети запрещается присваивать машинам IP-адреса, начинающиеся со 127! Этот адрес имеет название loopback**.

Можно отнести адрес **127.0.0.0** ко внутренней сети модуля маршрутизации узла, а адрес **127.0.0.1** - к адресу этого модуля на внутренней сети.

На самом деле любой адрес сети **127.0.0.0** служит для обозначения своего модуля маршрутизации, а не только **127.0.0.1**, например **127.0.0.3**.

В **протоколе IP** нет понятия широковещательности в том смысле, в котором оно используется в протоколах **канального уровня** локальных сетей, когда данные должны быть доставлены абсолютно всем узлам.

Как **ограниченный широковещательный IP-адрес**, так и **широковещательный IP-адрес** имеют свои пределы распространения в **интерсети**.

- они ограничены либо сетью, к которой принадлежит **узел-источник пакета**, либо сетью, **номер которой указан в адресе назначения**. Поэтому деление сети с помощью маршрутизаторов на части локализует широковещательный шторм пределами одной из составляющих общую сеть частей просто потому, что **нет способа адресовать пакет одновременно всем узлам всех сетей составной сети**.

Нами уже упоминалась выше в таблице форма **группового IP-адреса - multicast**. Так вот именно **IP адрес multicast** означает, что данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса.

Узлы сами идентифицируют себя, то есть определяют, к какой из групп они относятся. Один и тот же узел может входить в несколько групп. Члены какой-либо **группы multicast** не обязательно должны принадлежать одной сети. В общем случае они могут распределяться по совершенно различным сетям, находящимся друг от друга на произвольном количестве хопов.

Групповой адрес не делится на поля номера сети и узла и обрабатывается маршрутизатором особым образом.

Основное назначение **multicast-адресов** - распространение информации по схеме **"один-ко-многим"**.

Она работает следующим образом: хост, который хочет передавать одну и ту же информацию многим абонентам, с помощью **специального протокола IGMP (Internet Group Management Protocol)** сообщает о создании в сети новой **мультивещательной группы** с определенным адресом.

Машрутизаторы, поддерживающие **мультивещательность**, распространяют информацию о создании новой группы в сетях, подключенных к портам этого маршрутизатора.

Хосты, которые хотят присоединиться к вновь создаваемой **мультивещательной группе**, сообщают об этом своим локальным маршрутизаторам и те передают эту информацию хосту, инициатору создания новой группы.

Чтобы маршрутизаторы могли автоматически распространять пакеты с адресом **multicast** по составной сети, необходимо использовать в конечных маршрутизаторах специальные **модифицированные протоколы обмена маршрутной информацией**.

В общем, **групповая адресация** была предназначена для экономичного распространения в **Internet** или большой корпоративной сети аудио- или видеопрограмм, предназначенных сразу большой аудитории слушателей или зрителей.

Надо сказать, что если такие средства найдут широкое применение (сейчас они представляют в основном небольшие экспериментальные островки в общем **Internet**), то **Internet** сможет создать серьезную конкуренцию радио и телевидению.

Ну что ж, давайте, сделаем итог, который закрепит наше представление о том, что означает **IP-адрес**:

IP адрес может означать одно из трех:

1. **Адрес IP сети** (группа **IP** устройств, имеющих доступ к общей среде передаче - например, все устройства в сегменте **Ethernet**). **Сетевой адрес** всегда имеет биты

интерфейса (**хоста**) адресного пространства **установленными в 0** (если сеть не разбита на подсети - как мы еще увидим);

2. **Широковещательный адрес IP сети** (адрес для 'разговора' со всеми устройствами в **IP сети**). **Широковещательные адреса** для сети всегда имеют **хостовые биты адресного пространства установленными в 1** (если сеть не разбита на подсети - опять же, как мы вскоре увидим).
3. **Адрес интерфейса** (например **Ethernet-адаптер** или **PPP интерфейс** хоста, маршрутизатора, сервера печать итд). Эти адреса могут иметь любые значения **хостовых битов**, **исключая все нули или все единицы** - чтобы не путать с адресами сетей и **широковещательными адресами**.

Для сети класса A ...

(один байт под адрес сети, три байта под номер хоста)

10.0.0.0 сеть **класса A**, потому что **все хостовые биты равны 0**.

10.0.1.0 адрес хоста в этой сети

10.255.255.255 широковещательный адрес этой сети,
поскольку все сетевые биты установлены в **1**

Для сети класса B...

(два байта под адрес сети, два байта под номер хоста)

172.17.0.0 сеть **класса B**

172.17.0.1 адрес хоста в этой сети

172.17.255.255 сетевой широковещательный адрес

Для сети класса C...

(три байта под адрес сети, один байт под номер хоста)

192.168.3.0 адрес сети **класса C**

192.168.3.42 хостовый адрес в этой сеть

192.168.3.255 сетевой **широковещательный адрес**

Едва ли не все доступные сетевые **IP** адреса принадлежат **классу C**.

Маски в IP адресации

Итак, рассмотрена традиционная схема деления **IP-адреса** на **номер сети**, и **номер узла**, которая основана на понятии **класса**. **Класс** определяется значениями нескольких **первых бит адреса**. Теперь, например, можно определить, что поскольку первый байт адреса **185.23.44.206** попадает в диапазон **128-191**, то этот адрес относится к **классу B**, а значит, номером сети являются первые два байта, дополненные двумя нулевыми байтами - **185.23.0.0**, а номером узла - **0.0.44.206**.

Очевидно, что определение **номеров сети** по первым байтам адреса также не вполне гибкий механизм для адресации. А что если использовать какой-либо другой признак, с помощью которого можно было бы более **гибко** устанавливать границу между **номером сети** и **номером узла**?

В качестве такого признака сейчас получили широкое распространение **маски**.

Маска - это тоже **32-разрядное** число, она имеет такой же вид, как и **IP-адрес**. Маска **используется в паре с IP-адресом**, но не совпадает с ним.

Принцип отделения **номера сети** и **номера узла** сети с использованием **маски** состоит в следующем:

Двоичная запись маски содержит *единицы* в тех разрядах, которые в IP-адресе должны представляться как номер сети и *нули* в тех разрядах, которые представляются как номер хоста.

Каждый класс **IP-адресов** (**A, B и C**) имеет свою **маску**, используемую по умолчанию.

Поскольку **номер сети** является цельной частью адреса, **единицы в маске** также должны представлять непрерывную последовательность.

Таким образом, для стандартных **классов сетей маски** имеют следующие значения:

- **класс А - 11111111. 00000000. 00000000. 00000000 (255.0.0.0)** ;
- **класс В - 11111111. 11111111. 00000000. 00000000 (255.255.0.0)** ;
- **класс С - 11111111.11111111.11111111.00000000 (255.255.255.0)** .

Например:

Если адресу **185.23.44.206** назначить **маску 255.255.255.0**, то смотрим, что единицы в маске заданы в трех байтах, значит **номер сети** будет **185.23.44.0**, а не **185.23.0.0**, как это определено правилами системы классов.

Для записи **масок** используются и другие форматы, например, удобно интерпретировать значение **маски**, записанной в **шестнадцатеричном коде**:

FF.FF.00.00 - **маска для адресов класса В**.

Часто встречается и такое обозначение: IP-адрес/префикс сети. Например, **185.23.44.206/16** - эта запись говорит о том, что **маска** для этого адреса содержит **16 единиц** (префикс сети), или что в указанном **IP-адресе** под **номер сети** отведено **16** двоичных разрядов.

Нотация с префиксом сети также известна как бесклассовая междоменная маршрутизация (Classless Interdomain Routing - CIDR).

Таким образом, очень легко, снабжая каждый IP-адрес произвольной маской (не обязательно кратной 8), отказаться от понятий **классов адресов** и тем самым сделать более гибкой систему IP адресации.

Рассмотрим пример: для IP-адреса **129.64.134.5** назначим **маску 255.255.128.0,** что в двоичном виде будет выглядеть так:

IP-адрес 129.64. 134.5 - 10000001.01000000.1 0000110.00000101
Маска 255.255.128.0 - 11111111.11111111.1 0000000.00000000

Здесь **17 последовательных единиц в маске**, "накладываются" на IP-адрес, и определяют номер сети : **10000001. 01000000. 10000000. 00000000** или **129.64.128.0**, а номер узла **0000110.00000101** или **0.0.6.5**.

Механизм масок очень широко распространен в **IP-маршрутизации**, причем **маски** могут использоваться для самых разных целей. С их помощью администратор может структурировать свою сеть, **не требуя от поставщика услуг дополнительных номеров сетей!**

На основе этого же механизма поставщики услуг могут **объединять адресные пространства нескольких сетей** путем введения так называемых **"префиксов"** с целью уменьшения объема **таблиц маршрутизации**, и повышения за счет этого производительности маршрутизаторов. (Создание надсетей).

Маски при записи всегда "неразлучны" с соответствующими адресами, **IP-адрес маска подсети** - именно так теперь и мы будем описывать адрес любого хоста сети.

Порядок назначения IP адресов. Автономные IP адреса. Автоматизация назначения IP адресов

Номера сетей могут назначаться либо **централизованно**, если сеть является частью **Internet**, либо **произвольно**, если сеть работает **автономно**. **Номера узлов** и в том и в другом случае администратор назначает самостоятельно по своему усмотрению, не выходя, разумеется, из разрешенного для этого класса сети диапазона.

Главную роль в **централизованном распределении IP-адресов** до некоторого времени играла организация **InterNIC** (Network Information Center), однако с ростом сети задача распределения адресов стала слишком сложной. **InterNIC** делегировала часть своих функций другим организациям и крупным поставщикам услуг **Internet** -

провайдерам. В частности распределением **IP-адресов** для подключения к сети Internet теперь занимаются **провайдеры**.

С тех пор, как появилась и стала широко распространяться сеть **Internet**, уже прошло не мало времени. И теперь уже становится актуальным вопрос о **дефиците IP-адресов**. Если говорить о реальной обстановке при распределении адресов для пользователей **Internet**, то сейчас очень трудно получить адрес **класса B** и уже практически невозможно стать обладателем адреса **класса A**! При этом всем надо сказать, что **дефицит IP-адресов** вызван не совсем постоянным ростом сетей, а просто нерациональным их использованием. Очень часто владельцы сети **класса C** расходуют лишь небольшую часть из имеющихся у них **254 адресов**.

Рассмотрим пример, когда две сети необходимо соединить глобальной связью.
В таких случаях в качестве канала связи используют два маршрутизатора, соединенных по схеме **"точка-точка"**.

В ситуации, которая приведена в примере, для вырожденной сети, образованной каналом, связывающим порты двух смежных маршрутизаторов, приходится выделять **отдельный номер сети**, хотя в этой сети имеются всего **2 узла**.

Давайте рассмотрим другую ситуацию: какие **IP-адреса** может использовать администратор, если провайдер услуг **Internet** не назначил ему никакого адреса? Если, к примеру, мы точно знаем, что сеть, которую мы администрируем никогда в будущем не будет подключаться к **Internet** (работает в **"автономном режиме"**), тогда мы можем использовать любые **IP-адреса**, соблюдая правила их назначения, о которых шла речь выше. Для простоты можно использовать адреса **класса C**: в этом случае не придется вычислять значение **маски** подсети и вычислять адрес для каждого хоста.

В этом случае мы должны будем просто назначить каждому сегменту нашей локальной сети его собственный сетевой номер **класса C**.

Если все сегменты нашей локальной сети имеют собственные сетевые номера **класса C**, то в каждом сегменте можно создать по **254** номера хостов.

Однако если у нас есть хотя бы небольшая вероятность того, что когда-либо в будущем наша сеть может быть подключена к Internet, не следует использовать такие IP-адреса! Они могут привести к конфликту с другими адресами в Internet. Чтобы избежать таких конфликтов, нужно использовать IP-адреса, **зарезервированные для частных сетей**.

Для этой цели зарезервированы специально несколько блоков **IP-адресов**, которые называются **автономными**.

Автономные IP адреса

Автономные адреса зарезервированы для использования **частными сетями**. Они обычно используются организациями, которые имеют свою частную большую сеть - **intranet** (локальные сети с архитектурой и логикой **Internet**), но и маленькие сети часто находят их полезными.

Эти адреса не обрабатываются маршрутизаторами Internet, ни при каких условиях. Эти адреса выбраны из разных классов.

Класс	**От IP-адреса**	**До IP-адреса**	**Всего узлов адресов в диапазоне**

A	**10.0.0.0**	**10.255.255.255**	16 777 216-2
B	**172.16.0.0**	**172.31.255.255**	65 536-2
C	**192.168.0.0**	**192.168.255.255**	256-2

Эти адреса являются зарезервированными для **частных сетей**. Таким образом, если в будущем мы решим все-таки подключить свою сеть к **Internet**, то даже если трафик с одного из хостов в нашей сети и попадет каким-либо образом в **Internet**, конфликта между адресами произойти не должно. Маршрутизаторы в **Internet** запрограммированы так, чтобы не транслировать сообщения, направляемые с зарезервированных адресов или на них.

Надо сказать, что использование **автономных** IP-адресов имеет и недостатки, которые состоят в том, что если мы будем подключать свою сеть к **Internet**, то нам придется заново настроить конфигурацию хостов, соединяемых с **Internet**.

Можно сказать, что **подсеть** - это метод, состоящий в том, чтобы взять **сетевой IP адрес** и **локально** разбить его так, чтобы этот **один сетевой IP адрес** мог в действительности **использоваться в нескольких взаимосвязанных локальных сетях**.

О**дин сетевой IP адрес может использоваться только для одной сети! Самое важное**: разбиение на **подсети** - это **локальная настройка**, она не видна "снаружи". Разбиение одной большой сети на **подсети**, значительно разгружает общий трафик и позволяет повысить безопасность всей сети в целом.

Алгоритм разбиения сети на **подсети**

1) Устанавливаем физические соединения (сетевые кабели и сетевые соединители - такие как маршрутизаторы);
2) Принимаем решение насколько большие/маленькие **подсети** вам нужны, исходя из количества устройств, которое будет подключено к ним, то есть, сколько **IP адресов** требуется использовать в каждом сегменте сети.
3) Вычисляем соответствующие **сетевые маски** и **сетевые адреса**;
4) Раздаем каждому интерфейсу в каждой сети свой **IP адрес** и соответствующую **сетевую маску**;
5) Настраиваем каждый маршрутизатор и все сетевые устройства;
6) Проверяем систему, исправляем ошибки.
Сейчас наша задача разобраться с тем, как выполнить 2-й и 3-й шаги.

Пример 1

Предположим, что мы хотим разбить нашу сеть на подсети, но имеем только один **IP-адрес сети 210.16.15.0**.

Решение:

IP-адрес 210.16.15.0 - это адрес **класса C**. Сеть **класса C** может иметь до **254** интерфейсов (хостов) плюс **адрес сети (210.16.15.0)** и **широковещательный адрес (210.16.15.255)**.

Первое: определить **"размер" подсети**.

Существует зависимость между количеством создаваемых **подсетей** и "потраченными" **IP адресами**.

Каждая отдельная **IP сеть** имеет **два адреса, неиспользуемые для интерфейсов (хостов)**:

- **IP адрес собственно сети и широковещательный адрес**.

При разбивке на подсети **каждая подсеть требует свой собственный уникальный IP адрес сети и широковещательный адрес** - и они должны быть корректно выбраны из диапазона адресов **IP сети**, которую мы делим на **подсети**.

Итак, если при разбивке **IP сети** на **подсети**, в каждой из которых есть **два сетевых адреса** и **два широковещательных адреса** - надо помнить, что каждая из них уменьшит количество используемых интерфейсных (хостовых) адресов на два.

Это мы должны всегда учитывать при вычислении **сетевых номеров**. Следующий шаг - **вычисление маски подсети и сетевых номеров**.

Сетевая маска - это то, что выполняет все логические манипуляции по разделению **IP сети на подсети**.

Для всех трех классов **IP сетей** существуют стандартные сетевые **маски**:

- **Класс A** (8 сетевых битов) : **255.0.0.0**
- **Класс B** (16 сетевых битов): **255.255.0.0**
- **Класс C** (24 сетевых бита): **255.255.255.0**

Чтобы создать **подсеть**, нужно изменить маску подсети для данного класса адресов.

Номер подсети можно задать, позаимствовав нужное для нумерации подсетей количество разрядов в номере хоста. Для этого берутся левые (старшие) разряды из номера хоста, в маске же взятые разряды заполняются единицами, чтобы показать, что эти разряды теперь нумеруют не узел а подсеть. Значения в остающихся разрядах маски подсети оставляются равными **нулю**; это означает, что оставшиеся разряды в номере хоста в **IP-адресе** должны использоваться как новый (меньший) номер хоста.

Например, чтобы **разбить сетевой адрес** на **две** подсети, мы должны позаимствовать **один хостовый бит**, установив **соответствующий бит в сетевой маске первого хостового бита в 1**.

Если нам нужно **четыре подсети** - используем **два хостовых бита**, если **восемь подсетей** - **три бита** и т.д. Однозначно, что если нам нужно **пять подсетей**, то мы будем использовать **три хостовых бита**. Соответствующим образом изменяется и **маска подсети**:

Для адресов **класса C**, при разбиении на **2 подсети** это дает **маску** -
11111111.11111111.11111111.10000000 или **255.255.255.128**
при разбиении на **4 подсети** маска в двоичном виде -
11111111.11111111.11111111.11000000, или в десятичном **255.255.255.192**. и т.д.

Для нашего адреса сети класса C **210.16.15.0**, можно определить следующих несколько способов разбивки на **подсети**: -

Число подсетей	Число хостов	Сетевая маска
2	126	255.255.255.128 (11111111.11111111.11111111.10000000)
4	62	255.255.255.192 (11111111.11111111.11111111.11000000)
8	30	255.255.255.224 (11111111.11111111.11111111.11100000)
16	14	255.255.255.240 (11111111.11111111.11111111.11110000)
32	6	255.255.255.248 (11111111.11111111.11111111.11111000)
64	2	255.255.255.252 (11111111.11111111.11111111.11111100)

Теперь нужно решить вопрос об **адресах сетей и широковещательных адресах,** и о диапазоне **IP адресов** для каждой из этих сетей.
Снова, принимая во внимание только сетевые адреса **класса C.** и показав только последнюю (хостовую) часть адресов, мы имеем:

Сетевая маска	Подсети	Сеть	Broadcast	MinIP	MaxIP	Хосты	Всего хостов
128	2	0	127	1	126	126	
		128	255	129	254	126	252
192	4	0	63	1	62	62	

		64	127	65	126	62	
		128	191	129	190	62	
		192	255	193	254	62	248
224	8	0	31	1	30	30	
		32	63	33	62	30	
		64	95	65	94	30	
		96	127	97	126	30	
		128	159	129	158	30	
		160	191	161	190	30	
		192	223	193	222	30	
		224	255	225	254	30	240

Из этой таблицы сразу можем увидеть, что **увеличение количества подсетей сокращает общее количество доступных хостовых адресов**. Теперь, вооруженные этой информацией, мы готовы назначать **хостовые и сетевые IP адреса и сетевые маски**.

Пример 2
Определим, сколько нужно подсетей для нашей сети **класса С**, чтобы разбить ее на подсети по **10 хостов** в каждой.
Решение:

Сеть **класса С** может обслуживать всего **254** хоста плюс адрес сети и широковещательный адрес.
Для адресации **10-ти** хостов **3-х** разрядов недостаточно, поэтому необходимо **4-е** разряда. Итак, из восьми возможных для класса **С**, нам нужно только **4** разряда для адресации **10** хостов, остальные можно использовать как сетевые для адресации **подсетей**. Мы уже знаем, что каждая подсеть уменьшает количество возможных хостовых адресов в два раза. Для адресации **16 подсетей** необходимо использовать **4 разряда**. Итак, посчитаем теперь количество узлов в каждой из **16 подсетей**: $\mathbf{2^4 - 2 = 14}$ **хостов**. Это количество с запасом удовлетворяет условие задачи.

Вычислим **маску подсети**, в этом случае она имеет вид:
11111111.11111111.11111111.11110000 или
255.255.255.240

Мы должны будем указать эту маску при настройке конфигурации каждого хоста в нашей сети (независимо от того, в какой подсети находится хост).
Теперь, например, мы можем сказать, адрес **192.168.200.246** с маской **255.255.255.240** - означает номер сети **192.168.200.240** и номер узла **0.0.0.6**.

Пример 3
Теперь, для всех трех классов определим соответственно маски подсети, и максимальное количество узлов возможное в каждой из этих подсетей, если необходимо разбить соответственно сеть **класса А**, сеть **класса В**, сеть **класса С** на отдельные **4 подсети**.
Решение:

Для сети **класса А**:

Максимальное количество узлов **16 777 216**. Для адресации 4-х подсетей необходимо **2** разряда, значит остается **22 разряда** для адресации **хостов**. Таким образом, каждая из четырех подсетей способна обслуживать $\mathbf{2^{22} - 2 = 4\ 194\ 302}$ хоста в каждой из подсетей.

Число подсетей	Число хостов	Сетевая маска
4	4 194 302	255.192.0.0 (11111111. 11000000.00000000.00000000)

Для сети **класса B**
Максимальное количество узлов - **65 536**. Для адресации **4-х** подсетей в сетевом адресе **класса B** также нужно использовать **2 разряда**, но теперь свободными остается **14 разрядов**. Таким образом, каждая из подсетей может обслуживать 2^{14} **- 2 = 16 382** хостов.

Число подсетей	Число хостов	Сетевая маска
4	16 382	255.255.192.0 (11111111.11111111. 11000000.00000000)

Пример с сетью **класса C** мы уже рассматривали. Итак, теперь самое главное уметь в **двоичном виде** читать **IP адреса**, а с помощью маски легко можно определить **номер сети** и **номер узла**. Вот теперь, можно сказать, теория заканчивается, для нашей работы очень важно "окрепнуть" в навыках работы с **IP адресами**, уметь разделять сети на **подсети**, вычислять **маски подсети**, и назначать возможные **адреса сетей**, и **адреса хостов** - это прямая обязанность сетевых администраторов.

Надо сказать, что назначение **IP-адресов** узлам сети даже при не очень большом размере сети представляет для администратора очень утомительную процедуру. Поэтому сразу вторым шагом в **IP адресации** разработчики решили автоматизировать этот процесс.

С этой целью был разработан протокол **Dynamic Host Configuration Protocol (DHCP)**, который освобождает администратора от этих проблем, **автоматизируя процесс назначения IP-адресов**.

DHCP может поддерживать способ **автоматического динамического распределения адресов**, а также **более простые способы ручного и автоматического статического назначения адресов**. **Протокол DHCP** работает в соответствии с моделью **клиент-сервер**.

Во время старта системы компьютер, являющийся **DHCP-клиентом**, посылает в сеть **широковещательный запрос** на получение **IP-адреса**. **DHCP - сервер** откликается и посылает сообщение-ответ, содержащее **IP-адрес**. Предполагается, что **DHCP-клиент и DHCP-сервер находятся в одной IP-сети**.

При **динамическом** распределении адресов **DHCP-сервер** выдает адрес клиенту на **ограниченное время**, оно называется **временем аренды (lease duration)** . Это дает возможность впоследствии повторно использовать этот **IP-адрес** для назначения **другому** компьютеру.

Основное преимущество DHCP - автоматизация рутинной работы администратора по конфигурированию стека TCP/IP на каждом компьютере. Иногда **динамическое** разделение адресов позволяет строить **IP-сеть**, количество узлов которой превышает количество имеющихся в распоряжении администратора **IP-адресов**.

В **ручной процедуре** назначения **статических адресов** активное участие принимает администратор, который предоставляет **DHCP - серверу** информацию о **соответствии IP-адресов физическим адресам** или другим идентификаторам клиентов. **DHCP-сервер**, пользуясь этой информацией, всегда выдает определенному клиенту назначенный администратором адрес.

При **автоматическом статическом** способе **DHCP-сервер** присваивает **IP-адрес** из **пула наличных IP-адресов** без вмешательства оператора. А границы **пула назначаемых адресов** задает администратор при конфигурировании **DHCP-сервера**.

Адрес дается клиенту из **пула** в **постоянное пользование**, то есть с **неограниченным сроком аренды**. Между **идентификатором клиента** и его **IP-адресом** по-прежнему, как и при **ручном** назначении, существует постоянное соответствие. Оно устанавливается в момент **первого** назначения **DHCP-сервером IP-адреса** клиенту. При всех последующих запросах сервер возвращает тот же самый **IP-адрес**.

DHCP обеспечивает надежный и простой способ конфигурации сети **TCP/IP**, **гарантируя отсутствие дублирования адресов за счет централизованного управления их распределением**.
Администратору в этом случае остается только управляет **процессом назначения адресов** с помощью параметра **"продолжительность аренды"**, которая определяет, как долго компьютер может использовать назначенный **IP-адрес**, перед тем как снова запросить его от **DHCP-сервера** в аренду.

Задания

1) **IP-адрес 190.235.130.N** (где N-номер варианта согласно таблице, данной ниже), сетевая маска **255.255.192.0**. Определите, **адрес сети** и **адрес узла.**
2) Определите **маски подсети** для случая разбиения сети с номером **192.0.0.0** на **32 подсети**.
3) Существует единая корпоративная сеть, количество узлов сети - **50 450**. Этой сети выделен адрес для выхода в **Internet 192.124.0.0**. Вы решили не требовать от провайдера дополнительных адресов и организовать **8** филиалов в этой сети. Спрашивается:
- Какое максимальное количество узлов может быть в каждом из филиалов? Вычислите **сетевые маски** и возможный диапазон **адресов хостов** для каждого из филиалов.
4) Вы являетесь администратором корпоративной сети из **6 подсетей**, в каждой подсети по 25 компьютеров. Необходимо используя один номер сети **класса С 192.168.10.0**, определить правильно ли выбран **размер подсети**, и назначить маски и возможные **IP-адреса** хостам сети.
5)Разделить IP-сеть на подсети в соответствии с вариантом из таблицы. Для каждой подсети указать широковещательный адрес.

Таблица 5.

Вариант	**Сеть**	**Подсети**
1.	192.168.16.0/24	5 подсетей с 100, 20, 10, 6 и 40 узлами
2.	194.45.27.0/24	5 подсетей с 34, 20, 62,10 и 40 узлами
3.	56.1.1.0/16	4 подсети с 65, 22, 10 и 30 узлами
4.	147.168.0.0/16	5 подсетей с 56, 16, 10 и 70 узлами
5.	193.68.61.0/24	5 подсетей с 100, 20, 10 и 40 узлами
6.	192.100.0.0/24	4 подсети с 80, 20, 12 и 20 узлами
7.	195.18.11.0/24	4 подсети с 110, 11, 10 и 40 узлами
8.	207.15.0.0/24	4 подсети с 28, 80, 10 и 40 узлами
9.	222.11.0.0/24	4 подсети с 110, 20, 10 и 50 узлами
10.	200.2.2.0/24	4 подсети с 100, 20, 10 и 40 узлами
11.	201.111.32.0/16	5 подсетей с 170, 590, 1500, 800 и 254 узлами
12.	128.200.1.0/16	5 подсетей с 115, 300, 200, 128 и 420 узлами
13.	53.11.0.0/16	5 подсетей с 165, 222, 128, 110 и 430 узлами
14.	146.77.0.0/16	5 подсетей с 550, 116, 200, 256 и 170 узлами
15.	194.54.45.0/24	4 подсети с 103, 39, 10 и 16 узлами
16.	142.51.0.0/16	4 подсети с 180, 120, 12 и 30 узлами
17.	43.0.0.0/16	4 подсети с 151, 211, 16 и 70 узлами

Контрольные вопросы

1. Какие бывают классы IP-адресов.
2. Как по первому байту адреса определить его класс?
3. Что такое маска, на что она указывает?
4. Для чего нужны маски переменной длины?
5. Изложите алгоритм деления сетей на подсети с помощью VLM (variable length mask)

Лабораторная работа.

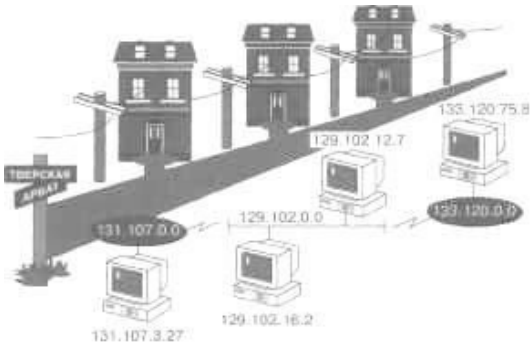
Тема: Определение диапазона IP – адресов. Выбор касса сети.

Цели работы: Изучить варианты записи IP – адресов, научиться осуществлять выбор класса сети.

Теоретическая часть

IP-адресация охватывает различные аспекты, такие как расчеты для определения IP-адреса, классы IP-адресов, общедоступные и частные IP-адреса.

Существует два типа IP-адресов: IP версии 4 (IPv4) и IP версии 6 (1Pv6). До настоящего времени наиболее распространенными были 32-битные адреса IPv4, однако 128-битные адреса IPv6 также используются и со временем, вероятно, станут основным типом IP-адресов.

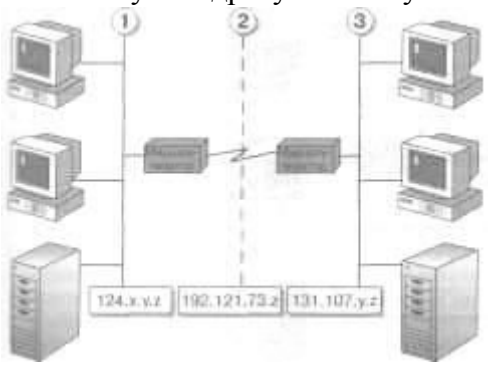


IP-адрес

IP-адрес определяет местонахождение узла в сети подобно тому, как адрес дома указывает его расположение в городе. Как и обычный адрес, IP-адрес должен быть уникальным и иметь единый формат.

Каждый IP-адрес состоит из двух частей — идентификатора сети (network ID) и идентификатора узла (host ID). Первый определяет физическую сеть. Он одинаков для всех узлов в одной сети и уникален для каждой из сетей, включенных в объединённую сеть.

Идентификатор узла соответствует конкретной рабочей станции, серверу, маршрутизатору или другому TCP/IP-узлу в данной сети. Он должен иметь уникальное значение в данной сети. Каждый узел TCP/IP однозначно определяется по своему логическому IP-адресу. Такой уникальный адрес необходим всем сетевым компонентам, взаимодействующим по TCP/IP.



Идентификаторы сетей и узлов

IP-адрес может быть записан в двух форматах — двоичном (binary) и десятичном с точками (dotted decimal). Каждый IP-адрес имеет длину 32 бита и состоит из четырёх 8-битных полей, называемых октетами (octets), которые отделяются друг от друга точками. Каждый октет представляет десятичное число в диапазоне от 0 до 255. Эти 32 разряда IP-адреса содержат идентификатор сети и узла.

Формат записи адреса в виде четырех десятичных чисел, разделенных точками, наиболее удобен для восприятия. Далее показаны различные формы записи IP-адреса.

Преобразование IP-адреса из двоичного формата в десятичный.

Вы должны уметь определять значения битов в октетах и преобразовывать их в десятичные числа. В двоичном формате каждому биту в октете сопоставлено определенное десятичное число. Максимальное десятичное значение октета равно 255 (участвует каждый бит). Каждый октет преобразуются в число отдельно от других.

Бит, установленный в 0, всегда соответствует нулевому значению. Бит, установленный в 1, может быть преобразован в десятичное число. Младший бит октета представляет десятичное число 1, а старший — 128. Максимальное значение октета (255) достигается, когда каждый его бит равен 1.

Ход работы

1.Переведите следующие двоичные числа в десятичные.

Двоичное значение	Десятичное значение
10001011	
10101010	
10111111 11100000 00000111 10000001	
01111111 00000000 00000000 00000001	

2.Переведите следующие десятичные числа в двоичные.

Двоичное значение	Десятичное значение
250	
19	
109.128.255.254	
131.107.2.89	

Теоретическая часть

Классы IP-адресов

Каждый класс IP-адресов определяет, какая часть адреса отводится под идентификатор сети, а какая — под идентификатор узла. На этом занятии Вы узнаете о различных классах IP-адресов: A,B,C.

Сообщество Интернета определило пять классов IP-адресов в соответствии с различными размерами компьютерных сетей. Microsoft TCP/IP поддерживает адреса классов A, B и C. Класс адреса определяет, какие биты относятся к идентификатору сети, а какие — к идентификатору узла. Также он определяет максимально возможное количество узлов в сети.

Класс IP-адреса идентифицируют по значению его первого октета, 32-разрядные IP-адреса могут быть присвоены в общей совокупности 3 720 314 628 узлам. Ниже показано, как определяются поля в IP-адресах разных классов.

Класс	IP-адрес	Идентификатор сети	Идентификатор узла
A	w.x.y.z	w	x.y.z
B	w.x.y.z	w.x	y.z
C	w.x.y.z	w.x.y	z

Класс A

Адреса класса A назначаются узлам очень большой сети. Старший бит в адресах этого класса всегда равен нулю. Следующие семь бит первого октета представляют идентификатор сети. Оставшиеся 24 бита (три октета) содержат идентификатор узла. Это позволяет иметь 126 сетей с числом узлов до 17 миллионов в каждой.

Класс B

Адреса класса B назначаются узлам в больших и средних по размеру сетях. В двух старших битах IP-адреса класса B записывается двоичное значение 10. Следующие 14 бит содержат идентификатор сети (два первых октета). Оставшиеся 16 бит (два октета) представляют идентификатор узла. Таким образом, возможно существование 16 384 сетей класса B, в каждой из которых около 65 000 узлов.

Класс C

Адреса класса C применяются в небольших сетях. Три старших бита IP-адреса этого класса содержат двоичное значение 110. Следующие 21 бит составляет идентификатор сети (первые три октета). Оставшиеся 8 бит (последний октет) отводится под идентификатор узла. Всего возможно около 2 000 000 сетей класса C, содержащих до 254 узлов.

Примечание В качестве идентификатора сети не может использоваться значение 127. Оно зарезервировано для диагностики и используется в качестве локальной заглушки.

Класс D

Адреса класса D предназначены для рассылки групповых сообщений. Группа получателей может содержать один, несколько или ни одного узла. Четыре старших бита в IP-адресе класса D всегда равны 1110. Оставшиеся биты обозначают конкретную группу получателей и не разделяются на части. Пакеты с такими адресами рассылаются избранной группе узлов в сети. Их получателями могут быть только специальным образом зарегистрированные узлы.

Класс E

Класс E — экспериментальный. Он зарезервирован для использования в будущем и в настоящее время не применяется. Четыре старших бита адресов класса E равны 1111.

Ход работы

Определите, к какому классу принадлежат указанные IP-адреса.

1. Укажите классы следующих IP-адресов.

Адрес	**Класс**
131.107.2.89	
3.3.57.0	
200.200.5.2	
191.107.2.10	

2. В сетях каких классов IP-адресов более 1 000 узлов?

   _____
   _____
   _____
   _____

3. В сетях каких классов IP-адресов только 254 узла?

   _____
   _____
   _____
   _____

Лабораторная работа

Конфигурирование портов и работа с таблицей коммутации.

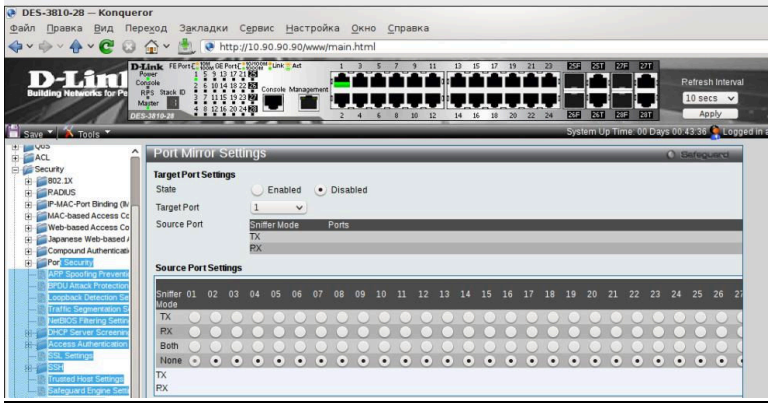
Цель работы: Получение навыков настройки портов коммутатора, изучение технологии зеркалирования портов (Port Mirroring) и принципов работы со статической таблицей перенаправления коммутатора.

Теоретические сведения:

Раздел Port Mirror:

Сегодня анализаторы сетевых протоколов эффективно используются ИТ-отделами и отделами информационной безопасности для решения широкого круга задач. С их помощью можно быстро определить причину медленной работы ИТ-сервиса или бизнес-приложения. Они позволяют документировать сетевую активность пользователей и использовать полученные данные, например, для определения источника утечки информации. Единственной «ложкой дегтя» является неудобство их использования в коммутируемых сетях. Дело в том, что анализатор протоколов должен «видеть» весь анализируемый трафик, в то время как в коммутируемой сети трафик между двумя портами коммутатора «невиден» на других его портах. Одним из способов решения данной проблемы является технология зеркалирования портов (Port Mirroring), которая поддерживается многими коммутаторами класса High End.

Зеркалирование позволяет копировать пакеты, получаемые и передаваемые с одного порта, на другой зеркальный порт (mirrored port). К зеркальному порту можно подключить устройство мониторинга (например, сетевой сниффер) для детального анализа пакетов, проходящих через первый порт.

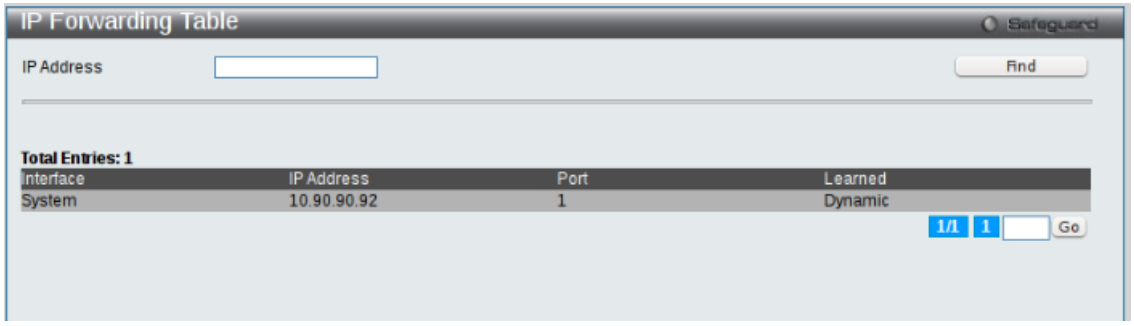


Позволяет управлять функцией зеркалирования портов

- Mirror Port State – активность функции
- Target Port – выходной порт
- Source Port – прослушиваемые порты
- Sniffer Mode – настройка прослушиваемых портов
- Tx – только исходящий трафик
- Rx – только входящий трафик
- Both – оба направления
- None – не прослушивать

Раздел Forwarding & Filtering:

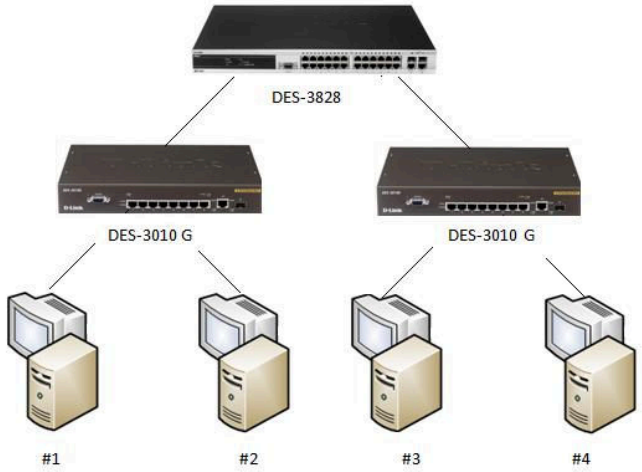
Коммутатор принимает все пакеты с присоединенных сегментов. Для каждого получаемого пакета устройство считывает адрес получателя из заголовка протокола Ethernet, и если этот пакет предназначен для системы, расположенный в другом сегменте, передает пакет в этот сегмент и только в этот сегмент. Если пакет послан системе в локальном сегменте, коммутатор отбрасывает его, поскольку данные уже достигли своего места назначения. Чтобы эффективно выполнять перенаправление получаемых пакетов, мост должен знать, какие системы в каком сегменте находятся. Мост хранит эту информацию во внутренней адресной таблице перенаправления (Forwarding Table). Механизм заполнения данной таблицы называется прозрачной маршрутизацией (Transparent Routing).



Позволяет управлять статическими записями таблицы коммутации

- Vlan ID - Vlan, в котором действительна запись
- MAC Address – MAC –адрес узла
- Port- порт , на котором находится узел

ПОРЯДОК выполнения работы:



1. Изучите раздел 2.2 «Administration» (меню «Port Configuration»).
2. Постройте топологию сети, показанную на рисунке 4.
3. Выключите один из портов коммутатора, к которому подключен один из компьютеров.
4. Попробуйте осуществить взаимодействие компьютеров. Сделайте выводы на основе полученного результата.
5. Изучите раздел 2.2 «Administration» (меню «Port Mirroring»).
6. Настройте на коммутаторе зеркало для любого из портов, к которому подключен один из компьютеров.
7. Запустите на машинах, подключенных к порту-источнику и порту-приемнику (зеркалу), утилиту tcpdump. Активизируйте сетевую активность. Сравните результаты работы утилит на обеих машинах.
8. Силами двух бригад соберите топологию сети, представленную на рисунке 5. Все линия связи должны быть подключены к портам с пропускной способностью 100 Мбит/с. Обязательно соблюдайте нумерацию портов.
9. Установите пропускную способность портов коммутатора DES-3010G, к которому подключены машины 3 и 4, равной 10 Мбит/с.
10. Настройте зеркало на коммутаторе DES-3010G, к которому подключены машины 1 и 2 следующим образом: машина 1 - приёмник, машина 2 - источник.
11. «Пингуйте» (утилита ping) одновременно машину 2 с машин 3 и 4.
12. Запустите на машинах 1 и 2 утилиту tcpdump. Сравните результаты работы утилит на обеих машинах.
13. Проделайте действия пунктов 8-12 в обратную сторону.
14. Изучите раздел 2.2 «Administration» (меню «Forward and Filtering»).
15. Создайте в статической таблице перенаправления коммутатора DES-3010G, к которому подключены машины 1 и 2, следующую некорректную запись: машина #4

подключена к порту 3. Вторая бригада должна сделать то же самое на своём коммутаторе - создать следующую некорректную запись: машина #1 подключена к порту 2.

16. Удалите из таблицы перенаправления все записи, полученные коммутатором в режиме самообучения.
17. «Пингуйте» машину #4 с машины #1 и машину #1 с машины #4.
18. На машинах #2 и #3 запустите утилиту tcpdump и убедитесь, что коммутатор перенаправляет пакеты в соответствие с созданными Вами некорректными записями в таблице коммутации.
19. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

Лабораторные работы на темы:

1. Организация статической и динамической маршрутизации

2.Настройка параметров статической и динамической маршрутизации

Теоретическая часть

Статическая маршрутизация не подходит для больших, сложных сетей потому, что обычно сети включают избыточные связи, многие протоколы и смешанные топологии. Маршрутизаторы в сложных сетях должны быстро адаптироваться к изменениям топологии и выбирать лучший маршрут из многих кандидатов.

IP сети имеют иерархическую структуру. С точки зрения маршрутизации сеть рассматривается как совокупность автономных систем. В автономных подсистемах больших сетей для маршрутизации на остальные автономные системы широко используются маршруты по умолчанию.

Динамическая маршрутизация может быть осуществлена с использованием одного и более протоколов. Эти протоколы часто группируются согласно того, где они используются. Протоколы для работы внутри автономных систем называют внутренними протоколами шлюзов (interior gateway protocols (IGP)), а протоколы для работы между автономными системами называют внешними протоколами шлюзов (exterior gateway protocols (EGP)). К протоколам IGP относятся RIP, RIP v2, IGRP, EIGRP, OSPF и IS-IS. Протоколы EGP3 и BGP4 относятся к EGP. Все эти протоколы могут быть разделены на два класса: дистанционно-векторные протоколы и протоколы состояния связи.

Маршрутизаторы используют метрики для оценки или измерения маршрутов. Когда от маршрутизатора к сети назначения существует много маршрутов, и все они используют один протокол маршрутизации, то маршрут с наименьшей метрикой рассматривается как лучший. Если используются разные протоколы маршрутизации, то для выбора маршрута используется административные расстояния, которые назначаются маршрутам операционной системой маршрутизатора.

RIP использует в качестве метрики количество переходов (хопов). EIGRP использует сложную комбинацию факторов, включающую полосу пропускания канала и его надёжность.

Результаты работы маршрутизирующих протоколов заносятся в таблицу маршрутов, которая постоянно изменяется при смене ситуации в сети. Рассмотрим типичную строку в таблице маршрутов, относящуюся к динамической маршрутизации

R 192.168.14.0/24 [120/3] via 10.3.0.1 00:00:06 Serial0

Здесь R определяет протокол маршрутизации. Так R означает RIP, а O – OSPF и т.д. Запись [120/3] означает, этот маршрут имеет административное расстояние 120 и метрику 3. Эти числа маршрутизатор использует для выбора маршрута. Элемент 00:00:06 определяет время, когда обновилась данная строка. Serial0 это локальный интерфейс,

через который маршрутизатор будет направлять пакеты к сети 192.168.14.0/24 через адрес 10.3.0.1.

Для того чтобы динамические протоколы маршрутизации обменивались информацией о статических маршрутах, следует осуществлять дополнительное конфигурирование.

Дистанционно-векторная маршрутизация

Эта маршрутизация базируется на алгоритме Белмана-Форда. Через определённые моменты времени маршрутизатор передаёт соседним маршрутизаторам всю свою таблицу маршрутизации. Такие простые протоколы как RIP и IGRP просто распространяют информацию о таблицах маршрутов через все интерфейсы маршрутизатора в широковещательном режиме без уточнения точного адреса конкретного соседнего маршрутизатора.

Соседний маршрутизатор, получая широковещание, сравнивает информацию со своей текущей таблицей маршрутов. В неё добавляются маршруты к новым сетям или маршруты к известным сетям с лучшей метрикой. Происходит удаление несуществующих маршрутов. Маршрутизатор добавляет свои собственные значения к метрикам полученных маршрутов. Новая таблица маршрутизации снова распространяется по соседним маршрутизаторам (см. рис.1).

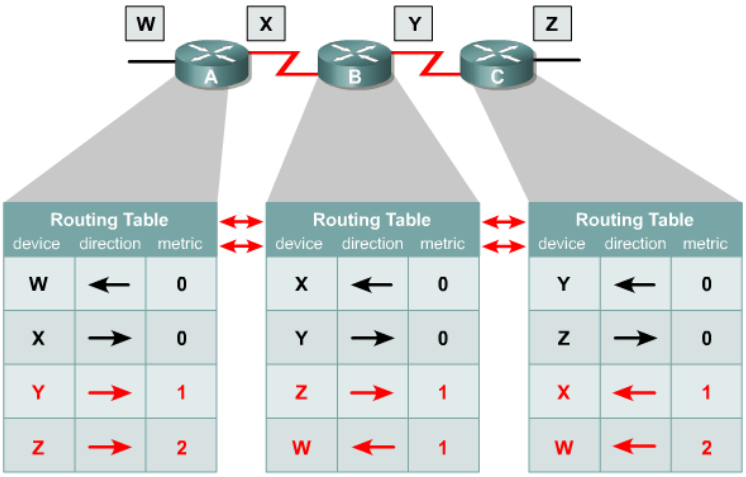


Рис.1. Дистанционно-векторная маршрутизация.

Протоколы состояния связи

Эти протоколы предлагают лучшую масштабируемость и сходимость по сравнению с дистанционно-векторными протоколами. Протокол базируется на алгоритме Дейкстры, который часто называют алгоритмом «кратчайший путь – первым» (shortest path first (SPF)). Наиболее типичным представителем является протокол OSPF (Open Shortest Path First).

Маршрутизатор берёт в рассмотрение состояние связи интерфейсов других маршрутизаторов в сети. Маршрутизатор строит полную базу данных всех состояний связи в своей области, то есть имеет достаточно информации для создания своего отображения сети. Каждый маршрутизатор затем самостоятельно выполняет SPF-алгоритм на своём собственном отображении сети или базе данных состояний связи для определения лучшего пути, который заносится в таблицу маршрутов. Эти пути к другим сетям формируют дерево с вершиной в виде локального маршрутизатора.

Маршрутизаторы извещают о состоянии своих связей всем маршрутизаторам в области. Такое извещение называют LSA (link-state advertisements).

В отличие от дистанционно-векторных маршрутизаторов, маршрутизаторы состояния связи могут формировать специальные отношения со своими соседями.

Имеет место начальный наплыв LSA пакетов для построения базы данных состояний связи. Далее обновление маршрутов производится только при смене состояний связи или,

если состояние не изменилось в течение определённого интервала времени. Если состояние связи изменилось, то частичное обновление пересылается немедленно. Оно содержит только состояния связей, которые изменились, а не всю таблицу маршрутов.

Администратор, заботящийся об использовании линий связи, находит эти частичные и редкие обновления эффективной альтернативой дистанционно-векторной маршрутизации, которая передаёт всю таблицу маршрутов через регулярные промежутки времени.

Протоколы состояния связи имеют более быструю сходимость и лучшее использование полосы пропускания по сравнению с дистанционно-векторными протоколами. Они превосходят дистанционно-векторные протоколы для сетей любых размеров, однако имеют два главных недостатка: повышенные требования к вычислительной мощности маршрутизаторов и сложное администрирование.

Сходимость.

Этот процесс одновременно и совместный, и индивидуальный. Маршрутизаторы разделяют между собой информацию, но самостоятельно пересчитывают свои таблицы маршрутизации. Для того чтобы индивидуальные таблицы маршрутизации были точными, все маршрутизаторы должны иметь одинаковое представление о топологии сети. Если маршрутизаторы договорились о топологии сети, то имеет место их сходимость. Быстрая сходимость означает быстрое восстановление после обрыва связей и других изменений в сети. О протоколах маршрутизации и о качестве проектирования сети судят главным образом по сходимости.

Когда маршрутизаторы находятся в процессе сходимости, сеть восприимчива к проблемам маршрутизации. Если некоторые маршрутизаторы определили, что некоторая связь отсутствует, то другие ошибочно считают эту связь присутствующей. Если это случится, то отдельная таблица маршрутов будет противоречива, что может привести к отбрасыванию пакетов и петлям маршрутизации.

Невозможно, чтобы все маршрутизаторы в сети одновременно обнаружили изменения в топологии. В зависимости от использованного протокола, может пройти много времени пока все процессы маршрутизации в сети сойдутся. На это влияют следующие факторы:

Расстояние в хопах до точки изменения топологии.

Число маршрутизаторов, использующих динамические протоколы.

Полоса пропускания и загрузка каналов связи.

Загрузка маршрутизаторов .

Эффект некоторых факторов может быть уменьшен при тщательном проектировании сети.

Конфигурирование динамической маршрутизации

Для конфигурирования динамической маршрутизации используются две основные команды: router i network. Команда router запускает процесс маршрутизации и имеет форму:

Router(config)# **router protocol [keyword]**

где Protocol - любой из протоколов маршрутизации: RIP, IGRP, OSPF и т.п., keyword – дополнительные параметры.

Затем необходимы команды network:

Router (config-router)# **network network-number [keyword]**

где network-number - идентифицирует непосредственно подключенную сеть, добавляемую в процесс маршрутизации, keyword –дополнительные параметры. network-number позволяет процессу маршрутизации определить интерфейсы, которые будут брать участие в отсылке и приёме пакетов актуализации маршрутной информации.

Для просмотра информации о протоколах маршрутизации используется команда show ip protocol., которая выводит значения таймеров процессов маршрутизации и сетевую информацию, имеющую отношение к маршрутизации. Эта информация может

использоваться для идентификации маршрутизатора, подозреваемого в поставке плохой маршрутной информации

Содержимое таблицы IP маршрутизации выводится командой show ip route. Она содержит записи про все известные маршрутизатору сети и подсети и указывает на способ получения этой информации.

Протокол RIP

Ключевые характеристики протокола RIP:

маршрутизация на основании вектора расстояния;

метрика при выборе пути в виде количества переходов (хопов);

максимально допустимое количества хопов- 15;

по умолчанию пакеты актуализации маршрутной информации посылаются в режиме широковещания каждые 30 секунд.

Выбор протокола RIP як протокола маршрутизации осуществляется командой:

Router(config)# **router rip**

Команда network назначает IP адрес сети с которой маршрутизатор имеет непосредственное соединение.

Router(config-router)# **network network-number**

Процесс маршрутизации связывает интерфейсы с соответствующими адресами и начинает обработку пакетов в заданных сетях.

В показанном на рис.2 примере команды network 1.0.0.0 и network 2.0.0.0 задают непосредственно подключенные к маршрутизатора Cisco A сети.

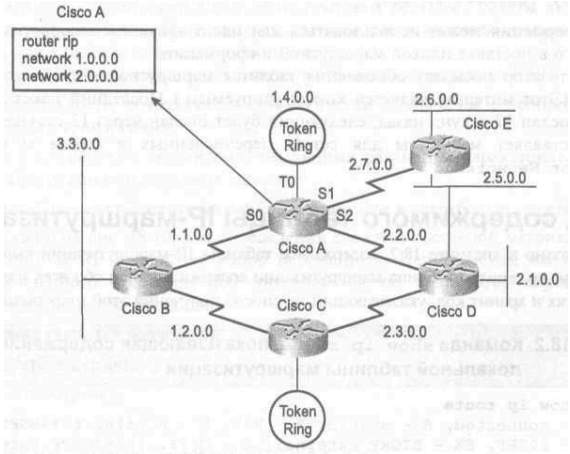


Рис.2.

Команда debug ip rip выводит содержание пакетов актуализации маршрутной информации протокола RIP в том виде, в котором эти данные посылаются и принимаются.

Протокол IGRP

IGRP представляет собою протокол маршрутизации по вектору расстояния разработанный компанией Cisco. Этот протокол посылает пакеты актуализации маршрутной информации с 90-секундным интервалом, в которых содержатся сведения о сетях для конкретной автономной системы. Этот протокол характеризует универсальность, позволяющую автоматически справляться со сложными топологиями, и гибкость в работе с сегментами, имеющими разные характеристики по полосе пропускания и величины задержки. Используемая им метрика не имеет свойственных протоколу RIP ограничений по количеству переходов. Она включает следующие составляющие: Ширина полосы пропускания; Величина задержки; Уровень загрузки; Надёжность канала; Размер максимального блока передачи в канале.

Выбор протоколу IGRP в качестве протокола маршрутизации осуществляется с помощью команды:

Router (config)# **router igrp autonomous-system**

где параметр Autonomous-system называют номером автономной системы и он идентифицирует вычислительный процесс IGRP- маршрутизации. Процессы в маршрутизаторах сети с одинаковым номером autonomous-system будут коллективно использовать маршрутную информацию.

Команда network задаёт непосредственно присоединённые сети, которые подлежат включению в данный процесс маршрутизации:

Router(config-router)#**network network-number**

В показанном примере на рис.3 на маршрутизаторе Cisco A запущен маршрутизирующий процесс, организующий IGRP маршрутизацию в автономной системе с номером 109. В маршрутизции будут участвовать сети 1.0.0.0 и 2.0.0.0.

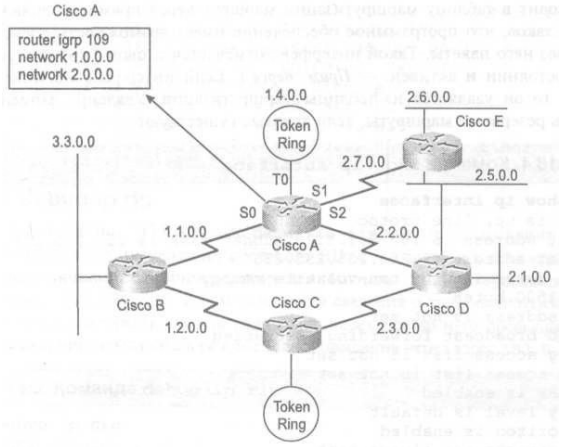


Рис.3.

Команда debug ip igrp transactions и debug ip igrp events выводят содержание пакетов актуализации маршрутной информации протокола IGRP в том виде, в котором эти данные посылаются и принимаются

Протокол OSPF

OSPF это динамический, иерархический протокол состояния связи, используемый для маршрутизации внутри автономных систем. Он базируется на открытых стандартах и был спроектирован как замена протоколу RIP. Он является развитием ранних версий протокола маршрутизации IS-IS. OSPF - устойчивый протокол, поддерживающий маршрутизацию с наименьшим весом и балансировку загрузки. Кратчайший путь в сети вычисляется по алгоритму Дейкстры. Cisco поддерживает свою версию стандарта OSPF.

Как только маршрутизатор настроен на работу с OSPF, он начинает процесс изучения окружения, проходя несколько фаз инициализации. В начале маршрутизатор использует Hello для определения своих соседей и создания отношений для обмена обновлением маршрутной информацией с ними. Затем маршрутизатор начинает фазу ExStart начального обмена между базами маршрутов. Следующей является фаза обмена, в которой назначеный маршрутизатор отсылает маршрутную информацию и получает подтверждения от нашего нового маршрутизатора. В течение стадии загрузки, новый маршрутизатор компилирует таблицу маршрутов. По окончании вычислений маршрутизатор переходит в полное состояние, в котором он является активным членом сети.

Для запуска OSPF маршрутизации служит команда

Router(config)#**router ospf N,**

где N-номер вычислительного процесса OSPF. В отличие от IGRP он может быть различным для разных маршрутизаторов автономной системы. OSPF область Area организуется командой

Router(config-router)# **network network-number area Area**

и определяет автономную систему.

В OSPF network-number имеет особый формат. Для подключаемой в процесс маршрутизации сети используетя инверсная маска. Так, чтобы сеть 212.34.0.0 255.255.0.0 поместить в область 7 OSPF маршрутизации следует дать команду

Router(config-router)# **network 212.34.0.0 0.0.255.255 area 7**

Команда show ip ospf interface для каждого интерфейса выводит всю OSPF информацию: IP адрес, область, номер процесса, идентификатор маршрутизатора, стоимость, приоритет, тип сети, интервалы таймера.

Команда show ip ospf neighbor показывает важную информацию, касающуюся состояния соседей.

Практическая часть

1. Загрузите в симулятор топологию и конфигурацию, использованную практической части лабораторной работы №2.
2. Если сделано всё правильно вы сможете пропинговать из любого маршрутизаторы адреса непосредственно соединённых интерфейсов других маршрутизаторов. На каждом устройстве, используя команды CDP show cdp neighbors detail, получите IP адреса соседних устройств и пропингуйте их.
3. В лабораторной работе №2 мы не смогли пинговать дальние интерфейсы. Из Router2 была недоступна сеть 172.16.10.0/24, а из Router4 была недоступна сеть 10.1.1.0/24. В лабораторной работе №3 с помощью статической маршрутизации мы решили проблему. В этой работе для решения проблемы используем разные формы динамической маршрутизации.

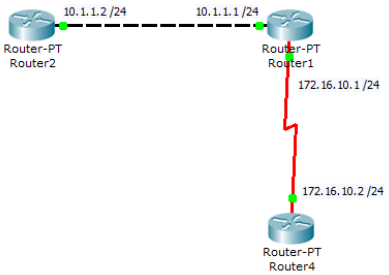


Рисунок 4.

Посмотрим таблицы маршрутов

Router2# **sh ip route**

Нет маршрута на сеть 172.16.10.0/24.

Поэтому в эту сеть из Router2 не идут пинги.

Router4# **sh ip route**

Нет маршрута на сеть 10.1.1.0/24.

Поэтому в эту сеть из Router4 не идут пинги.

RIP

1. Включим RIP на всех маршрутизаторах

Router1(config)# **router rip**

Router1(config-router)# **network 172.16.10.0**

Router1(config-router)# **network 10.1.1.0**

Router2(config)# **router rip**

Router2 (config-router)# **network 10.1.1.0**

Router4(config)# **router rip**

Router4 (config-router)# **network 172.16.10.0**

2. На каждом роутере командой show running-config посмотрим как маршрутизаторы поняли наши команды. Видим, что сеть 10.1.1.0/24 воспринята как сеть 10.0.0.0/8, а сеть 172.16.10.0/24 воспринята как сеть 172.16.0.0/16. Это связано с классами IP адресов.

3. Командой show ip protocols посмотрим с какими параметрами работает протокол RIP. Например, для Router1 имеем

```
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 6 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial2/0             1     2 1
  FastEthernet0/0       1     2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
        10.0.0.0
        172.16.0.0
Passive Interface(s):
Routing Information Sources:
        Gateway         Distance      Last Update
Distance: (default is 120)
```

Переведите сообщение.

4. Посмотрим таблицы маршрутов

Router2# **sh ip route**

```
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
R    172.16.0.0/16 [120/1] via 10.1.1.1, 00:00:15, FastEthernet0/0
```

Есть маршрут на сеть 172.16.10.0/24 через интерфейс Ethernet на адрес 10.1.1.1.

Пинги в эту сеть из Router2 пойдут. Проверьте

Router2#ping 172.16.10.1

Router2# ping 172.16.10.2

5. Перейдём на другой маршрутизатор

Router4# **sh ip route**

```
R    10.0.0.0/8 [120/1] via 172.16.10.1, 00:00:22, Serial2/0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.10.0 is directly connected, Serial2/0
```

Есть маршрут на сеть 10.1.1.0/24 через интерфейс Serial на адрес 172.16.10.1.

Пинги в эту сеть из Router4 пойдут. Проверьте

Router4#ping 10.1.1.1

Router4# ping 10.1.1.2.

4. Командой debug ip rip посмотрим как маршрутизаторы обмениваются маршрутной информацией. Например, для Router1 имеем повторяющиеся каждые 30 секунд сообщения

5.

Router1# **debug ip rip**

```
RIP: sending update to 255.255.255.255 via Serial0 (172.16.10.1)
 subnet 10.1.1.0, metric 1

RIP: sending update to 255.255.255.255 via Ethernet0 (10.1.1.1)
 subnet 172.16.10.0, metric 1

RIP: received update from 172.16.10.2 on Serial0

RIP: received update from 10.1.1.2 on Ethernet0
```

Выключим трассировку

Router1# **no debug ip rip**
Сохраните конфигурацию.

EIGRP

Остановим на всех маршрутизаторах RIP командой
Router(config)#no router rip.

1. Включим EIGRP на всех маршрутизаторах, образуя автономную систему с номером 100

Router1(config)# **router eigrp 100**
Router1(config-router)# **network 172.16.10.0**
Router1(config-router)# **network 10.1.1.0**

Router2(config)# **router eigrp 100**
Router2 (config-router)# **network 10.1.1.0**

Router4(config)# **router eigrp 100**
Router4 (config-router)# **network 172.16.10.0**

2. На каждом маршрутизаторе командой show running-config посмотрим как маршрутизаторы поняли наши команды. Видим, что сеть 10.1.1.0/24 воспринята как сеть 10.0.0.0/8, а сеть 172.16.10.0/24 воспринята как сеть 172.16.0.0/16. Это связано с классами IP адресов.

3. Командой show ip protocols посмотрим с какими параметрами работает протокол EIGRP. Например, для Router1 имеем

```
Routing Protocol is "eigrp  100 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 100
  Automatic network summarization is in effect
  Automatic address summarization:
    172.16.0.0/16 for FastEthernet0/0
      Summarizing with metric 20512000
    10.0.0.0/8 for Serial2/0
      Summarizing with metric 28160
  Maximum path: 4
  Routing for Networks:
     172.16.0.0
     10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.10.2     90            8321604
    10.1.1.2        90            8350639
  Distance: internal 90 external 170
```

Переведите сообщение.

4. Посмотрим таблицы маршрутов

Router2# **sh ip route**

```
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
D    172.16.0.0/16 [90/20514560] via 10.1.1.1, 00:08:37, FastEthernet0/0
```

Есть маршрут на сеть 172.16.10.0/24 через интерфейс Ethernet на адрес 10.1.1.1.

Пинги в эту сеть из Router2 пойдут. Проверьте

Router2#ping 172.16.10.1

Router2# ping 172.16.10.2

5. Перейдём на другой маршрутизатор

Router4# **sh ip route**

```
D    10.0.0.0/8 [90/20514560] via 172.16.10.1, 00:12:30, Serial2/0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.10.0 is directly connected, Serial2/0
```

Есть маршрут на сеть 10.1.1.0/24 через интерфейс Serial на адрес 172.16.10.1.

Пинги в эту сеть из Router4 пойдут. Проверьте

Router4#ping 10.1.1.1

Router4# ping 10.1.1.2.

6. Командами debug ip eigrp transactions и debug ip eigrp events посмотрите как маршрутизаторы обмениваются маршрутной информацией.

Сохраните конфигурацию.

OSPF

Остановим на всех маршрутизаторах EIGRP командой

Router(config)#**no router eigrp 100**

1. Включим OSPF на всех маршрутизаторах. Дадим процессу OSPF номер 100. Образуем OSPF область 0

Router1(config)#**router ospf 100**
Router1(config-router)# **network 172.16.10.0 0.0.0.255 area 0**
Router1(config-router)# **network 10.1.1.0 0.0.0.255 area 0**

Router2(config)#**router ospf 100**
Router2(config-router)# **network 10.1.1.0 0.0.0.255 area 0**

Router4(config)# **router ospf 100**
Router4(config-router)# **network 172.16.10.0 0.0.0.255 area 0**

2. Команда show running-config показывает, что маршрутизаторы поняли наши команды в том же виде, как мы их и задавали.

3. Командой show ip protocols посмотрим с какими параметрами работает протокол OSPF. Например, для Router1 имеем

```
Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.16.10.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.10.0 0.0.0.255 area 0
    10.1.1.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.1.2             110      00:01:40
    172.16.10.2          110      00:01:45
  Distance: (default is 110)
```

Переведите сообщение.

4. Посмотрим таблицы маршрутов

Router2# **sh ip route**

```
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
     172.16.0.0/24 is subnetted, 1 subnets
O       172.16.10.0 [110/782] via 10.1.1.1, 00:08:26, FastEthernet0/0
```

Есть маршрут на сеть 172.16.10.0/24 через интерфейс Ethernet на адрес 10.1.1.1.

Пинги в эту сеть из Router2 пойдут. Проверьте

Router2# ping 172.16.10.1

Router2# ping 172.16.10.2

5. Перейдём на другой маршрутизатор

Router4# **sh ip route**

```
     10.0.0.0/24 is subnetted, 1 subnets
O       10.1.1.0 [110/782] via 172.16.10.1, 00:03:26, Serial2/0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.10.0 is directly connected, Serial2/0
```

Есть маршрут на сеть 10.1.1.0/24 через интерфейс Serial на адрес 172.16.10.1.

Пинги в эту сеть из Router4 пойдут. Проверьте

Router4# ping 10.1.1.1

Router4# ping 10.1.1.2.

7. Команды show ip ospf interface, show ip ospf database и debug ip igrp neighbor покажут вам всю информацию о параметрах протокола OSPF.

Сохраните конфигурацию.

Контрольные вопросы

1. Что такое автономная система.
2. Что такое метрика?
3. Какие существуют два класса протоколов динамической маршрутизации.
4. Объясните работу дистанционно-векторных протоколов.
5. Объясните работу протоколов состояния связи.
6. Как узнать, какие протоколы маршрутизации запущены на маршрутизаторе?
7. В чём преимущества и недостатки дистанционно-векторных протоколов и протоколов состояния связи?
8. Что такое сходимость протоколов маршрутизации?
9. Какие параметры влияют на скорость сходимости?
10. Как на маршрутизаторе запустить и настроить протокол маршрутизации RIP?
11. Как на маршрутизаторе запустить и настроить протокол маршрутизации EIGRP?
12. Как на маршрутизаторе запустить и настроить протокол маршрутизации OSPF?
13. Как посмотреть содержание пакетов актуализации маршрутной информации протокола RIP?
14. Как посмотреть содержание пакетов актуализации маршрутной информации протокола EIGRP?
15. Уточните, что в EIGRP понимается под автономной системой?
16. В чём различие в формате команды router для EIGRP и OSPF?
17. В чём различие в формате команд network для RIP, EIGRP и OSPF?

Порядок выполнения и сдачи работы

1. Изучить теоретическую и практическую часть.
2. Сдать преподавателю теорию работы путём ответа на контрольные вопросы.
3. Выполнить в Packet Tracer практическую часть.
4. Используя вариант из предыдущей лабораторной работы, выполните в Boson задание для самостоятельной работы.

5. Предъявите преподавателю результат выполнения пунктов 7, 10, 14 и 18 задания для самостоятельной работы.
6. Оформите отчёт. Содержание отчёта смотри ниже.
7. Защитите отчёт.

Задание для самостоятельной работы

1. Используйте топологию своего варианта из предыдущей лабораторной работы, представленную на рисунке 5.

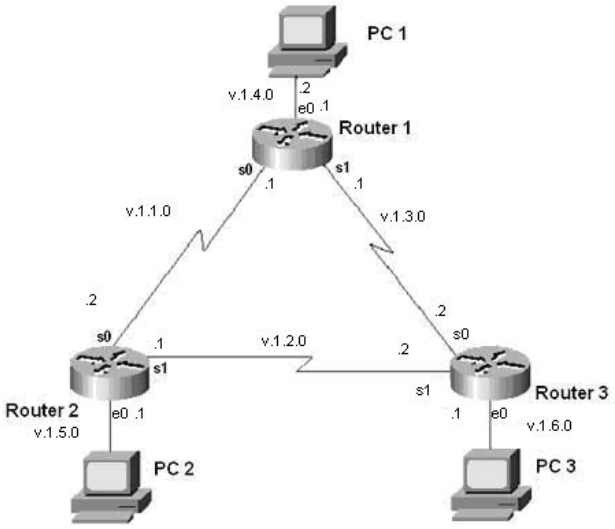


Рисунок 5.

В нашей сети шесть подсетей. Вы видите, что каждый маршрутизатор подключён к трём подсетям.

2. Отредактируйте вручную сохранённую конфигурацию предыдущей успешно выполненной лабораторной работы: уберите в rtr файлах маршрутизаторов команды статической маршрутизации.

3. Загрузите отредактированную конфигурацию в симулятор.

4. На каждом маршрутизаторе проверьте правильность загрузки конфигурации командами show cdp neighbors и show ip interface brief.

Если последовательный интерфейс не поднялся, проверьте командой **show running-config**, что на интерфейсе DCE стороны последовательной связи задана команда **clock rate!** Если не задана, то задайте её.

5. Настройте на каждом маршрутизаторе динамическую маршрутизацию по протоколу RIP.

6. На каждом маршрутизаторе посмотреть таблицу маршрутизации командой show ip route. Сделать скриншоты. Например, для маршрутизатора router1 для варианта 1 (v=1) имеем

```
C       1.1.4.0/24 is directly connected, Ethernet0
C       1.1.1.0/24 is directly connected, Serial0
C       1.1.3.0/24 is directly connected, Serial1
R       1.1.6.0/24 [120/1] via 1.1.3.2, 00:01:43, Serial1
R       1.1.5.0/24 [120/1] via 1.1.1.2, 00:06:30, Serial0
R       1.1.2.0/24 [120/1] via 1.1.1.2, 00:03:35, Serial0
```

7. На каждом компьютере выполните команды трассировки tracert других компьютеров. Сделайте скриншоты. Всего шесть скриншотов. Например, трассировка из PC1 на PC2 для варианта 1 (v=1) имеет вид

```
PC1:#tracert 1.1.5.2


"Type escape sequence to abort."
Tracing the route to 1.1.5.2

 1 1.1.4.1 0 msec 16 msec 0 msec
 2 1.1.1.2 20 msec 16 msec 16 msec
 3 1.1.5.2 20 msec 16 msec *
```

Видим, что путь для пакетов из PC1 на PC2 (1.1.5.2) лежит последовательно через Router1 (Ethernet 1.1.4.1) и затем через Router2 (serial0 1.1.1.2)

8. Отключим на маршрутизаторе router1 последовательный интерфейс serial 0

Router1(config)#**interface serial 0**

Router1(config-if)#**shutdown**

9. Через пару минут, когда в сети пройдут обновления маршрутной информации, на каждом маршрутизаторе посмотреть таблицу маршрутизации командой show ip route. Сделать скриншоты. Например, для маршрутизатора router1 для варианта 1 (v=1) имеем

```
C       1.1.4.0/24 is directly connected, Ethernet0
C       1.1.3.0/24 is directly connected, Serial1
R       1.1.2.0/24 [120/1] via 1.1.3.2, 00:07:26, Serial1
R       1.1.6.0/24 [120/1] via 1.1.3.2, 00:08:41, Serial1
R       1.1.5.0/24 [120/2] via 1.1.3.2, 00:07:44, Serial1
```

Видим, что таблица изменилась: пропала сеть 1.1.1.0/24 и все пакеты теперь маршрутизируются на адрес 1.1.3.2 через интерфейс Serial1.

10. На каждом компьютере выполните команды трассировки tracert других компьютеров. Сделайте скриншоты. Всего шесть скриншотов. Например, трассировка из PC1 на PC2 для варианта 1 (v=1) имеет вид

```
PC1:#tracert 1.1.5.2


"Type escape sequence to abort."
Tracing the route to 1.1.5.2

 1 1.1.4.1 0 msec 16 msec 0 msec
 2 1.1.3.2 20 msec 16 msec 16 msec
 3 1.1.2.1 20 msec 16 msec 16 msec
 4 1.1.5.2 20 msec 16 msec *
```

Видим, что теперь путь для пакетов из PC1 на PC2 (1.1.5.2) лежит последовательно через Router1 (Ethernet 1.1.4.1) , затем через Router3 (serial0 1.1.3.2) и затем через Router2 (serial1 1.1.2.1).

11. Сохраните конфигурацию.

12. Отключите RIP и настройте на каждом маршрутизаторе динамическую маршрутизацию по протоколу IGRP.

13. На каждом маршрутизаторе посмотреть таблицу маршрутизации командой show ip route. Сделать скриншоты. Например, для маршрутизатора router1 для варианта 1 (v=1) имеем

```
C       1.1.4.0/24 is directly connected, Ethernet0
C       1.1.1.0/24 is directly connected, Serial0
C       1.1.3.0/24 is directly connected, Serial1
I       1.1.6.0/24 [100/651] via 1.1.3.2, 00:02:38, Serial1
I       1.1.5.0/24 [100/651] via 1.1.1.2, 00:04:26, Serial0
I       1.1.2.0/24 [100/651] via 1.1.1.2, 00:08:28, Serial0
```

14. Проверьте, что вы всё сделали правильно. На каждом компьютере выполните команд трассировки tracert других компьютеров.

15. Сохраните конфигурацию.

16. Отключите IGRP и настройте на каждом маршрутизаторе динамическую маршрутизацию по протоколу OSPF.

17. На каждом маршрутизаторе посмотреть таблицу маршрутизации командой show ip route. Сделать скриншоты. Например, для маршрутизатора router1 для варианта 1 (v=1) имеем

```
C       1.1.4.0/24 is directly connected, Ethernet0
C       1.1.1.0/24 is directly connected, Serial0
C       1.1.3.0/24 is directly connected, Serial1
O       1.1.5.0/24 [110/65] via 1.1.1.2, 00:00:39, Serial0
O       1.1.2.0/24 [110/65] via 1.1.3.2, 00:00:22, Serial1
O       1.1.6.0/24 [110/65] via 1.1.3.2, 00:00:26, Serial1
```

18. Проверьте, что вы всё сделали правильно. На каждом компьютере выполнените команд трассировки tracert других компьютеров.

19. Сохраните конфигурацию.

Лабораторнвя работа
Темы: Организация доступа к сетям Wi-Fi

В современном мире все большее применение находят беспроводные сети Wi-Fi, позволяющие давать клиентам доступ к ресурсам сетей, например к **Internet**, с ноутбука или персонального компьютера, используя в качестве среды передачи данных радиоканал, что не требует наличия специальных проводных соединений клиентов с сетью, обеспечивая таким образом их мобильность.

Преимущества Wi-Fi

- Отсутствие проводов.

Передача данных в сети осуществляется по радиоканалу . Возможна установка в местах, где прокладка проводной сети по тем или иным причинам невозможна или нецелесообразна, например на выставках, залах для совещаний.

- Мобильность, как рабочих мест, так и самого офиса.

Так как беспроводная сеть не привязана к проводам, Вы можете свободно изменять местоположение Ваших компьютеров в зоне покрытия точки доступа, не беспокоясь о нарушениях связи. Сеть легко монтируется/демонтируются, при переезде в другое помещение Вы можете даже забрать свою сеть с собой.

Недостатки Wi-Fi

- Относительно высокая стоимость оборудования

- Небольшая дальность действия – 50-100 метров

- **Велика опасность несанкционированного подключения к сети сторонних пользователей**

В предлагаемой лабораторной работе ***мы освоим*** создание простейшей сети Wi-Fi на примере подключения ноутбука к точке доступа Wi-Fi с использованием статической и динамической IP-адресации с последующим доступом к WEB серверу сети СГУПСа через шлюз.

Схема взаимодействия двух сетей имеет следующий вид:

Монтаж Wi-Fi сети.

1. Возьмите у преподавателя Wi-Fi-адаптер. Подключите адаптер к USB-порту **ноутбука**. (См. схему сети).
2. Включите ноутбук. Пароль **12345**. После загрузки операционной системы на ноутбуке, на адаптере должны загореться сигнальные лампочки, свидетельствующая об установке радиообмена между адаптером и точкой доступа.
3. Сеть Wi-Fi собрана, теперь ее необходимо настроить.

1-я часть работы. Настройка сети со статическим адресом компьютера клиента.

Настройка сети заключается в установке **протоколов ноутбука клиента**, которые необходимы для его работы, а так же включение и настройка **DHCP-сервера**, который находится в **точке доступа**.

Запомните. **Протокол – это специальная программа, посредством которой компьютеры сети обмениваются между собой данными по специальным правилам.** В нашей сети рабочим протоколом будет протокол **TCP/IP**. Чтобы компьютеры могли обмениваться между собой данными этот протокол должен быть установлен на всех компьютерах, которые находятся в сетях.

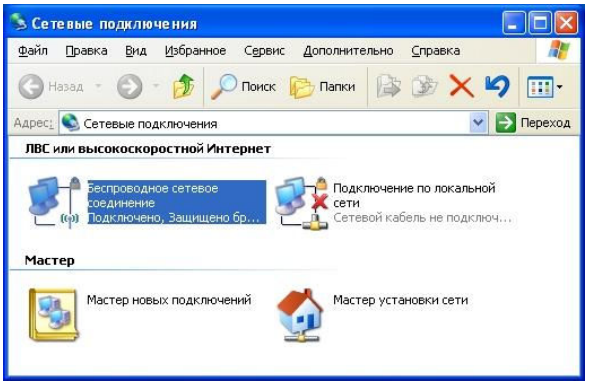
На **WEB сервере** СГУПСа протокол TCP/IP уже установлен, нам осталось установить и настроить этот протокол на **ноутбуке клиенте** (см. схему сети). *Помните*, что все пункты настройки должны выполняться в той последовательности, в которой они указаны. Не нарушайте последовательность настройки.

На ноутбуке **Клиенте** выполните следующие действия:

1. Щелкните правой клавишей мыши на значке «**Мое сетевое окружение**» 

, выберите в меню «**Свойства**». Откроется список сетевых подключений (рис.1.).

Рис.1.



2. Выберите в списке свободное «**Беспроводное сетевое соединение**», щелкните по нему правой клавишей мыши и выберите пункт «**Свойства**». Откроется окно свойств соединения (рис.2.).

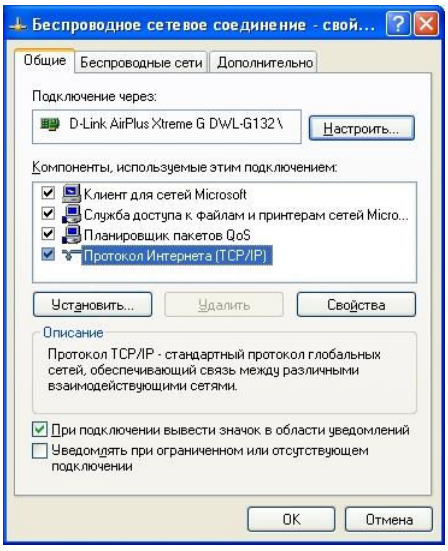


Рис.2.

3. В появившемся окне выберите «**Протокол Интернета (TCP/IP)**», нажмите «**Свойства**». Откроется окно настроек протокола (рис.3.). Активируйте флажок «**Использовать следующий IP-адрес**». Введите в поля **IP-адрес** и **Маска подсети** адреса установок, которые изображены на рис.3.

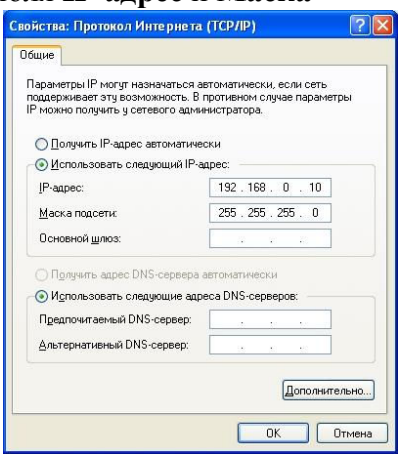


Рис.3.

Здесь **192.168.0.10** – это IP-адрес компьютера в сети.
255.255.255.0 – маска подсети. Это специальный параметр, который вместе с адресом однозначно определяет сеть, в которой находится компьютер.

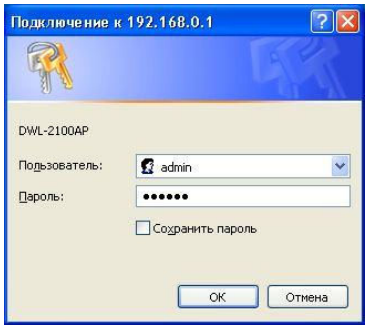
4. После ввода настроек, нажмите «**ОК**», окно «**Свойства: Протокол Интернета (TCP/IP)**» закроется. В окне «**Беспроводное сетевое соединение**» (рис.2.) нажмите «**OK**».

Мы настроили ноутбук клиент для работы с беспроводной сетью. Для ноутбука прописан статический IP-адрес , это означает что мы присвоили ноутбуку выделенный, постоянный IP-адрес, который можно менять и назначать только вручную. Статический IP-адрес нам необходим для того, чтобы подключиться к точке доступа Wi-Fi для ее настройки.

Для того чтобы начала функционировать сеть **Wi-Fi** необходимо настроить точку доступа.

Настройка точки доступа Wi-Fi и DHCP-сервера.

1. Загрузите обозреватель **Internet Explorer**. Введите в его адресной строке адрес: http://192.168.0.50/ Это IP-адрес **точки доступа Wi-Fi**. По этому адресу расположена система ее конфигурации. Вход в систему конфигурации защищен логином и паролем и на экране появится окно для ввода этих данных.

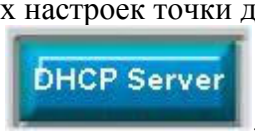


Введите **Пользователь – admin, Пароль – 12345678** и нажмите кнопку «**OK**».

Откроется главная страница систему конфигурации точки доступа Wi-Fi.

2. Щелкните по рисунку 

. Откроется страница расширенных настроек точки доступа.

3. Щелкните по рисунку 

. Откроется страница для изменения настроек **DHCP-сервера**.

Установите следующие параметры **DHCP**, либо измените существующие, если они не совпадают с указанными:

1. Function Enable / Disable – **Enabled**
2. IP Assigned From – **192.168.0.51**
3. The Range Of Pool (1-255) – **200**
4. SubMask – **255.255.255.0**
5. lease Time (60 – 31536000 sec) – **10000000**
6. Status **– ON**

Щелкните по рисунку 

чтобы сохранить сделанные настройки. Точка доступа **Wi-Fi** уйдет на перезагрузку, которая занимает примерно полминуты.

Разберитесь и Запомните. Выполненные выше настройки обеспечивают выполнение следующих функций:

Function Enable / Disable – Включает (Enabled) или отключает (Disabled) DHCP-сервер.

IP Assigned From – задает начальный IP-адрес, с которого начинается диапазон IP-адресов, выделяемых динамически пользователям (пользователи, которые подключаются временно).

The Range of Pool – задает конец **диапазона IP-адресов**, конечное значение последней цифры IP-адреса.

Таким образом в нашем примере мы задали **диапазон IP-адресов** от **192.168.0.51** до **192.168.0.200** включительно.

SubMask – маска подсети. Это специальный параметр, который вместе с адресом однозначно определяет сеть, в которой находится компьютер.

Lease Time – время «жизни» выделенных пользователю сетевых настроек. При динамической адресации настройки пользователя существуют определенное время, после чего сбрасываются и программное обеспечение пользователя запрашивает новые настройки. Здесь задается время существования выделенных пользователю настроек (в секундах).

Status – специальный параметр, он ставится в значение **ON**, если в сети используется совместно **динамическая** и **статическая** адресации. В нашем случае этот параметр установлен в **ON**, поскольку на **ноутбуке клиента** прописан статический, постоянный адрес.

Запомните. Статическая IP-адресация имеет следующие недостатки:

1. Для того, чтобы узнать все настройки сети, необходимо обратиться к администратору сети, который должен индивидуально выделить для каждого клиента свой уникальный IP-адрес. Это неудобно как для клиента, так и для администратора.
2. При подключении к какой-либо другой беспроводной сети, настройки компьютера клиента приходится снова изменять под новую сеть, узнавая их у администратора.
3. Если случайно ваши настройки совпадут с настройками другого клиента, вы не сможете подключиться к сети.

Всех указанных недостатков лишена **динамическая IP-адресация .**

2-я часть работы. Настройка сети с динамическим адресом компьютера клиента.

Динамическая IP-адресация осуществляется с помощью **DHCP-сервера**, который находится в точке доступа. Разберемся что это такое.

Запомните. DHCP-сервер использует **DHCP** протокол **(англ. Dynamic Host Configuration Protocol — протокол динамической конфигурации узла)** — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети **TCP/IP**. Для этого компьютер, подключаемый к сети, обращается к серверу, **DHCP** , который на время проведения сеанса работы с сетью ему выдает **динамический IP-адрес.** Это позволяет избежать ручной настройки компьютеров сети, уменьшает количество ошибок и позволяет клиентам быстро подключаться к сети не тратя время на настройку протоколов связи вручную.

Настройка ноутбука на динамическую IP-адресацию.

1. Вернитесь к началу лабораторной работы, где вы осуществляли настройку сети ноутбука №2. (Раздел «**Настройка сети**»).
2. Повторите шаги 1-3, только на 3-м шаге, где вы вводили статический IP-адрес активируйте флажок «**Получить IP-адрес автоматически**». Это опция и включает динамическую IP-адресацию.
3. Нажмите «**ОК**», окно «**Свойства: Протокол Интернета (TCP/IP)**» закроется. В окне «**Беспроводное сетевое соединение**» (рис.2.) нажмите «**ОК**».

Динамическая IP-адресация на ноутбуке настроена!
Проверка динамической IP-адресации.

1. **Используя процедуру «**Безопасного извлечения устройства**» отключите Wi-Fi адаптер от** ноутбука клиента**. Она выполняется так же, как и при отключении флеш-карт.**
2. **Удалите адаптер из разъема** USB**.**
3. **Подождите несколько секунд и снова вставьте адаптер в разъем** USB**. Произойдет автоматическое подключение** ноутбука клиента **к беспроводной сети** Wi-Fi **и ноутбуку будет присвоен динамический IP-адрес.**

Для того, чтобы убедиться в том, что сетевые настройки были динамически присвоены, сделайте следующее:

1. **Откройте** «Пуск / Стандартные / Командная строка»**. Появится строка для ввода команд операционной системы.**
2. **Введите в строке команду:**

ipconfig **и нажмите** Enter

Эта команда отображает на экран настройки протокола TCP/IP **вашего компьютера и конкретно значение полученного динамического** IP- адреса **от** DHCP-сервера **точки доступа.**

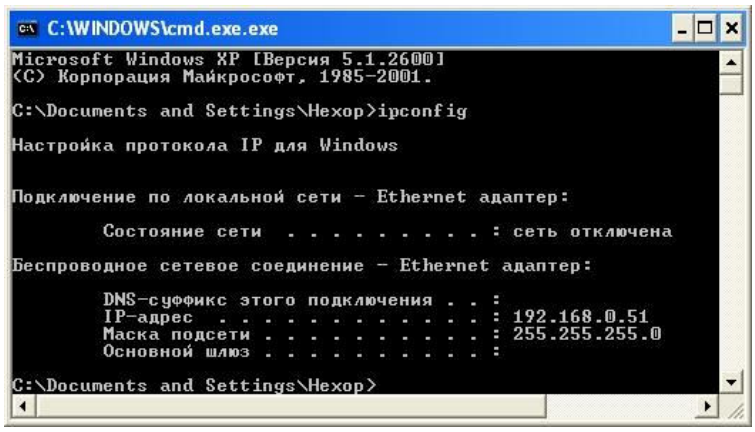


Рис .4.

Если указанный командой IP-адрес компьютера находится в диапазоне 192.168.0.51 – 192.168.0.200, **значит динамическая IP-адресация работает нормально.**

В случае, если указанный командой IP-адрес компьютера НЕ находится **в диапазоне** 192.168.0.51 – 192.168.0.200**), необходимо:**

1. **Произвести настройку сети заново, установив статический IP-адрес, затем, подключившись к точке доступа Wi-Fi проверьте, включен - ли** DHCP**-сервер и правильно - ли выставлены его параметры.**
2. **Если ошибка не исчезла – обратитесь к преподавателю.**

Проверка работы DHCP-сервера беспроводной сети и подключение к Web-серверу СГУПСа.

Для того, чтобы проверить работу **DHCP-сервера** беспроводной сети и подключение к Web-серверу СГУПСа, запустите на **ноутбуке клиенте** обозреватель Интернета **Internet Explorer** и в его адресной строке введите доменный адрес сервера СГУПСа http://www.stu.ru/

Ваш **http** запрос по радиоканалу поступил на точку доступа, оттуда ретранслировался по радиоканалу на рабочую **станцию-шлюз** и затем по проводной сети

университета поступил на **Web-сервер** СГУПСа. В ответ **Web-сервер** СГУПСа послал по этим же каналам **html-страницу** сайта СГУПСа на компьютер Клиент **Wi-Fi сети.**

Если страница сайта СГУПСа загрузится, работа завершена. Предъявите работу преподавателю.

Если страница не загрузилась, значит сеть настроена неправильно. Тогда сделайте следующее:

1. Проверьте еще раз настройки протокола TCP/IP **ноутбука** и убедитесь, что они введены правильно. IP-адрес должен назначаться динамически, включите динамическую адресацию, если это не было сделано.
2. Если ошибка не исчезает, позовите преподавателя.

Отчет по циклу лабораторных работ «Локальные вычислительные сети».

По циклу работ «**Установка и настройка сети на витой паре**» и «**Установка и настройка беспроводной сети Wi-Fi**» составляется один общий отчет. Отчет составляется индивидуально каждым студентом по номеру варианта и защищается преподавателю. Номер варианта прописан на сайте http://uvsr.stu.ru/foto в папке **Методические пособия** в разделе Курс «Интернет технологии» . Группы БС-311, Т-311 (5 семестр).Требования к отчету:

1. Объем отчета 1.5 – 2 страницы. Отчет выполняется в редакторе Microsoft Word. Используйте для оформления схем функции «**Автофигуры**» редактора Microsoft Word.
2. В конце отчета укажите свои ФИО и номер группы.

Лабораторная работа
Тема: «Организация кэширующего proxy-сервера для доступа в Интернет. Настройка параметров»

Цель работы: знакомство с настройкой **кэширующего proxy-сервера**

Теоретические сведения.

1 Функции различных прокси-серверов

В компьютерных сетях под прокси-сервером (компьютерной системой или приложением) понимается сервер, который выступает в роли промежуточного звена для запросов клиентами различных ресурсов с других серверов. Клиент подключается к прокси-серверу, запрашивая какие-либо ресурсы, такие как файл, соединение, веб-страница или другие виды ресурсов, доступных на удаленном сервере. Прокси-сервер обрабатывает запрос согласно правилам фильтрации. Например, он может фильтровать трафик по IP-адресу или протоколу. Если запрос был одобрен фильтром, прокси предоставляет ресурс, предварительно запрашивая его как клиент у соответствующего сервера. Дополнительно, прокси-сервер может изменять запросы клиента или ответы сервера, также он может предоставить запрашиваемый ресурс без подключения к какому-либо серверу вообще. В этом случае, прокси-сервер "кэширует" ответы от удаленных серверов и предоставляет сохраненную информацию в ответ на все последующие запросы.

Два основных назначения прокси-сервера заключаются в следующем:

Сохранить анонимность своих клиентов (в основном для безопасности),

Ускорить доступ к ресурсу (посредством кэширования). Обычно это функция используется для ускорения доступа к веб-страницам.

Прокси-сервер, который передает запросы и ответы в неизменном виде обычно называется шлюзом или, иногда, "туннелирующим прокси".

Прокси-сервер может быть расположен как на локальном компьютере пользователя, так и в других точках между пользователем и серверами в Интернет. Обратный прокси-сервер это прокси, использующийся в качестве front-end сервера для ускорения и кэширования ресурсов, предоставляемых по требованию (таких как веб-страницы).

Далее попробуем раскрыть функции основных типов прокси-серверов.

Обратный прокси - это прокси-сервер, который ставится по соседству с одним или несколькими веб-серверами. Весь трафик, приходящий из Интернета в их направлении проходит через прокси-сервер. Причин для установки обратного прокси-сервера несколько:

- Шифрование, ускорение SSL: часто, при создании защищенных веб-сайтов, SSL-шифрование осуществляется не веб-сервером, а обратным прокси-сервером, снабженным специальным оборудованием для ускорения SSL. Кроме того, один "SSL-прокси" можно использовать для организации шифрования на нескольких веб-серверах, без необходимости получения отдельного сертификата на каждый из них. Недостатком такого способа является необходимость того, чтобы все сервера обладали одним и тем же доменным именем или IP-адресом для SSL подключений.
- Балансировка нагрузки: обратный прокси-сервер может распределять нагрузку между несколькими веб-серверами, при этом веб-сервера могут обслуживать различные области веб-приложения. В таком случае у обратного прокси-сервера может возникнуть потребность в переформировании адресов каждой веб-страницы (преобразование имен ресурсов, доступных снаружи, в имена, доступные во внутренней сети).
- Выдача/кэширование статического содержимого: обратный прокси-сервер может снять нагрузку с веб-серверов за счет кэширования статического содержимого, такого как фотографии или статические графические изображения.
- Сжатие: прокси-сервер может оптимизировать и сжимать передаваемую информацию и, таким образом, увеличивать скорость ее загрузки.
- "Кормление с ложки" уменьшает количество ресурсов, используемых "медленными" клиентами путем кэширования передаваемого веб-сервером содержимого, а затем медленной передачей его клиенту. Весомый выигрыш в экономии ресурсов наблюдается для динамически создаваемых страниц.
- Безопасность: обратный прокси-сервер представляет из себя дополнительный слой безопасности и может защитить некоторые операционные системы, веб-сервера и приложения от специфических атак. Однако, возможности прокси-сервера по защите веб-приложений (а именно веб-приложения подвергаются атакам чаще всего), весьма ограничены.
- Публикация внутренних ресурсов во внешней сети: обратный прокси-сервер, имеющий выход в Интернет, можно использовать для предоставления доступа к закрытым брандмауэрам внутренним серверам компании, без необходимости выведения серверов из под его защиты. При использовании обратного прокси-сервера таким образом следует предпринять дополнительные меры безопасности для того, чтобы защитить внутреннюю инфраструктуру сети, в том случае если сервер будет взломан в результате атаки из Интернет.

Кэширующий прокси-сервер ускоряет обработку запросов путем предоставления данных, сохраненных во время предыдущего запроса от того же самого или других клиентов. Кэширующие прокси сохраняют локальные копии часто запрашиваемых ресурсов, позволяя большим организациям существенно снизить расходы на доступ в Интернет и уменьшить потребление полосы пропускания при значительном увеличении

быстродействия. Большинство провайдеров и крупных организаций имеют собственный кэширующий прокси. Эти сервера настроены так, чтобы обеспечить максимальную производительность файловой системы (обычно используется RAID с журналированием) и используют "разогнанные" версии протокола TCP. Кэширующие прокси были первым типом прокси-серверов.

Некоторые недоработанные прокси-серверы обладают существенными недостатками (например, не поддерживают аутентификацию пользователя). Некоторые проблемы, связанные с прокси-серверами, описаны в RFC 3143 (Известные проблемы HTTP-прокси/Проблемы кэширования).

Другим важным преимуществом использования прокси-сервера является снижение общей стоимости необходимого оборудования и программного обеспечения. Организация может контролировать множество узлов при помощи одного прокси-сервера, запрещающего прямое подключение к Интернет каждому из них. В этом случае, отдельные узлы подключаются к единому прокси-серверу, который, в свою очередь, подключен к основному серверу организации.

Прокси-сервер, который работает с WWW трафиком, называется "*веб прокси-сервером*". Типичное использование веб-прокси - кэширование страниц. Большинство программных прокси-серверов (например, Squid) предоставляют средства для блокировки доступа к определенным адресам, находящимся в черном списке, таким образом предоставляя возможности фильтрации содержимого. Эта возможность часто используется как в корпоративной, образовательной и библиотечной среде, так и в других местах. Некоторые веб-прокси переформатируют страницы с учетом специфических нужд или аудитории (например, для мобильных телефонов или КПК).

Веб-прокси, фильтрующий содержимое. Данный тип прокси-сервера предоставляет административный контроль за передаваемым через него содержимым. Обычно, фильтрующий прокси используется в коммерческих и некоммерческих организациях (особенно часто - в школах) для обеспечения того, что использование Интернет соответствует принятым в организации нормам. Однако, в некоторых случаях, несогласные с данными нормами пользователи могут найти способы обхода ограничений, накладываемых прокси-сервером (особенно это касается программных прокси-серверов).

Наиболее распространенными методами, используемыми для фильтрации содержимого, являются: черные списки URL и DNS, фильтрация по регулярным выражениям, фильтрация по типам MIME и ключевым словам. Некоторые продукты используют специализированные техники для поиска содержимого, обычно предоставляемого определенными типами контент-провайдеров.

Веб-прокси, фильтрующий содержимое, обычно поддерживает аутентификацию пользователей для контроля доступа к веб-ресурсам. Также он ведет файлы журналов для того, чтобы предоставить детальную информацию о ссылках, посещенных пользователями, или для того, чтобы отслеживать статистику использования полосы пропускания. Фильтрующий веб-прокси может взаимодействовать с антивирусной службой, либо с антивирусом, поддерживающим протокол ICAP, для того, чтобы обеспечить защиту от вирусов и других вредоносных программ. Данный вид фильтрации содержимого осуществляется путем сканирования всех входящих данных в реальном времени и их блокировки до того, как они попадут во внутреннюю сеть.

Анонимный прокси-сервер (иногда называемый веб-прокси) применяется для анонимизации веб-серфинга, т.е. для сокрытия информации о серфере. Существует множество различных вариантов анонимизаторов, наиболее типичным из которых является открытый прокси-сервер. Благодаря тому, что их весьма трудно отследить, открытые прокси особенно полезны тем, кому необходима анонимность в онлайне - от политических диссидентов до кибер-преступников. Некоторые пользователи принципиально соблюдают анонимность, например для обеспечения конституционных прав на свободу слова. Сервер в Интернет получает запросы от анонимного прокси-

сервера и таким образом не получает информации об адресе конечного пользователя. Однако, запросы к анонимизирующему прокси-серверу не являются анонимными, поэтому необходима определенная степень доверия прокси-серверу со стороны пользователя. Множество анонимных прокси-серверов финансируются рекламой, демонстрируемой пользователю на протяжении всего сеанса работы.

Некоторые прокси-серверы требуют входа. В больших организациях, пользователи должны войти на прокси-сервер прежде чем получить доступ в Интернет. Исходя из этих данных, организация может установить личность, совершившую тот или иной запрос.

В заголовок запроса некоторые анонимизирующие прокси-серверы включают такие строки как HTTP_VIA, HTTP_X_FORWARDED_FOR или HTTP_FORWARDED, содержащие информацию об IP-адресе клиента. Другие анонимизирующие прокси, также называемые прокси-серверами высокой анонимности, включают в заголовок только одну строку, содержащую IP-адрес прокси-сервера - REMOTE_ADDR. Таким образом серверу в Интернет передается информация о том, что его клиент использует прокси-сервер. Сайт может также заподозрить использование прокси-сервера в том случае, если клиент передает серверу cookie своих предыдущих визитов, во время которых он не использовал прокси-сервер высокой степени анонимности. Очистка cookies и кэша решит эту проблему.

Враждебный прокси-сервер. Прокси-сервер можно установить для того, чтобы перехватить поток данных между клиентами и Интернет. Все полученные веб-страницы или отправленные формы данных могут быть сохранены и проанализированы оператором прокси-сервера. По этой причине, пароли к онлайн-сервисам (к электронной почте или клиент-банку) следует передавать по шифрованному каналу связи, например используя SSL.

Прозрачный прокси (также известный как перехватывающий прокси-сервер) сочетает в себе функции прокси-сервера и шлюза. Соединения, устанавливаемые браузерами клиентов проходят через шлюз, где перенаправляются на прокси-сервер без какой-либо необходимости в настройке клиентских программ (часто, клиентам даже не известно то, что все их запросы проходят через прокси-сервер).

Прозрачные прокси часто используются бизнесом для предотвращения обхода ограничений на использование Интернет, а также для облегчения администрирования сети - снимается необходимость настройки браузеров сотрудников.

Часто можно определить наличие прозрачного прокси-сервера, сравнив внешний IP-адрес, с IP-адресом, определяемым внешними веб-серверами, либо изучив доступные внешнему веб-серверу заголовки HTTP.

Принудительный прокси-сервер. Термин "принудительный прокси" является двусмысленным. С одной стороны он похож на прозрачный прокси-сервер (так как фильтрует весь трафик, проходящий через шлюз, который запрещает доступ к ресурсам Интернет минуя прокси-сервер), а с другой стороны - прямо противоположен ему, так как требует обязательной настройки со стороны пользователя, которому необходимо получить доступ в Интернет.

Принудительный прокси-сервер иногда необходим из-за некоторых проблем с HTTP, возникающих при перехвате TCP-сессий. Например, перехват HTTP запросов может сильно повлиять на эффективность кэша прокси-сервера, а также на некоторые механизмы аутентификации. В основном, эти проблемы возникают как следствие уверенности клиента в том, что он работает с сервером напрямую и вытекающей из этого невозможности отделить заголовки запроса, необходимые прокси-серверу от заголовков, необходимых вышестоящему серверу (особенно это касается авторизационных заголовков). Кроме того, спецификации HTTP, запрещают кэширование ответов, содержащих авторизационные заголовки.

Суффиксный прокси-сервер позволяет получить доступ к веб-страницам приписывая имя прокси-сервера к их адресу (например, "ru.wikipedia.org.statoscope.ru"). Суффиксные прокси-серверы проще в использовании, чем другие виды прокси-серверов.

Открытый прокси-сервер отличается от прочих тем, что доступ к ресурсам Интернет при помощи этого прокси-сервера может получить любой желающий. Часто открытые прокси-сервера появляются в результате неверной конфигурации программного обеспечения системным администратором. Открытый прокси-сервер часто используется с враждебными целями, и именно поэтому системные администраторы разработали ряд способов отказать в обслуживании клиенту, работающему через открытый прокси. Множество IRC-сетей автоматически тестируют клиентскую систему на известные типы открытых прокси-серверов. Схожим образом, почтовый сервер может быть настроен на блокировку сообщений, отправленных через открытые прокси.

IRC группы и операторы электронной почты поддерживают черные списки IP-адресов открытых прокси-серверов (DNSBL). В качестве примеров таких списков можно привести AHBL, CBL, NJABL и SORBS.

Этика автоматического тестирования клиентов на работу через открытые прокси противоречива. Некоторые эксперты полагают, что такое тестирование является аналогом сканирования атакующим портов клиентского компьютера. Другие считают, что клиент одобряет такое сканирование, если подключается к сервису, условия использования которого содержат информацию о наличии такого сканирования.

SOCKS proxy – прокси сервер передающий абсолютно все данные от клиента к серверу, не изменяя и не добавляя ничего. С точки зрения web-сервера SOCKS proxy является клиентом, т.е. SOCKS proxy анонимны по определению. Имеет подтипы SOCKS4, SOCKS4a, SOCKS5. Чаще всего SOCKS proxy имеют 1080, 1081 номер порта.

HTTP-прокси — самый распространенный. Он предназначен для организации работы браузеров и других программ, использующих протокол HTTP. Браузер передает прокси-серверу URL ресурса, прокси-сервер получает его с запрашиваемого веб-сервера (или с другого прокси-сервера) и отдает браузеру. У HTTP-прокси широкие возможности при выполнении запросов:

Можно сохранять полученные файлы на диске сервера. Впоследствии, если запрашиваемый файл уже скачивался, то можно выдать его с диска без обращения в интернет — увеличивается скорость и экономится внешний трафик (который может быть платным). Эта опция называется кэшированием — именно её очень любят администраторы и пользователи — настолько, что считают её главной функцией прокси. Однако приводимые оценки экономии (в описаниях встречалось от 30 до 60%) слишком оптимистичны, не верьте им. На деле получается не более 10-15% — современный интернет очень динамичен, страницы часто меняются, зависят от работающего с ними пользователя и т.д. — такие данные кэшировать нельзя, веб-серверы обычно вставляют в HTTP-заголовки специальные указания об этом, чтобы браузеры и прокси имели это в виду. Хотя многие прокси-серверы можно настроить так, чтобы эти указания частично игнорировались — например, перечитывать страницу не чаще одного раза в день.

Можно ограничивать доступ к ресурсам. Например, завести "черный список" сайтов, на которые прокси не будет пускать пользователей (или определенную часть пользователей, или в определенное время и т.д.). Ограничения можно реализовать по-разному. Можно просто не выдавать ресурс — например, выдавая вместо него страницу "запрещено администратором" или "не найдено". Можно спрашивать пароль и авторизованных пользователей допускать к просмотру. Можно, не спрашивая пароля, принимать решение на основании адреса или имени компьютера пользователя. Условия и действия в принципе могут быть сколь угодно сложными (не во всех прокси, но в нашем точно .

Можно выдавать не тот ресурс, который запрашивается браузером. Например, вместо рекламных баннеров и счетчиков показывать пользователям прозрачные картинки,

не нарушающие дизайн сайта, но существенно экономящие время и трафик за счет исключения загрузки картинок извне.

Можно ограничивать скорость работы для отдельных пользователей, групп или ресурсов. Например, установить правило, чтобы файлы *.mp3 качались на скорости не более 1кб/сек, чтобы предотвратить забивание вашего интернет-канала трафиком меломанов, но не лишать их полностью этого удовольствия. Эта возможность, к сожалению, есть не во всех прокси. В Eproxy эта возможность есть. Она реализуется дополнением TrafC, который кроме ограничения пропускной способности (скорости) может ограничивать и суммарный трафик.

Ведутся журналы работы прокси — можно подсчитывать трафик за заданный период, по заданному пользователю, выяснять популярность тех или иных ресурсов и т.д.

Можно маршрутизировать веб-запросы — например, часть направлять напрямую, часть через другие прокси (прокси провайдера, спутниковые прокси и т.д.). Это тоже помогает эффективнее управлять стоимостью трафика и скоростью работы прокси вцелом.

HTTPS-прокси – фактически часть HTTP-прокси. S в названии означает “secure”, т.е. безопасный. Не смотря на то, что программно это часть HTTP-прокси, обычно HTTPS выделяют в отдельную категорию (и есть отдельное поле для него в настройке браузеров). Обычно этот протокол – безопасный HTTP – применяют, когда требуется передача секретной информации, например, номеров кредитных карт. При использовании обычного HTTP-прокси всю передаваемую информацию можно перехватить средствами самого прокси (т.е. это под силу администратору ЛС) или на более низком уровне, например, tcpdump (т.е. и администратор провайдера и любого промежуточного узла и вообще любой человек, имеющий физический доступ к маршрутам передачи ваших данных по сети, может при большом желании узнать ваши секреты). Поэтому в таких случаях применяют secure HTTP – всё передаваемое при этом шифруется. Прокси-серверу при этом дается только команда «соединится с таким-то сервером», и после соединения прокси передает в обе стороны шифрованный трафик, не имея возможности узнать подробности (соответственно и многие средства управления доступом – такие как фильтрация картинок – не могут быть реализованы для HTTPS, т.к. прокси в этом случае неизвестно, что именно передается). Собственно в процессе шифрации/дешифрации прокси тоже участия не принимает – это делают клиентская программа и целевой сервер. Наличие команды «соединиться с таким-то сервером» в HTTPS-прокси приводит к интересному и полезному побочному эффекту, которым все чаще пользуются разработчики клиентских программ. Так как после соединения с указанным сервером HTTPS-прокси лишь пассивно передает данные в обе стороны, не производя никакой обработки этого потока вплоть до отключения клиента или сервера, это позволяет использовать прокси для передачи почти любого TCP-протокола, а не только HTTP. То есть HTTPS-прокси одновременно является и простым POP3-прокси, SMTP-прокси, IMAP-прокси, NNTP-прокси и т.д. – при условии, что соответствующая клиентская программа умеет так эксплуатировать HTTPS-прокси (увы, далеко не все еще это умеют, но есть вспомогательные программы, «заворачивающие» трафик обычных клиентов через HTTPS-прокси). Никаких модификаций целевого сервера не требуется. Фактически HTTPS-прокси является программируемым mapping-proxy, как и Socks-proxy.

FTP-прокси бывает двух основных видов в зависимости от протокола работы самого прокси. С ftp-серверами этот прокси, конечно, всегда работает по протоколу FTP. А вот с клиентскими программами – браузерами и ftp-клиентами (CuteFTP, FAR, и др.) прокси может работать как по FTP, так и по HTTP. Второй способ удобнее для браузеров, т.к. исторически является для них «родным». Браузер запрашивает ресурс у прокси, указывая протокол целевого сервера в URL – http или ftp. В зависимости от этого прокси выбирает протокол работы с целевым сервером, а протокол работы с браузером не меняется – HTTP. Поэтому, как правило, функцию работы с FTP-серверами также

вставляют в HTTP-прокси, т.е. HTTP-прокси, описанный выше, обычно с одинаковым успехом работает как с HTTP, так и с FTP-серверами. Но при «конвертации» протоколов FTP<->HTTP теряется часть полезных функций протокола FTP. Поэтому специализированные ftp-клиенты предпочитают и специальный прокси, работающий с обеими сторонами по FTP. В различных приложениях это называется этот прокси FTP-gate, чтобы подчеркнуть отличие от FTP-прокси внутри HTTP-прокси. Хотя встречаются и вносящие путаницу названия. Например, в программе CuteFTP FTP-gate называют firewall, хотя FireWall в общем случае – это вообще не прокси, а фактически программа обратного назначения – не для подключения к интернету, а для изоляции от него Для прокси в FireWall оставляют специальные «дыры». FTP-gate поддерживают различные способы указания в FTP-протоколе целевого сервера, с которым FTP-клиент хочет работать, в настройке FTP-клиентов обычно предлагается выбор этого способа.

Здесь USER user@site, OPEN site, и т.д. – способ указания сервера, с которым производится работа. Такое многообразие связано с тем, что нет общепринятого стандарта на этот вид прокси, и применяются такие хитрые добавки к стандартным командам FTP-протокола.

Mapping-прокси — способ заставить работать через прокси те программы, которые умеют работать с интернетом только напрямую. При настройке такого прокси администратор создает как бы "копию" целевого сервера, но доступную через один из портов прокси-сервера для всех клиентов локальной сети — устанавливает локальное "отображение" заданного сервера. Например, пользователи локальной сети хотят работать с почтовым сервером mail.ru не через браузер, а с использованием почтовой программы Outlook Express или TheBat. Эти программы не умеют работать через прокси (кроме случая, когда Outlook получает почту по HTTP с hotmail.com — тогда он, как и браузер, пользуется HTTP-прокси). Простейший способ работать с mail.ru по POP3 через прокси — установить локальное отображение сервера pop.mail.ru. И в Outlook'ах вместо pop.mail.ru написать имя прокси-сервера и порт отображения. Outlook будет соединяться с прокси-сервером ("думая", что это почтовый сервер), а прокси при этом будет соединяться с pop.mail.ru и прозрачно передавать всю информацию между Outlook и pop.mail.ru, таким образом "превращаясь" на время соединения в POP3-сервер. Неудобство mapping-прокси в том, что для каждого необходимого внешнего сервера нужно вручную устанавливать отдельный порт на прокси. Но зато не требуется модификация ни серверов, ни клиентов. Особенно это помогает в случае необходимости "проксирования" многочисленных "доморощенных" протоколов, реализованных в играх или финансовых программах. Почему-то они часто игнорируют существование прокси и стандартных протоколов. Такие программы можно "обмануть" и направить через прокси практически всегда, если они не делают другой глупости — передачи клиентского IP-адреса внутри протокола и пытаются с ним соединяться напрямую еще раз (что невозможно, т.к. локальные адреса недоступны извне).

2 Сравнение «Кэширующего прокси-сервера» с другими прокси-серверами.

2.1. Squid

Squid — программный пакет, реализующий функцию кэширующего прокси-сервера для протоколов HTTP, FTP, Gopher и (в случае соответствующих настроек) HTTPS. Разработан сообществом как программа с открытым исходным кодом (распространяется в соответствии с GNU GPL). Все запросы выполняет как один неблокируемый процесс ввода/вывода.

Используется в UNIX-like системах и в ОС семейства Windows NT. Имеет возможность взаимодействия с Active Directory Windows Server путём аутентификации через LDAP, что позволяет использовать разграничения доступа к интернет ресурсам пользователей, которые имеют учётные записи на Windows Server, также позволяет организовать «нарезку» интернет трафика для различных пользователей. Используется

вместе с движками Mediawiki на wiki хостингах. Использование кэширующего прокси-сервера становится выгодно примерно с 2000 посетителей в сутки.

Squid имеет возможность переписывать запрашиваемые URL. Squid может быть сконфигурирован так, чтобы пропускать входящие URL через процесс редиректора выполняемого как внешний процесс (подобно dnsserver), который возвращает новый URL или пустую строку, обозначающую отсутствие изменений. Редиректор не является стандартной частью пакета Squid. Редиректор предоставляет администратору контроль за передвижениями пользователей. Использование редиректора в сочетании с прозрачным проксированием дает простой, но эффективный контроль, над доступом к нежелательным ресурсам (например к развлекательным ресурсам и социальным сетям в корпоративной сети, порнографии). Программа-редиректор должна читать URL (один на строку) со стандартного входа и записывать измененные URL или пустые строки на стандартный выход. Нужно заметить, что программа-редиректор не может использовать буферизированный ввод/вывод. Squid дописывает дополнительную информацию после URL, которую редиректор может использовать для принятия решения.

Главным достоинством squid является его модульность. Существует множество надстроек, которые существенно повышают степень надежности соединения и безопасности.

- SQUID Account Management System(SAMS) - программное средство для администрирования доступа пользователей к прокси-серверу SQUID, сбора статистики и генерации отчетов о потреблении трафика.
  SAMS - это система для управления доступа пользователей через прокси сервер к ресурсам интернет. Она идеально подходит для использования как в частных фирмах так и в государственных учереждениях. Всю работу по проксированию, перенаправлению запросов, кэшированию и авторизации берет на себя proxy-сервер Squid а SAMS занимается учетом трафика и управлением пользователями.
- NeTAMS позволяет контролировать расходы на использование сети Интернет сотрудниками, получать статистику по трафику, устанавливать ограничения.

И многие другие…

К недостаткам SQUID можно отнести:

- Отсутствие полной функциональности в среде ОС семейства Windows, т.е. многие компоненты невозможно установить.
- Негибкие настройки. В случае внесения изменений в конфигурацию необходимо перезапускать службу (а в отдельных случаях и весь сервер)
- Усложненная настройка правил.

В программе «Кэширующий прокси-сервер» файлы правил достаточно просты для понимания.

2.2. DeleGate

DeleGate - Многоцелевой прокси-сервер, работающий с различными TCP-, UDP-протоколами, такими как HTTP, HTTPS, FTP, NNTP, SMTP, SOCKS, IMAP, ICP и т. д. Delegate работает как прокси уровня приложения (application-level), который пропускает через себя различные протоколы, производя необходимые изменения в данных. Также Delegate может быть использован как прокси для передачи любых данных между клиентом и сервером по протоколам TCP, UDP. Являясь прокси уровня приложения, Delegate обеспечивает виртуальное представление ресурсов, расположенных на различных серверах. В случаях HTTP, FTP, NNTP, Delegate может выступать самостоятельным сервером. Поддерживается фильтрация данных. Для фильтрации используется собственный интерфейс CFI (Common Filtering Interface). В качестве фильтров могут быть использованы как внутренние средства Delegate, так и обычные внешние приложения (sed, awk...), работающие со стандартным вводом/выводом. В случае

когда Delegate выступает в качестве HTTP прокси-сервера, для хранения объектов может быть использован постоянный кэш, размещенный на диске. Поддержка протокола ICP позволяет эффективнее взаимодействовать с другими кэш-серверами. Авторизация пользователей, если она необходима, происходит через PAM и собственную службу авторизации DGAuth.

Для ограничения загрузки сервера поддерживается ограничение по количеству соединений, тайм-ауту. Если взглянуть на Delegate, создается ощущение, что он представляет собой гигантский запутанный конструктор, из которого можно смастерить практически любой прокси-сервис.

Тем не менее функциональности для кэширующего прокси недостаточно.

Прозрачное HTTP-проксирование поддерживается не полностью, поскольку реализация опирается только на данные «Host:» HTTP-заголовка, а он не всегда присутствует. Не поддерживаются протоколы WCCP, CARP. Вместо стандартного протокола ICAP поддерживается свой собственный интерфейс фильтрации, что затрудняет встраивание стандартных сервисов фильтрации и аудита. Не поддерживаются схемы авторизации NTLM, MSNT, что затрудняет интеграцию в сеть, построенную на технологии Windows.

Скажем несколько слов об архитектуре Delegate. Сервер каждого протокола работает в отдельном процессе и при каждом соединении с пользователем порождает новый процесс.

Для пересылки информации по каналу данных в протоколе FTP создаются дополнительные процессы. Фильтры также создают дополнительные процессы для запуска внешних программ фильтрации. Скорость работы таких фильтров оставляет желать лучшего. Когда количество клиентов достигает хотя бы тысячи, создается большое количество процессов, что ведет к неразумному расходу ресурсов и большой загрузке системы.

Несмотря на все перечисленные недостатки, Delegate может быть весьма полезен в небольших сетях для решения простых задач, поскольку весьма прост в конфигурации. В таких сетях загрузка прокси будет небольшой, и проблемы с производительностью не возникнут.

Большинство офисных ПК работают под управлением ОС семейства Windows(как правило, Windows XP SP3), именно поэтому данный продукт не подойдет для данных сетей. «Кэширующий прокси-сервер» способен обслуживать как ПК под управлением Windows, так и UNIX-подобных систем.

2.3. WinGate

WinGate - один из популярных прокси-серверов, позволяющий нескольким пользователям локальной сети получить доступ в Интернет.

К положительным сторонам Wingate относятся его стабильность и простота установки, настройки и использования. Реализована поддержка всех новейших протоколов и возможностей.

К недостаткам можно отнести:

- Невозможность работы в корпоративных сетях.
- Слабая защищенность пользователей от внешних угроз

Данный прокси-сервер не может корректно работать с запросами более чем 25 машин и число коллизий возрастает до 10%. В «Кэширующем прокси-сервере» эта проблема решена путем расширения таблиц кэширования.

2.2.4. UserGate

UserGate - это комплексное решение для подключения пользователей к сети Интернет, обеспечивающее полноценный учет трафика, разграничение доступа и предоставляющее встроенные средства сетевой защиты.

UserGate позволяет тарифицировать доступ пользователей к сети Интернет, как по трафику, так и по времени работы в сети. Администратор может добавлять различные

тарифные планы, осуществлять динамическое переключение тарифов и регулировать доступ к ресурсам Интернет. Встроенный межсетевой экран и антивирусный модуль позволяют защищать сервер UserGate и проверять проходящий через него трафик на наличие вредоносного кода.

UserGate состоит из нескольких частей: сервер, консоль администрирования («UserGate Administrator») и несколько дополнительных модулей. Сервер UserGate (процесс usergate.exe) - это основная часть прокси - сервера, в которой реализованы все его функциональные возможности. Сервер UserGate предоставляет доступ в сеть Интернет, осуществляет подсчет трафика, ведет статистику работы пользователей в сети и выполняет многие другие задачи. Консоль администрирования UserGate - это программа, предназначенная для управления сервером UserGate. Консоль администрирования UserGate связывается с серверной частью по специальному протоколу поверх TCP/IP, что позволяет выполнять удаленное администрирование сервера.

UserGate включает четыре дополнительных модуля: «Статистика UserGate», «Веб-статистика», «Клиент авторизации UserGate» и модуль «Контроль приложений».

Данный прокси-сервер является весьма популярным программным продуктом на IT-рынке

К недостаткам можно отнести:

- Достаточно высокая стоимость программного продукта.
- Сложность настройки NAT.

UserGate является отличным решением для однородных сетей Windows. Однако его стоимость достаточно высока, и не каждый руководитель может себе позволить себе оплатить расходы на ее эксплуатацию. «Кэширующий прокси сервер» задумывался как бесплатное ПО с открытым кодом.

2.5. Traffic Inspector

Traffic Inspector - позволяет решить большинство задач, возникающих при подключении к Интернет по выделенному каналу: обеспечение доступа в сеть Интернет из внутренней сети; авторизация и разграничение доступа пользователей; билинг (тарификация пользователей, подсчет трафика и блокировка доступа при перерасходе); обеспечение пользователей средствами экономии трафика и предоставление возможности самостоятельно контролировать свою работу в Интернет; сетевая защита (Firewall), позволяющая закрыть сервер доступа и внутреннюю сеть от несанкционированного доступа извне; подробный анализ сетевого трафика, потребляемого у провайдера; динамическое ограничение скорости работы пользователей или их групп; Advanced Routing (Policy Routing или Source Routing) — возможность гибкой настройки перенаправления разных пользователей и видов трафика на разные каналы доступа; отключение пользователей от сети Интернет при заражениях сетевыми вирусами и др.

Основным недостатком данного прокси-сервера является его низкая устойчивость к сбоям даже в сетях малого офиса. В случае внезапной остановки службы сервера необходимо перезапускать все машины в локальной сети за минимальный промежуток времени.

3 Настройка КЭШа в UserGate

Одним из назначений прокси-сервера является кэширование сетевых ресурсов. Кэширование снижает нагрузку на подключение к сети Интернет и ускоряет доступ к часто посещаемым ресурсам. Прокси-сервер UserGate выполняет кэширование HTTP и FTP-трафика. Кэшированные документы помещаются в локальную папку %UserGate_data%\Cache. В настройках кэша указывается: предельный размер кэша и время хранения кэшированных документов.

Дополнительно можно включить кэширование динамических страниц и подсчет трафика из кэша. Если включена опция Считать трафик из кэша, на пользователя в UserGate будет записываться не только внешний (Интернет) трафик, но также и трафик, полученный из кэша UserGate.

Параметр «Игнорировать заголовок Pragma - No Cache» позволяет кэшировать все документы, которые будут отдавать Веб-сервера, и помещать их соедржимое в базу кэш UserGate. Использовать этот параметр нужно очень осторожно и исключительно в нужных ситуациях или для целей тестирования.

Внимание! Чтобы посмотреть текущие записи в кэш, необходимо запустить специальную утилиту для просмотра базы данных кэш. Она запускается через нажатие правой кнопки мыши на иконке «UserGate агент», в системном трее и выборе пункта «Открыть обозреватель кэш».

Внимание! Если вы включили кэш, а в «обозревателе кэш» у вас по прежнему нет ни одного ресурса, то вам скорей всего необходимо включить прозрачный прокси-сервер для протокола HTTP, на странице «Сервисы – Настройка прокси - HTTP».

Обозреватель кэш в UserGate

Модуль Обозреватель кэш (рис. 2) предназначен для просмотра содержимого базы кэш в UserGate. Обозреватель кэш может быть запущен через пункт Запустить обозреватель кэш меню UserGate агента в системном трее или через соответствующий пункт в меню Пуск – Программы. При запуске требуется указать расположение файла cache.dat (база Кэш UserGate).

Интерфейс обозревателя позволяет выполнять поиск, сортировку и фильтрацию содержимого кэш. Дополнительно предоставлена возможность сохранения выделенных или всех документов кэш в указанную папку.

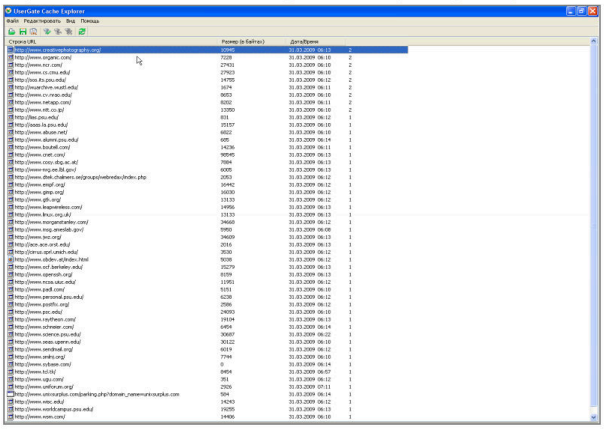


Рисунок 2. Обозреватель КЭШ

рактическое задание

Выполните установку прокси-сервера UserGate. (С особенностями установки и системными требованиями познакомьтесь в Инструкции пользователя.)

Используя панель администрирования подключитесь к прокси-серверу.

Перейдите в раздел КЭШ.

Познакомьтесь с особенностями настройки параметров кэширования.

Выполните просмотр содержимого базы кэш при помощи обозревателя КЭШ.

Контрольные вопросы

1. Определите назначение прокси-сервера.
2. Раскройте функции основных типов прокси-серверов
   - *Обратный прокси*,
   - *Кэширующий прокси-сервер*
   - *Веб-прокси, фильтрующий содержимое*
   - *Анонимный прокси-сервер*
   - *Враждебный прокси-сервер*
   - *Прозрачный прокси*
   - *Принудительный прокси-сервер*

- *Суффиксный прокси-сервер*
- *Открытый прокси-сервер*
- *HTTP-прокси*
- *SOCKS proxy*
- *HTTPS-прокси*
- *FTP-прокси*
- *Mapping-прокси*

3. Охарактеризуйте следующие прокси (*Squid, DeleGate, WinGate, UserGate, Traffic Inspector*)
4. Раскройте особенности настройки кэширования в прокси-сервере *UserGate.*

Лабораторная работа
Тема: «Настройка брандмауэра для доступа к локальным и глобальным сетям»

Цель работы: научиться настраивать брандмауэр

Теоретические сведения

Брандмауэр Windows 7

Брандмауэр Windows7 — тема нашей сегодняшней статьи, в ней мы рассмотрим его и узнаем ответы на следующие вопросы: **Как отключить брандмауэр в Windows 7**, **Как включить брандмауэр в Windows 7** и как выполнить настройку брандмауэра. *Брандмауэр* или **Firewall** — это одно и тоже,так же брандмауэр называется межсетевым экраном, по этому научившись работать с брандмауэром, вы научитесь настраивать**Фаервол и Межсетевой экран Windows 7.**

Нужен ли брандмауэр Windows 7

Брандмауэр Windows 7 - это специальная служебная программа, предназначенная для контроля за сетевыми интерфейсами, контролирует выход программ в интернет, является своего рода защитой от проникновения вирусов и предотвращает их распространение. Для многих пользователей компьютеров, брандмауэр кажется совершенно не нужным, по этому они сразу же его отключают, так же как и отключают сразу же надоедливый контроль учетных записей в Windows 7.

Практически все современные антивирусные программы, поставляются вместе с фаерволом. Когда вы устанавливаете сторонний антивирус, встроенный брандмауэр перестает работать, для того что бы предотвратить проблемы связанные с конфликтами 2х программ.

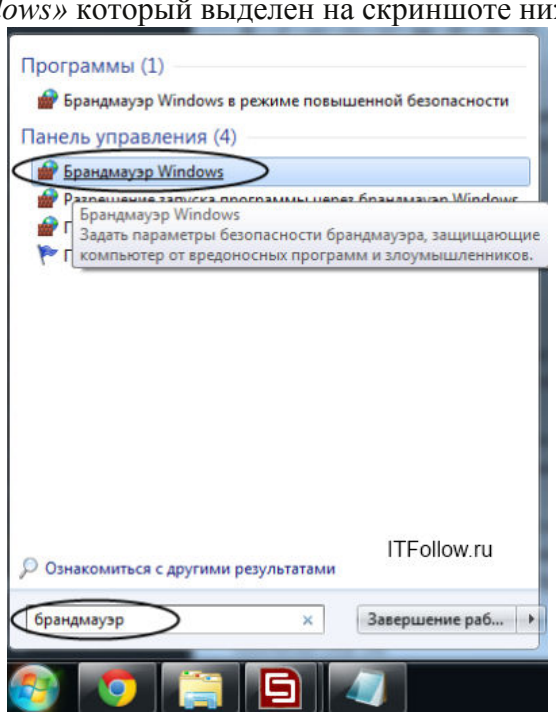
Существуют и простые антивирусы, которые не содержат встроенный фаервол, тот же антивирус от Microsoft -Security Essentails, не содержит встроенного брандмауэра.

Когда устанавливается Windows 7, брандмауэр автоматически включается и настраивается по умолчанию. Для многих пользователей ПК — этих настроек достаточно.

Мы же рассмотрим способы повышения безопасности компьютера, путем внесения изменений в настройки брандмауэра, определяя что он должен пропускать, а что блокировать.

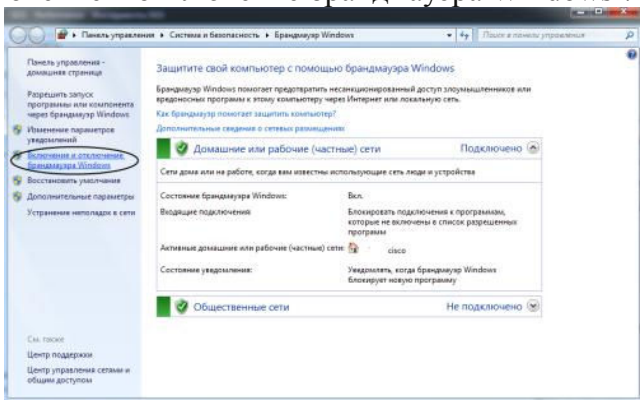
Как открыть брандмауэр в Windows 7

Проще всего найти брандмауэр в Windows 7 — это воспользоваться поиском через меню пуск. Для этого кликните по кнопке «Пуск» в левом нижнем углу экрана и в строку поиска вбейте Брандмауэр и кликните на появившемся значке *«Брандмауэр Windows»* который выделен на скриншоте ниже:



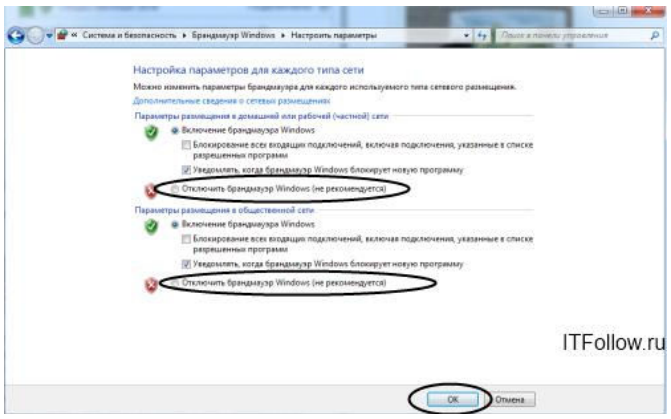
Как выключить брандмауэр Windows 7?

После того как откроется страница брандмауэра, выберите в левом меню пункт «Включение и отключение брандмауэра Windows 7″



Отключение брандмауэра Windows 7

Кликнув по вкладке включение и отключение брандмауэра Windows, вы попадете на страницу, на которой можно как включить, так и отключить брандмауэр Windows 7, просто выбрав пункт меню **«Отключить Брандмауэр (не рекомендуется)»,** причем можно выбрать отключение как только для своей домашней сети, так и для всех остальных.

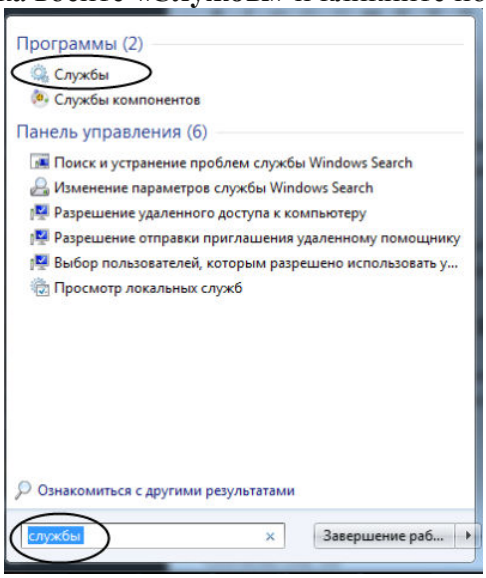


Как вы понимаете, включить брандмауэр Windows 7 (если он выключен) можно точно так же, только лишь необходимо отметить пункт меню**«Включение брандмауэра Windows».**

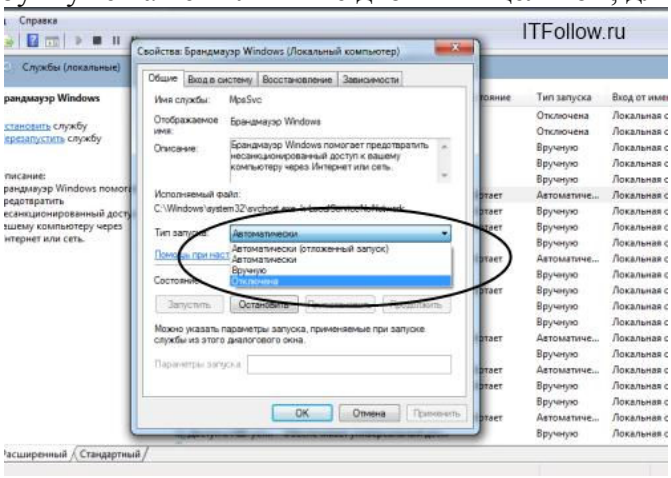
Кстати, в этом же окошке можно снять галочки различных уведомлений когда брандмауэр блокирует новые программы.

Отключение службы Брандмауэр Windows

Для оптимизации операционной системы, так же рекомендуется отключить службу Брандмауэра Windows 7. Проще всего опять использовать поиск в меню **«Пуск».** В строку поиска вбейте **«Службы»** и кликните по ним, для того что бы их открыть.

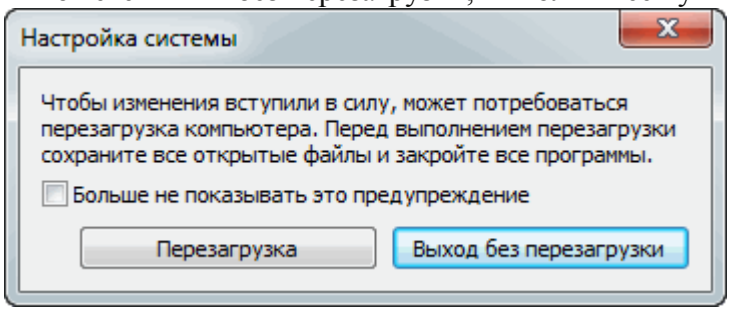


Для того что бы быстро найти службу Брандмауэр Windows, кликните на любой службе одни раз и нажмите на клавиатуре букву Б, вы сразу же найдете нужную нам службу и уже на ней кликните двойным щелчком, для того что бы ее открыть.



В строке Состояние — нажмите О**становить**. Откройте выпадающее меню Тип запуска и выберите **Отключена** и нажмите **ОК.**

Появится диалоговое окно с предложением перезагрузить компьютер прямо сейчас или вы можете выйти без перезагрузки, выполнив ее чуть позже.



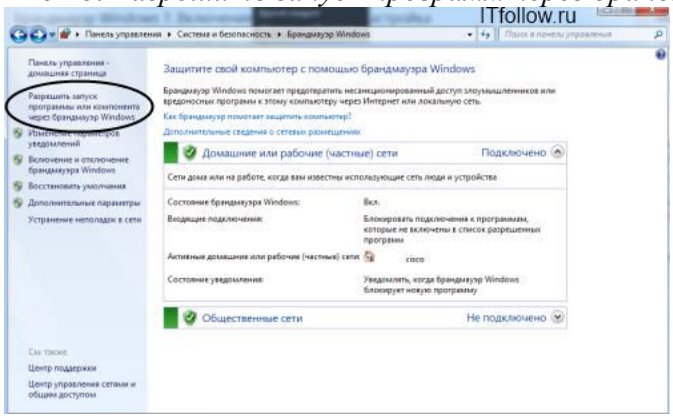
Для того что бы включить брандмауэр Windows 7, выполните те же действия в обратном порядке.

Настройка брандмауэра Windows 7

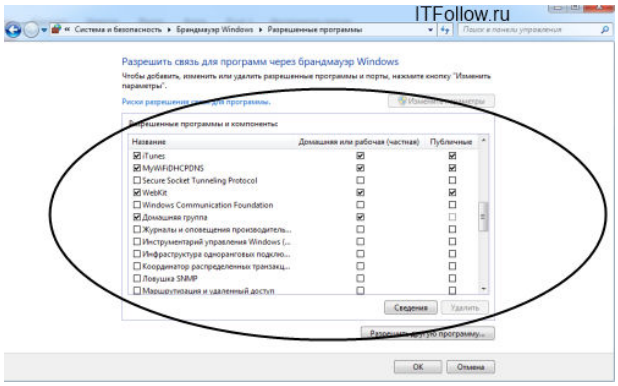
Исключения брандмауэра Windows 7

Когда брандмауэр блокирует приложения или например брандмауэр порой блокирует доступ к интернет сети для некоторых игр, существует достаточно простой способ снять это ограничение и дать полный доступ на выход в интернет для этого приложения, в этой сети, к которой вы подключены.

Для этого на странице межсетевого экрана (брандмауэра) выберите в левом меню пункт меню: *Разрешить запуск программ через брандмауэр Windows.*



Далее найдите в списке свою программу и дайте ей доступ в нужной сети или сразу во всех, где нет галочек, таким образом можно добавлять **исключения брандмауэра Windows 7.**

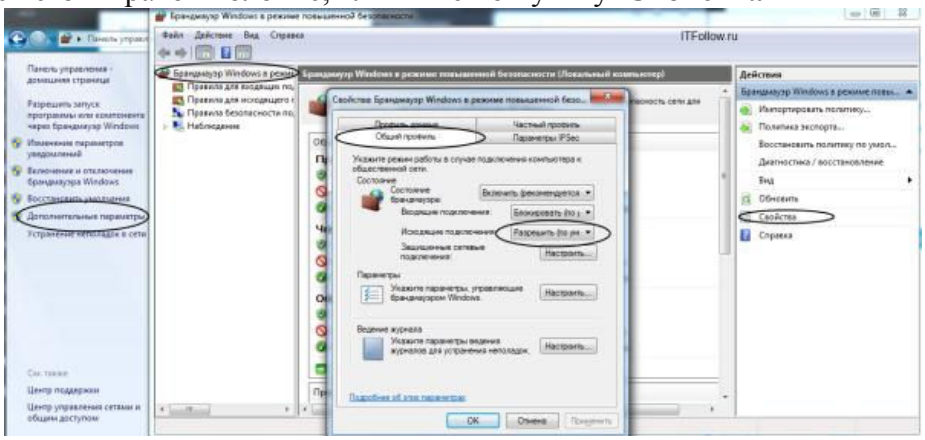


Блокировка исходящего трафика

Для повышения безопасности компьютера, что иногда бывает особенно необходимо, можно воспользоваться способом полной блокировки исходящего трафика, т.е. такого трафика, который передается от вашего компьютера к удаленному серверу, разрешить лишь для некоторых необходимых приложений и их соответствующих служб.

Для настройки брандмауэра Windows , необходимо перейти на вкладку **Дополнительные параметры** в окне Брандмауэра.

Выберите *Брандмауэр Windows в режиме повышенной безопасности* в левом меню, после чего в правой колонке, кликните по пункту**«Свойства»**



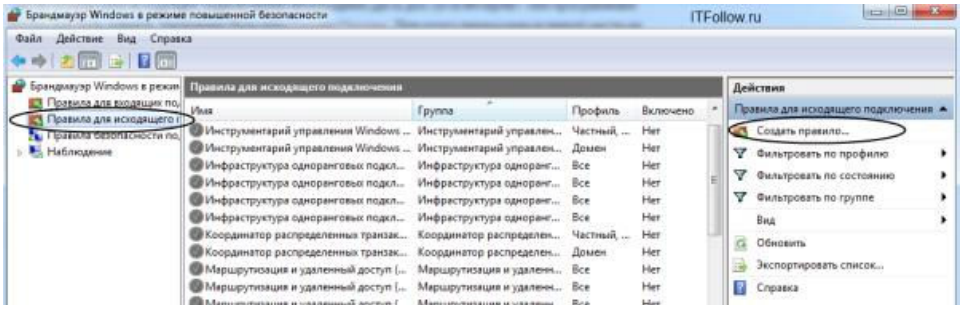
Откроется меню **Свойства Брандмауэра,** в котором можно заблокировать весть исходящий трафик, на вкладке *Исходящие подключения.*

В выпадающем меню выберите *«Блокировать»* и нажмите Ок.

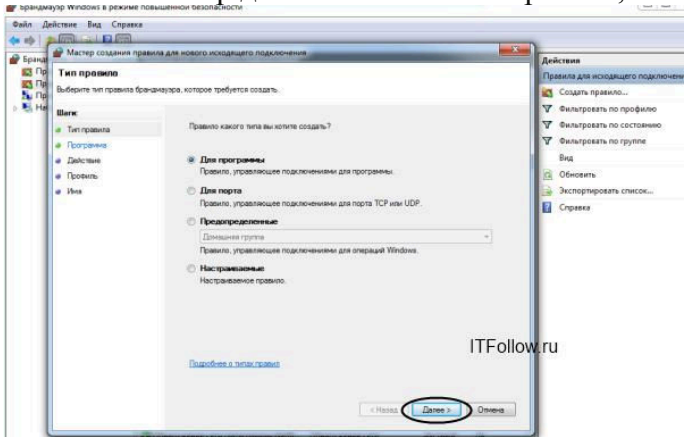
Разрешение для программ после блокировки

После того как были заблокированы все исходящие подключения к интернет, можно создать правило, которое позволит подключаться к интернету некоторым программам. Давайте для примера создадим правило разрешающее браузеру Google Chrome подключаться к сети интернет.

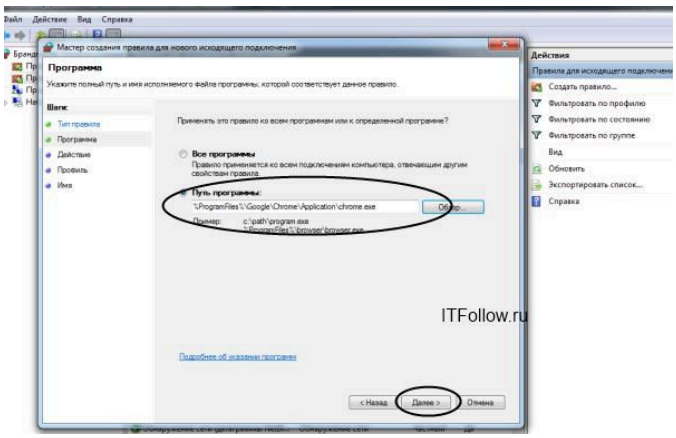
Для того что бы создать правило исходящего подключения, выберите «Правила для исходящего подключения», а в колонке действия выберите «Создать правило»:



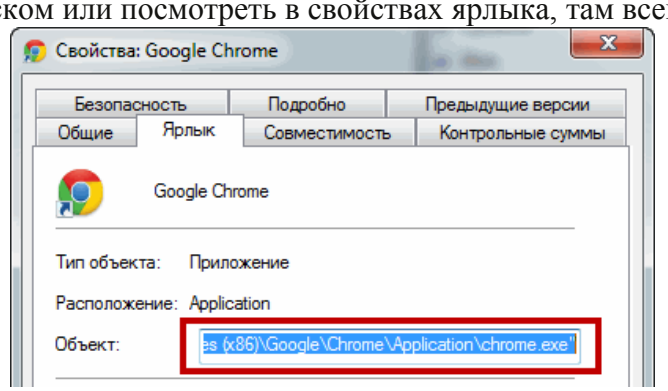
Появится мастер добавления нового правила, в котором необходимо нажать Далее→



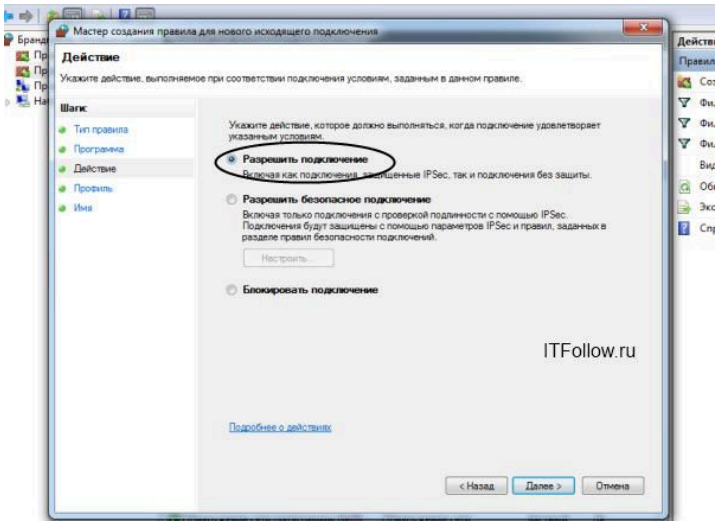
На следующей странице, используя кнопку Обзор добавляете путь к приложению, в нашем случае к браузеру Google Chrome.



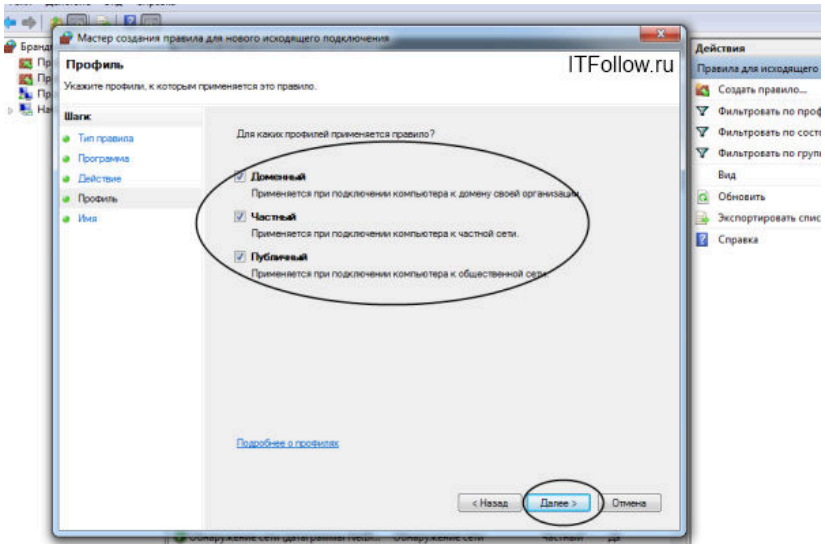
Для поиска пути расположения нужного exe файла, вы можете воспользоваться поиском или посмотреть в свойствах ярлыка, там всегда указан путь к приложению.



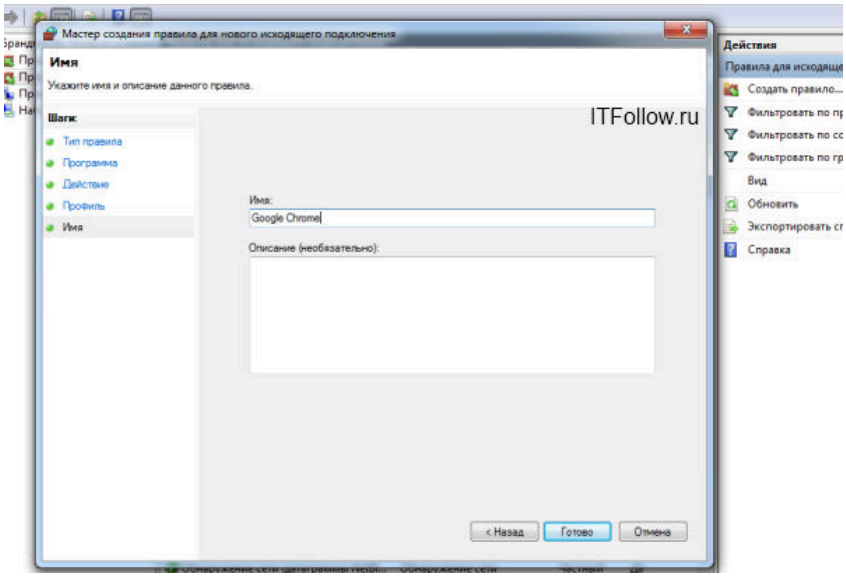
Нажимаете далее →на следующем шаге отмечаете **Разрешить подключение** и опять **далее→**



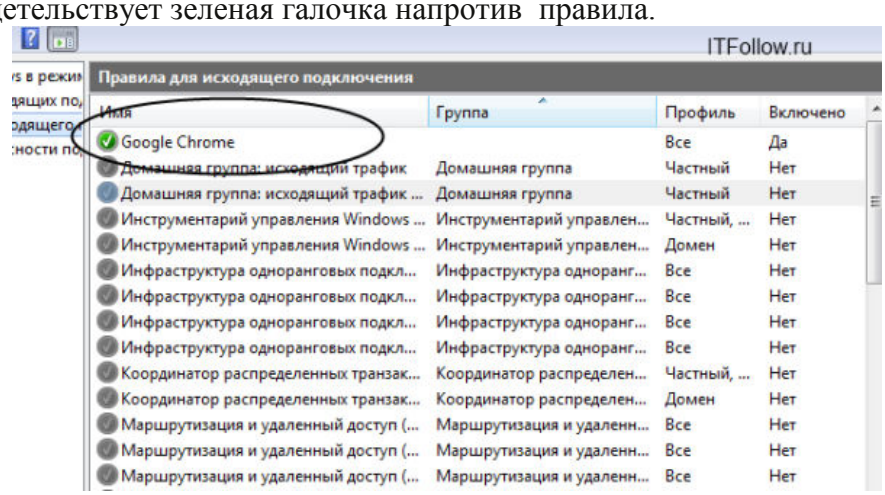
Отмечаете как на скриншоте ниже и нажимаете Далее



На следующем шаге необходимо ввести имя для правила и если необходимо, то и его описание



Вот и все, новое правило для брандмауэра успешно создано и работает, о чем свидетельствует зеленая галочка напротив правила.



Точно таким же образом можно добавить правило в брандмауэр для любого нужного порта, для этого в начале необходимо выбрать «Создать правило для порта».

Проверка Брандмауэра

По завершению проведения всех работ по настройке брандмауэра, рекомендуем проверить его работоспособность, воспользуйтесь для этого простым сервисом для тестирования фаерволов на сайте 2IP- http://2ip.ru/firewalltest/

Контрольные вопросы

1. Брандмауэр Windows 7

2 Как открыть брандмауэр в Windows 7

3 Как выключить брандмауэр Windows 7?

4 Отключение брандмауэра Windows 7

5 Отключение службы Брандмауэр Windows

6 Настройка брандмауэра Windows **7**

- Исключения брандмауэра Windows 7
- Блокировка исходящего трафика
- Разрешение для программ после блокировки
- Проверка Брандмауэра

Лабораторная работа
Тема: «Трансляция ip NAT»

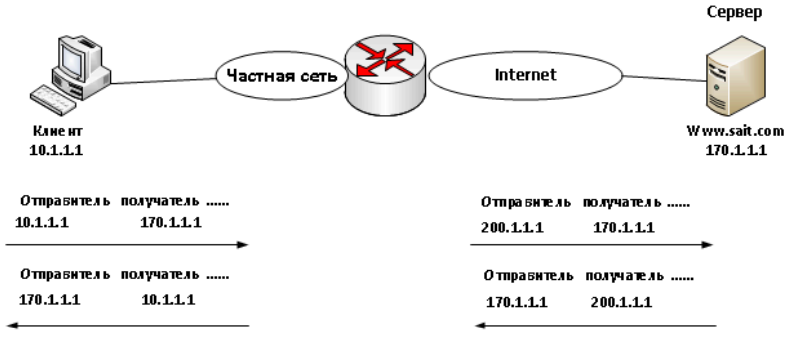
Цель работы: знакомство трансляцией ip NAT

Теоретические сведения.

Трансляция ip NAT

Трансляция ip NAT, определенная в RFC 3022, позволяет узлу, который не имеет действительного, зарегистрированного глобального уникального IP адреса, осуществлять связь с другими узлами через сети передачи данных. Эти узлы могут использовать частные адреса. *Трансляция NAT* позволяет продолжать использование этих адресов, не готовых для интернета, и осуществлять связь с узлами в интернете.

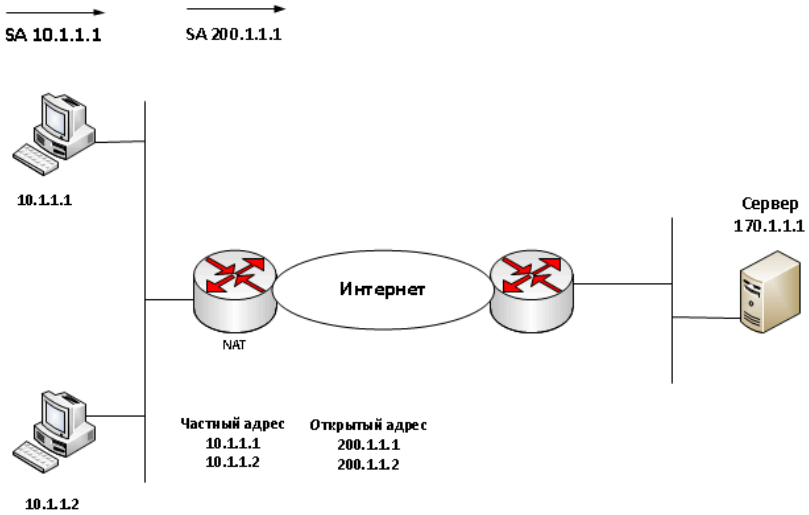
Эта цель достигается настройкой NAT, и дальнейшим использования действительных зарегистрированных IP-адресов для представления данного частного адреса всем остальным узлам интернета. Функция NAT заменяет частные IP-адреса открытыми зарегистрированными IP-адресами в каждом пакете протокола IP, как показано на рисунке ниже



Обратите внимание на то, что, выполняя трансляцию NAT, маршрутизатор изменяет IP адрес отправителя в тот момент, когда пакет покидает организацию. Маршрутизатор, выполняющий трансляцию сетевых адресов, также изменяет адрес получателя каждого пакета, который возвращается назад в частную сеть. Функция NAT, сконфигурированная на маршрутизаторе, выполняет трансляцию адресов. Программное обеспечение Cisco IOS поддерживает несколько разновидностей трансляции ip NAT. Далее в настоящей статье описываются принципы, лежащие в основе этих разновидностей трансляции.

Статическая трансляция NAT

Статическая трансляция NAT работает точно так же, как было показано в примере выше, однако IP-адреса преобразуются друг в друга статически. Для того чтобы читателю стали понятными результаты статической трансляции NAT, и для объяснения некоторых ключевых терминов, ниже приведен более подробный пример.



Сначала рассмотрим основные принципы. ISP-провайдер компании назначает ей зарегистрированный номер сети 200.1.1.0. Соответственно, маршрутизатор NAT должен сделать так, чтобы этот частный адрес выглядел таким образом, как если бы он находился в сети 200.1.1.0. Для этого маршрутизатор NAT изменяет IP адрес отправителя в пакетах, которые на рисунке пересылаются слева направо.

В данном примере маршрутизатор NAT изменяет адрес отправителя 10.1.1.1 (на рис. обозначен как «SA») на адрес 200.1.1.1 . При использовании статической трансляции NAT маршрутизатор NAT просто осуществляет взаимно однозначное преобразование между частным адресом и зарегистрированным адресом, от имени которого он выступает. На маршрутизаторе NAT сконфигурировано статическое преобразование частного адреса 10.1.1.1 в открытый зарегистрированный адрес 200.1.1.1 .

Поддержка двух IP-узлов в частной сети требует второго взаимно однозначного преобразования с использованием второго IP-адреса в диапазоне открытых адресов. Например, для поддержки адреса 10.1.1.2 маршрутизатор просто преобразует адрес 10.1.1.2 в адрес 200.1.1.2 . Поскольку предприятие имеет одну зарегистрированную сеть класса C, используя трансляцию NAT, оно может поддерживать до 254 частных IP-адресов (при этом зарезервированы два обычных адреса — номер сети и ее широковещательный адрес).

Терминология, используемая для трансляции сетевых адресов, особенно касающаяся ее конфигурирования, может оказаться несколько непривычной. Обратите внимание на то, что в таблице NAT частные IP-адреса приводятся как «частные», открытые зарегистрированные адреса сети 200.1.1.0 — как «открытые». К примеру компания Cisco использует термин «внутренний локальный адрес» для частных IP-адресов (как это сделано в данном примере) и термин «внутренний глобальный адрес» для открытых IP-адресов.

В терминологии Cisco сеть предприятия, которая использует частные адреса и, следовательно, требует использование трансляции сетевых адресов, является «внутренней» частью сети. Интернет-интерфейс трансляции NAT является «внешней» частью сети. Узел, которому необходима трансляция ip NAT (в данном примере 10.1.1.1), имеет IP адрес, который он использует внутри сети, и ему требуется IP адрес, который будет представлять его вне этой сети.

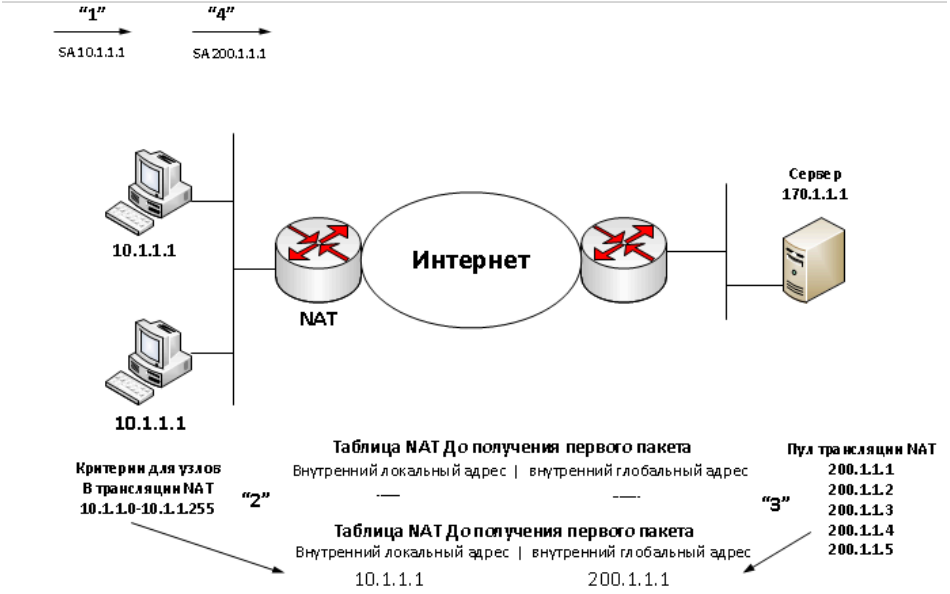
Термины адресации NAT

ТЕРМИН	ОПРЕДЕЛЕНИЕ
Внутренний локальный адрес (inside local)	При типичном проектировании NAT термин "внутренний" относится к адресу, используемому для узла на предприятии. Внутренним локальным называется действующий IP-адрес, назначенный узлу в частной сети предприятия. Более наглядным термином мог бы быть "внутренний частный адрес"
Внутренний глобальный адрес (indide global)	При типичном проектировании NAT термин "внутренний" относится к адресу, используемому для узла на предприятии. Трансляция NAT использует внутренний глобальный адрес для представления внутреннего узла, когда пакет пересылается через внешнюю сеть, обычно через сеть интернет. Маршрутизатор NAT изменяет IP-адрес отправителя в пакете, посылаемом внутренним узлом, с внутреннего локального адреса на внутренний глобальный адрес, в то время, когда пакет пересылается из внутренней сети во внешнюю. Более наглядным мог бы быть термин "внутренний открытый (общедоступный)", поскольку при использовании на предприятии адресов RFC 1918 внутренний глобальный представляет внутренний узел с открытым IP-адресом, который может быть использован для маршрутизации в открытой сети интернет.
Внешний глобальный адрес (Outside global)	При типичном проектировании NAT термин "внешний" относится к адресу, используемому для узла вне предприятия, иными словами - в интернете. Внешний глобальный адрес представляет собой реальный IP-адрес, назначенный узлу, который находится в сети, обычно в сети интернет. Более содержательным (точным) термином мог бы быть "внешний открытый", поскольку внешний глобальный адрес представляет внешний узел открытым IP-адресом, который может использоваться для маршрутизации в интернет
Внешний локальный адрес (Outside local)	NAT может транслировать внешние IP-адреса, т.е. IP-адреса, представляющие узел вне сети предприятия, хотя эта опрция не очень популярна. Когда маршрутизатор NAT пересылает пакет из внутренней сети во внешнюю, используя NAT для изменения внешнего адреса, IP-адрес, представляющий внешний узел в качестве IP-адреса получателя в заголовке пакета, называется внешним локальным IP-адресом. Более содержательным мог бы быть термин "внешний частный", поскольку, используя адреса RFC 1918 На предприятии, внешний локальный адрес представляет внешний узел с частным IP-адресом из RFC 1918

Динамическая трансляция NAT

В сравнении со статической динамическая *трансляция NAT* имеет как сходства, так и отличия. Как и в случае использования статической NAT, маршрутизатор NAT осуществляет взаимно однозначное преобразование между внутренним локальным и внутренним глобальным адресами и изменяет IP-адреса в пакетах, когда они входят во внутреннюю сеть и выходят из нее. Однако преобразование внутренних локальных адресов во внутренние глобальные адреса происходит динамически.

Динамическая трансляция NAT создает пул возможных внутренних глобальных адресов и определяет критерий соответствия для определения того, какие внутренние глобальные IP-адреса должны транслироваться с помощью NAT. Например, на рисунке ниже, был установлен пул из пяти глобальных IP-адресов в диапазоне 200.1.1.1 — 200.1.1.5 . Трансляция NAT также сконфигурирована для трансляции всех внутренних локальных адресов, которые начинаются с октетов 10.1.1 .



Номера 1,2,3 и 4 на рисунке относятся к такой последовательности событий.

- узел 10.1.1.1 посылает свой первый пакет на сервер, расположенный по адресу 170.1.1.1
- Когда данный пакет поступает на маршрутизатор NAT, этот маршрутизатор применяет логику проверки соответствия и решает, следует ли применить к этому пакету трансляцию NAT. Поскольку логика маршрутизатора сконфигурирована на

соответствие IP-адресам отправителя, которые начинаются с 10.1.1, маршрутизатор добавляет запись в свою таблицу NAT для адреса 10.1.1.1 в качестве внутреннего адреса

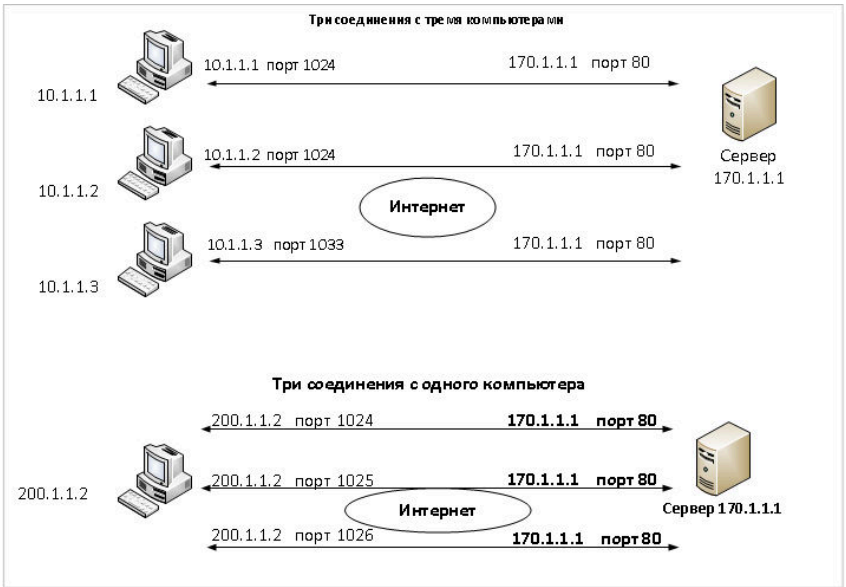
- Маршрутизатору NAT Требуется выделить IP адрес из пула действительных внутренних глобальных адресов. Он выбирает первый доступный адрес (в данном случае 200.1.1.1) и добавляет его в таблицу NAT для завершения записи.
- Маршрутизатор NAT транслирует IP адрес отправителя и пересылает пакет. Динамическая запись остается в таблице до тех пор, пока продолжается передача данных. Можно задать значение тайм-аута, который определяет, как долго должен ожидать маршрутизатор пока не транслируются пакеты с таким адресом, перед удалением этой динамической записи.

Трансляция NAT может быть сконфигурирована с большим количеством IP-адресов в списке внутренних локальных адресов, чем в пуле внутренних глобальных адресов. Маршрутизатор выделяет адреса из пула до тех пор, пока все они не будут выделены. Если поступает новый пакет от еще одного внутреннего узла и ему требуется запись NAT, а все находящиеся в пуле IP-адреса уже используются, то маршрутизатор просто отбрасывает данный пакет. Пользователь должен повторять попытку до тех пор, пока не истечет время тайм-аута записи NAT; в этот момент функция NAT работает для следующего узла, который отправляет пакет. По существу, размер внутреннего глобального пула адресов должен соответствовать максимальному количеству конкурирующих узлов, которым требуется одновременный доступ к сети интернет (кроме случая использования трансляции PAT, описанной ниже).

Трансляция на основе портов PAT

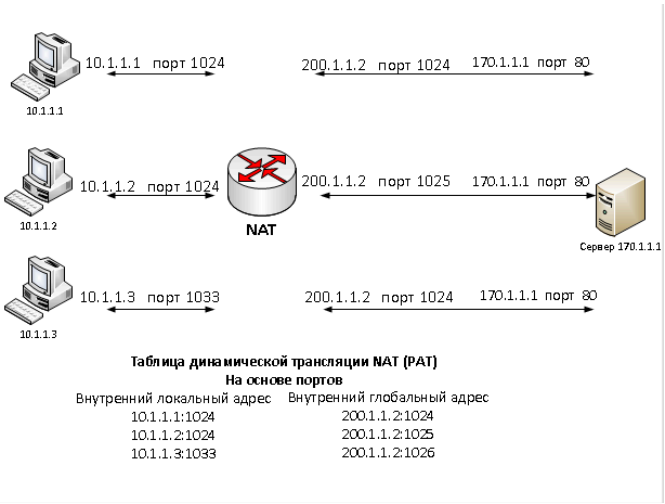
В некоторых сетях требуется, чтобы большинство их IP-узлов, если не все, имели доступ к Интернету. Если такая сеть использует частные IP-адреса, то маршрутизатору NAT необходим очень большой набор зарегистрированных IP-адресов. При использовании статической трансляции ip NAT для каждого частного IP-узла, которому требуется доступ к интернету, необходимо иметь открытый зарегистрированный IP-адрес, что полностью подрывает намерение уменьшить количество нужных организации открытых адресов протокола IPv4. Динамическая трансляция NAT в определенной степени смягчает эту проблему, поскольку редко требуется одновременный выход в интернет всем узлам объединенной сети. Однако если большей части узлов сети необходим доступ к Интернету в течении всего обычного рабочего дня, то трансляции NAT по-прежнему нужно большое количество зарегистрированных IP-адресов, что вновь не позволяет уменьшить расход адресов протокола IPv4.

Функция PAT, также называемая трансляцией адресов портов, решает эту проблему. PAT позволяет трансляции NAT выполнить масштабирование для поддержки многих клиентов всего лишь несколькими открытыми IP-адресами. Для того чтобы понять функционирование перезагрузки, следует вспомнить, как узлы используют порты протоколов TCP и UDP (транспортный уровень). Ниже будет приведен пример, который помогает понять и сделать более ясной логику PAT.



В верхней части рисунка показана сеть с тремя различными узлами, подключенными к веб-серверу с использованием протокола TCP. В нижней части рисунка показана та же самая сеть позднее, с тремя соединениями протокола TCP от одного и того же клиента. Все шесть соединений связывают IP адрес сервера (170.1.1.1) с портом (в данной ситуации общеизвестный порт 80 для веб-служб). В каждом случае сервер различает отдельные соединения, поскольку комбинация «IP-адрес — номер порта» уникальны.

Трансляция NAT Учитывает тот факт, что серверу не важно, имеется ли одно соединение с тремя различными узлами или три соединения с одним IP-адресом узла. Поэтому для поддержки многих внутренних локальных IP-адресов с помощью всего лишь нескольких внутренних глобальных открытых зарегистрированных IP-адресов, PAT транслирует как адрес, так и, возможно, номера портов. На рисунке ниже проиллюстрирована логика этого процесса.



При создании динамического преобразования PAT cisco выбирает не только внутренний глобальный IP адрес, но и уникальный номер порта, который будет использоваться с этим адресом. Маршрутизатор поддерживает запись в таблице NAT для каждой уникальной комбинации внутреннего локального адреса и порта; при этом поддерживается трансляция во внутренний глобальный адрес и уникальный номер порта, связанный с внутренним глобальным адресом. И поскольку поле номера порта состоит из 16 бит, PAT позволяет использовать более 65тыс. номеров портов, что предоставляет возможность выполнять масштабирование без необходимости иметь много зарегистрированных IP-адресов (во многих случаях требуется лишь один внешний глобальный IP адрес).

Из рассмотренных типов трансляции, PAT, безусловно, является наиболее популярным. Как статическая ip NAT, так и динамическая NAT требуют взаимно однозначного

преобразования внутреннего локального адреса во внутренний глобальный. Трансляция PAT значительно уменьшает количество необходимых зарегистрированных IP-адресов по сравнению с двумя другими NAT-альтернативами.

Правила трансляции сетевого адреса (NAT) UserGate

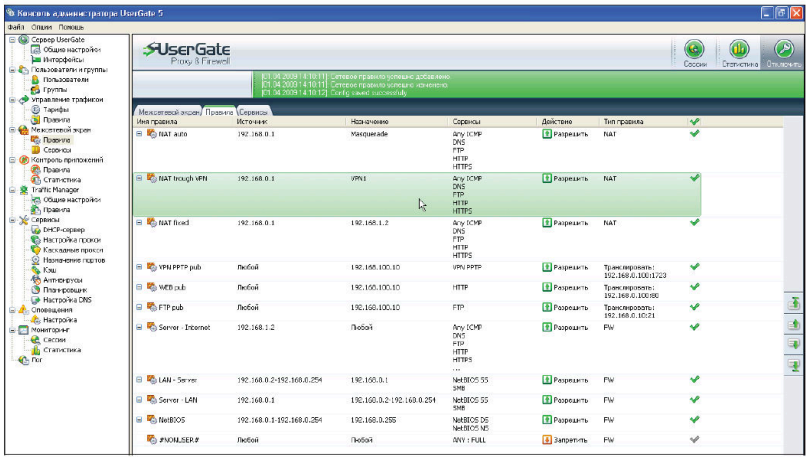
Для создания правила трансляции (рис. 17) в качестве источника требуется выбрать LAN-адаптер, в качестве назначения — WAN-адаптер сервера UserGate, указать один или несколько сервисов, а также выбрать пользователей или группы, которым разрешено использовать данное правило.

Рисунок 17. Создание правила трансляции (NAT)

Для работы правил трансляции в сетевых настройках TCP/IP рабочей станции пользователя необходимо указать шлюз — локальный IP-адрес сервера UserGate и DNS-сервер, поскольку при работе через NATразрешение доменных имен выполняется локально, т.е. на рабочей станции пользователя. Если необходимый сервис (пара «протокол-порт») в списке предопределенных сервисов отсутствует, его можно добавить в диалоге создания правила для межсетевого экрана, или через раздел Сервисы консоли администрирования.

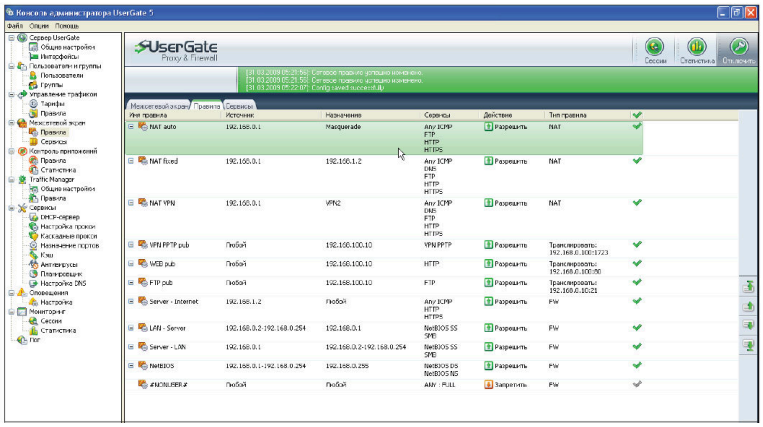
Работа с несколькими провайдерами

Драйвер NATUserGate поддерживает работу с несколькими подключениями к Интернет одновременно. Для такой работы администратор UserGate может создать несколько наборов правил NAT(рис. 18), различающихся только внешними интерфейсами (WAN или PPP). Такая возможность драйвера NATUserGate позволяет предоставить доступ в Интернет для одной части пользователей через одного провайдера, а для другой группы пользователей — через другого. Применять одновременно два набора правил трансляции для пользователя или группы пользователей не рекомендуется.



Автоматический выбор исходящего интерфейса

При наличии нескольких внешних интерфейсов (WAN или PPP) на компьютере с сервером UserGate, в правилах NATв качестве исходящего интерфейса можно выбрать пункт **Masquerade**. Функция **Masquerade** используется, если исходящий сетевой интерфейс сервера при трансляции пакетов, заранее неизвестен. В этом случае интерфейс будет определяться динамически, путем сравнения сетевого адреса хоста назначения с сетевой частью адреса всех WAN-адаптеров сервера UserGate. Если сетевая часть хоста назначения не подходит ни под один из WAN-адаптеров (PPP- адаптеров), пакет будет отправлен через основное подключение Интернет. Функцию Masquerade можно использовать для трансляции пакетов в несколько внешних сетей или, например, для работы NATс резервным каналом.



Важно! Во время работы резервного подключения к Интернет, функция автоматического выбора исходящего интерфейса в правилах NATUserGate отключается. Весь NATтрафик правил с типом назначения **Masquerade** замыкается на резервный интерфейс.

Публикация сетевых ресурсов

С помощью межсетевого экрана UserGate можно открыть доступ к внутренним ресурсам компании, например к Web, FTP, VPN или к почтовому серверу из сети Интернет. В этом случае обращения на определенный порт внешнего IP-адреса сервера UserGate будут переадресованы на внутренний сервер, в соответствии с созданным правилом. Доступ к внутреннему ресурсу компании можно предоставить для всех (**Любой** источник) или только для определенных хостов из сети Интернет. Для создания публикации ресурса (рис. 20) в правиле межсетевого экрана необходимо указывать один сервис.

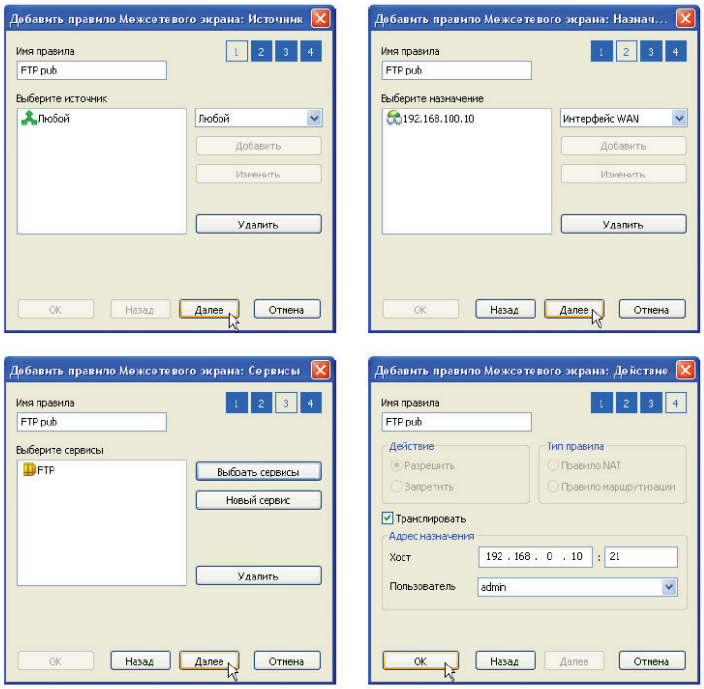
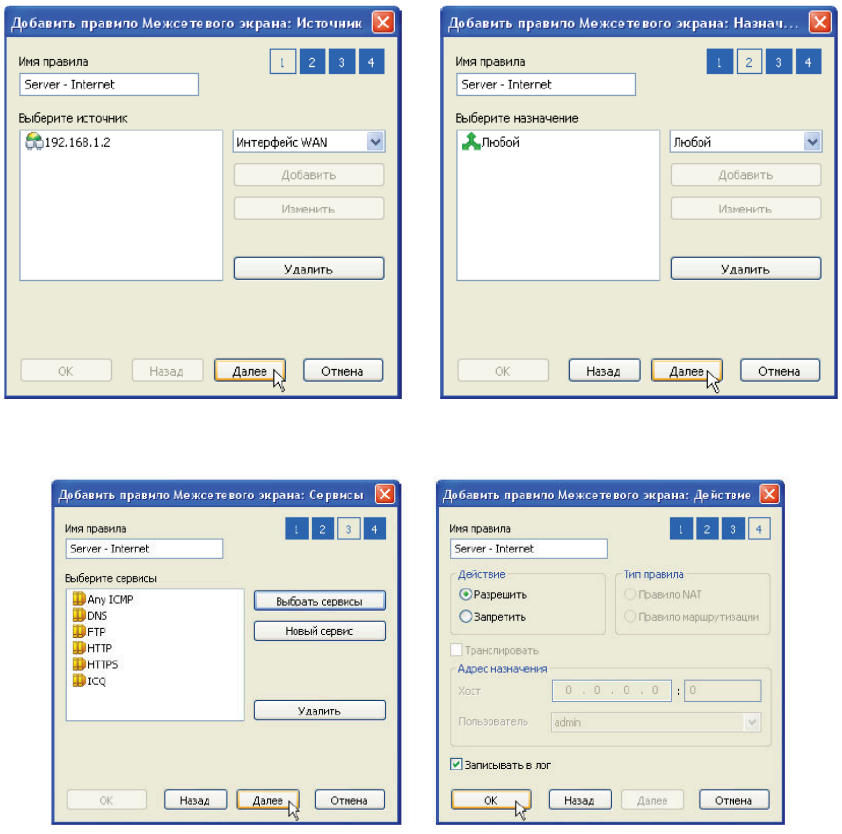


Рисунок 20. Публикация FTP-сервера

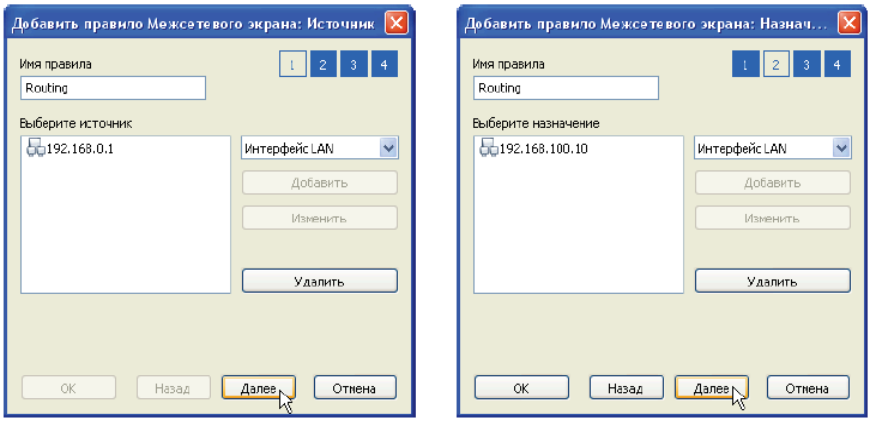
Настройка правил фильтрации

Распространенной является ситуация, когда компьютер с установленным UserGate является одновременно и рабочей станцией и файловым сервером в небольшой локальной сети. Если правило #NONUSER# включено в режим **Запретить**, необходимо создать несколько специальных разрешающих правил для межсетевого экрана. Правила должны разрешать исходящие запросы в Интернет для таких основных сервисов как HTTP, HTTPS, FTP, POP3 и SMTP. Пример таких правил приведен на рисунке 17.



Поддержка маршрутизации

Если компьютер с UserGate подключен к нескольким локальным сетям, сервер UserGate можно настроить как маршрутизатор (router), обеспечив прозрачную, двунаправленную связь между сетями. Правила маршрутизации настраиваются между любой парой LAN-интерфейсов (рис. 22).



Контрольные вопросы

1 Трансляция ip NAT
2 Статическая трансляция NAT
3 Термины адресации NAT
4 Динамическая трансляция NAT
5 Трансляция на основе портов PAT
6 Правила трансляции сетевого адреса (NAT) UserGate
7 Работа с несколькими провайдерами
8 Автоматический выбор исходящего интерфейса
9 Публикация сетевых ресурсов
10 Настройка правил фильтрации
11 Поддержка маршрутизации

Лабораторная работа

Тема: Изучение структуры протоколов SLIP, PPP, PPTP.

Цели работы: Изучить назначение дополнительных протоколов глобальных сетей.

Ход работы.

1. **Протокол SLIP.**

1.1. Опишите назначение протокола

_____
_____
_____
_____
_____
_____
_____

1.2. Область применения

_____
_____
_____

2. **Протокол PPP.**

2.1. Опишите назначение протокола

_____
_____

_____
_____
_____
_____
_____
2.2. Область применения
_____
_____
_____
3. **Протокол PPPoE.**
3.1. Опишите назначение протокола
_____
_____
_____
_____
_____
_____
_____
3.2. Область применения
_____
_____
_____
4. **Протокол PPTP.**
4.1. Опишите назначение протокола
_____
_____
_____
_____
_____
_____
_____
4.2. Область применения
_____
_____
_____

Вывод:

_____
_____
_____
_____

Лабораторная работа
Настройка и использование межсетевого экрана в ОС Windows XP.

Цель работы: Настройка встроенного межсетевого экрана (брандмауэра).

Краткие теоретические сведения:

Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней сети, тем самым обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет **межсетевой экран или брандмауэр (firewall),** под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в систему и/или выходящих из неё, и обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решений о её приеме и/или передаче.

Брандмауэр в ОС Windows XP – это система защиты подключения к Интернет (Internet Connection Firewall, ICF), представляет собой программу настроек ограничений, регулирующих обмен данными между Интернетом и небольшой локальной сетью или локальным компьютером. Брандмауэр ICF необходимо установить для любого компьютера, подключенного к Интернету с помощью модема удаленного доступа, брандмауэр ICF обеспечивает защиту подключения.

Задание: Активизировать встроенный брандмауэр операционной системы Windows XP и настроить его параметры.

Алгоритм выполнения работы:

A. Активизация встроенного сетевого экрана.

1. Откройте компонент Сетевые подключения.
2. Для этого наберите последовательно Пуск-Панель Управления- Сетевые подключения.
3. Выделите подключение удаленного доступа, подключение по локальной сети или высокоскоростное подключение к Интернету, которое требуется защитить брандмауэром, и затем выберите в контекстном меню (при выделенном подключении нажать правую клавишу мыши) команду Свойства.
4. На вкладке Дополнительно в группе Брандмауэр подключение к Интернету отметьте пункт Защитить моё подключение к Интернету. (рис 1.), отметьте пункт Включить.

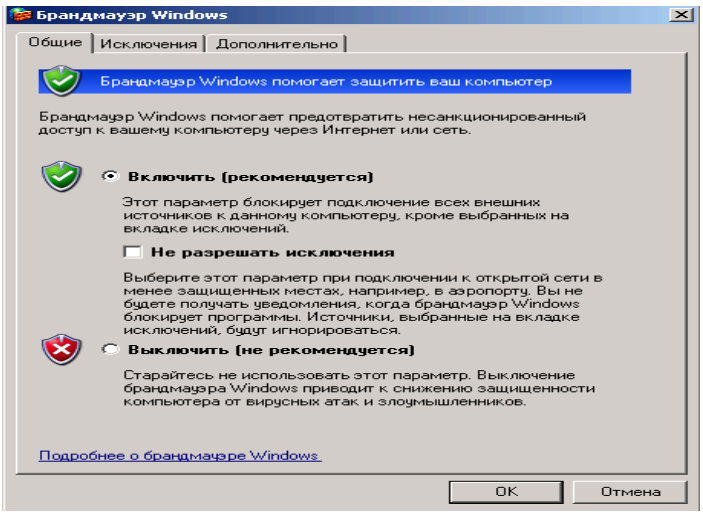


Рис. 1

Примечание: *Для отключения брандмауэра достаточно поставить флажок Выключить.*

B. **Настройка параметров брандмауэра.**

1. Выполните пункты 1-3 предыдущего задания.
2. Выберите кнопку Параметры в верхней части окна (рис.2).

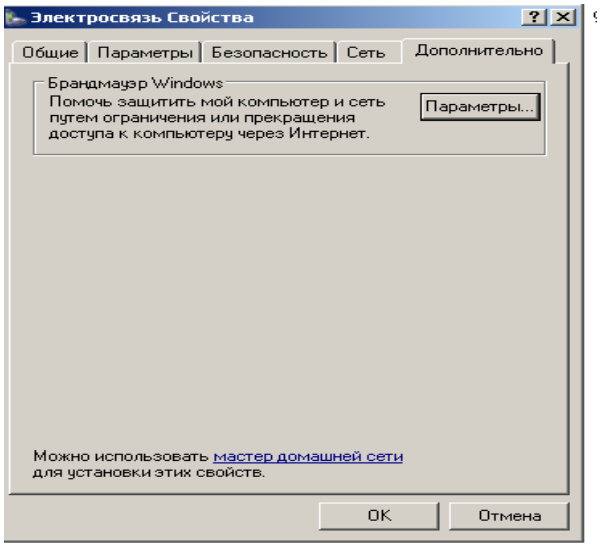


Рис. 2

3. В результате откроется окно Дополнительные параметры (рис. 3) с четырьмя закладками (параметры сетевого подключения, параметры по умолчанию, ведение журнала безопасности, протокол ICMP).

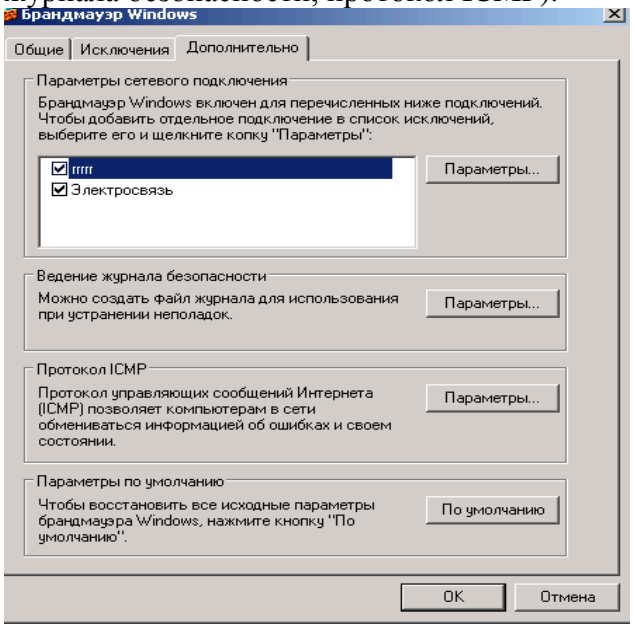


Рис. 3

4. Выберите закладку Службы (рис. 4).

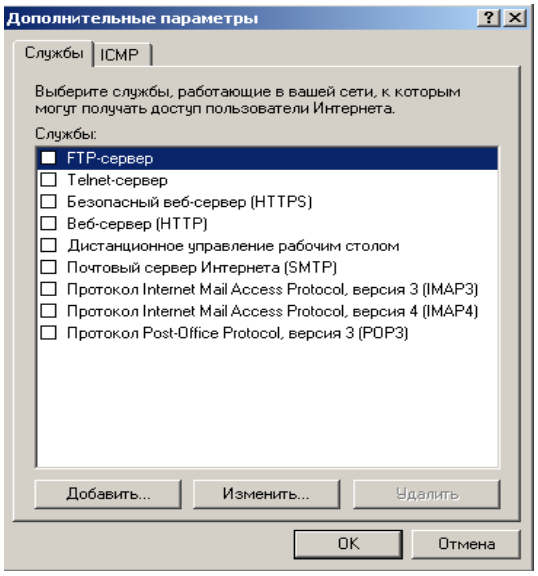


Рис. 4

Примечание: *На закладке службы Вы можете в явном виде указать службы Интернета, прохождение трафика, которых разрешено. Например, чтобы обеспечить прохождение web страниц из Интернета на компьютер, необходимо включить службу «Веб-сервер HTTP».*

5. Отметьте все службы.
6. Выберите закладку Ведение журнала безопасности (рис. 5).

Примечание: *Для брандмауэра подключение к Интернету предусмотрен журнал безопасности для записи событий, связанных с его работой. Журнал безопасности ICF поддерживает следующие возможности.*

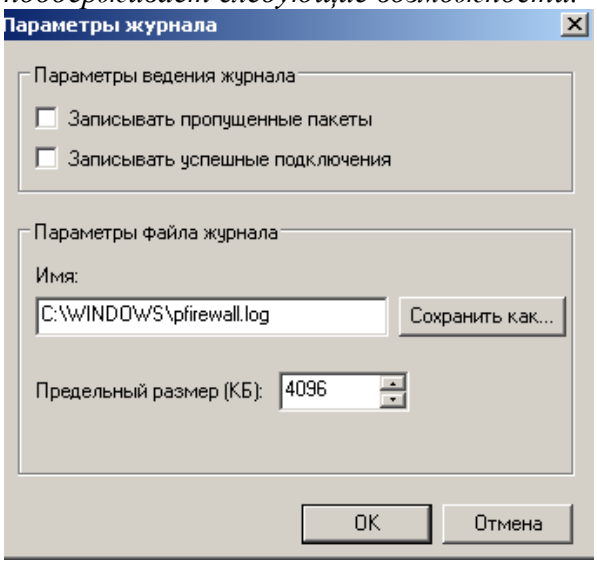


Рис. 5

Запись пропущенных пакетов. Этот параметр задает запись в журнал сведений обо всех потерянных пакетах, исходящих из сети (компьютера) или из Интернета. Если установить флажок **Записывать пропущенные пакеты,** будут собираться сведения о каждом пакете, который пытается пройти через ICF, но был обнаружен и отвергнут брандмауэром.

Запись успешных подключений. Этот параметр задает запись в журнал сведений обо всех успешных подключениях, инициированных из сети (компьютера) или из Интернета.

7. Отметьте пункты **Записывать пропущенные пакеты и Записывать успешные подключения.** Обратите внимание на местоположение журнала безопасности.

Примечание: *Журнал безопасности брандмауэра состоит из двух разделов. В заголовке журнала содержатся сведения о версии журнала и полях, в которые можно записывать данные. Содержимое заголовка имеет вид статического списка. Содержимое журнала безопасности представляет собой откомпилированные данные, которые вводятся при обнаружении трафика, пытающегося пройти через брандмауэр. Поля журнала заполняются слева на право, как они расположены на странице. Для того чтобы в журнал вводились данные, необходимо выбрать хотя бы один параметр ведения журнала или оба параметра.*

8. Теперь Ваш брандмауэр настроен и готов к защите Вашего компьютера от внешних угроз.

Задание для самостоятельной работы:

1. Настройте брандмауэр для работы с Веб - сервером (HTTP), FTP-сервером и зафиксируйте соответствующее окно для отчета.
2. Включите журнал безопасности.
3. После выполнения задания 1 и 2 подключитесь и просмотрите какой либо ресурс на внутреннем FTP-сервере.
4. Завершите работу и просмотрите журнал безопасности.
5. Зафиксируйте записи журнала безопасности для отчета.

Контрольные вопросы:

1. Что такое брандмауэр?
2. Какие бывают брандмауэры?
3. Что фиксирует журнал безопасности брандмауэра?

Лабораторная работа
VPN-подключения средствами ОС Windows XP.

Цель работы: Научится создавать VPN- подключения средствами ОС Windows XP и выполнять его настройку.

Краткие теоретические сведения:

Технология виртуальных частных сетей (VPN-Virtual Private Network) является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях.

Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности: шифрования, экранирования и туннелирования.

Задание: Создать VPN подключение и выполнить его настройку.

Алгоритм выполнения работы:

Создание VPN подключения.

1. Откройте компонент Сетевые подключения.
2. Для этого выберите последовательно **Пуск-Панель управления - Сетевые подключения.**
3. Выберите пункт **Создание нового подключения** и нажмите кнопку **Далее.**
4. В открывшемся окне выберите пункт **Подключит к сети на рабочем месте** (используя удаленный доступ или VPN) рис. 1 и нажмите кнопку **Далее**. После этого выберите **Подключение к виртуальной частной сети** (рис. 2) и нажмите **Далее.**

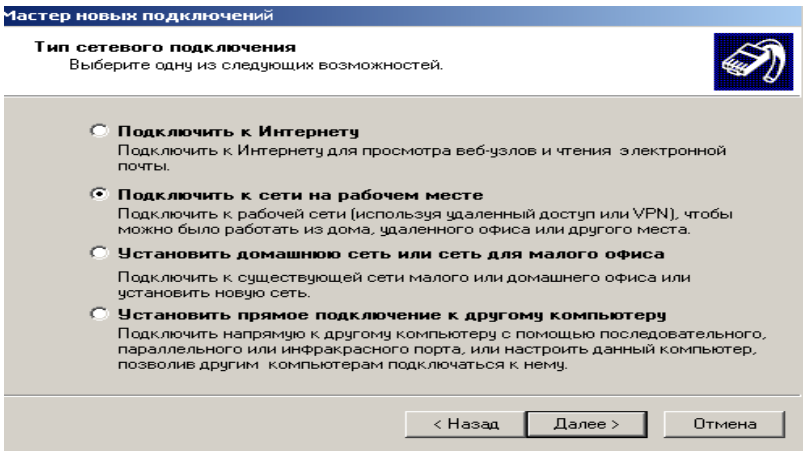


Рис. 1

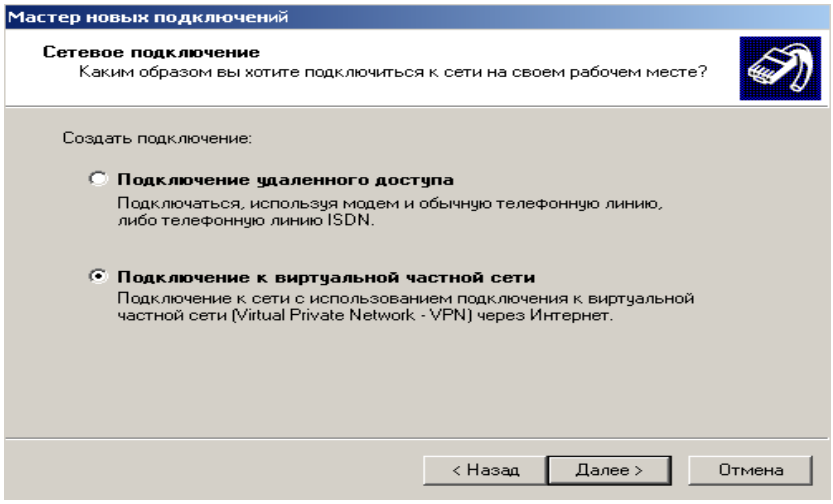


Рис. 2

5. Введите имя подключения и перейдите к следующему шагу командой **Далее.**
6. Если перед установкой «туннельного доступа» требуется подключение к провайдеру услуг Интернета, то выберите (рис. 3) **Набрать номер для следующего предварительного подключения** и, выбрав нужное подключение, нажмите **Далее.** В противном случае выберите **Не набирать номер для предварительного подключения** и нажмите **Далее.**
7. Введите имя узла (сети) или его IP-адрес, к которому идёт подключение.
8. Завершите работу **Мастера подключений**.
9. В результате в папке Подключения появится новое подключение (рис. 4).
10. Для настройки параметров подключения выделите **подключение VPN**

И вызовите его свойства из контекстного меню (нажатие правой клавиши мыши).

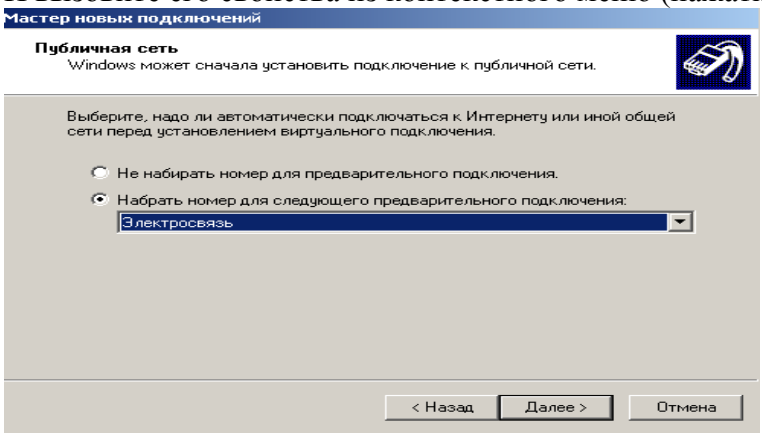


Рис. 3

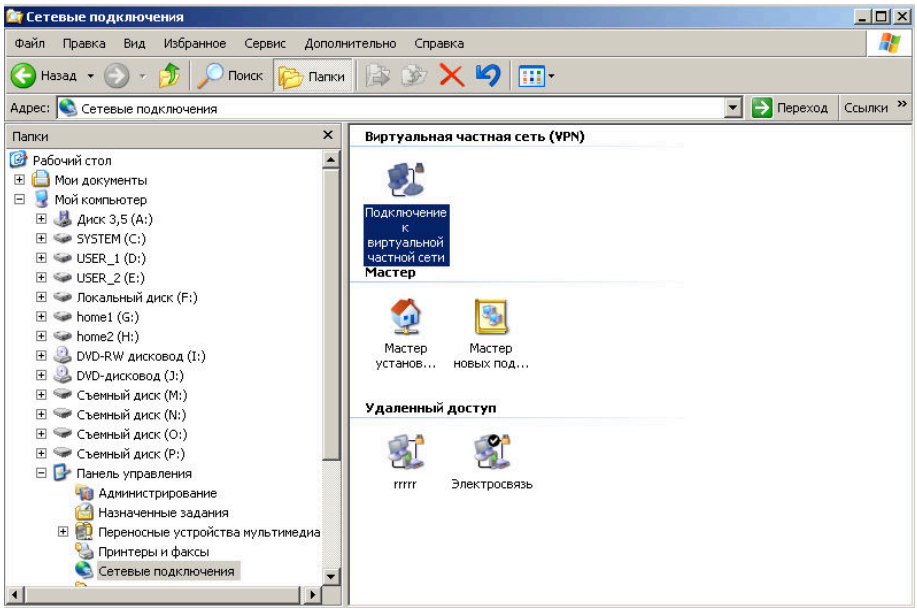


Рис. 4

11. Рассмотрим все имеющиеся параметры VPN подключения (рис. 5) и при необходимости воспользуйтесь соответствующими разделами справки.

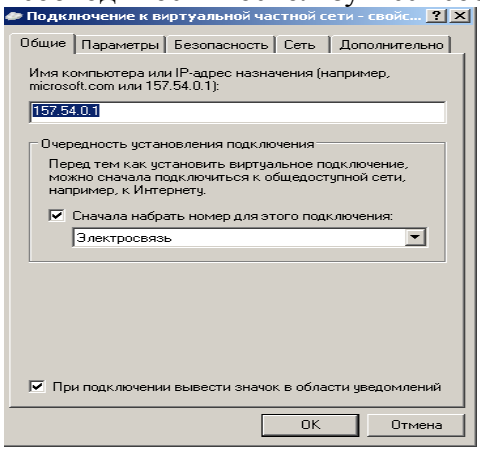


Рис. 5

Задание для самостоятельной работы:

Создайте VPN подключение к узлу с адресом 122.122.122.122 и зафиксируйте окно его свойств (Print Screen) на закладке **Общие** (как показано на рис. 5) в качестве отчета.

Контрольные вопросы:

1. Какие механизмы безопасности используются при реализации VPN подключения?
2. Что такое «туннель» и в чем состоит принцип «туннелирования»?
3. В чем заключаются защитные функции виртуальных частных сетей?

Лабораторная работа

Тема: Использование инструментов для создания карты Интернета

Цель занятия: Научиться запускать сервисную программу tracert, отслеживающую маршрут следования данных от локального компьютера к веб-сайту, находящемуся на другом континенте; научиться строить схему маршрута

Краткие теоретические сведения и справочно-информационные материалы по теме занятия.

В этой лабораторной работе для определения маршрута прохождения данных по Интернету от вашего ISP к другим ISP будет использоваться сервисная программа Windows — tracert, и это позволит понять, каким образом обеспечивается мировой доступ к сети Интернет. Также, на схему будут нанесены связи со следующими основными региональными регистрирующими организациями (RIR).

Преподаватель, однако, может предлагать сайты, находящиеся в других регионах.

AfriNIC (African Network Information Centre) — Африканский регион

APNIC (Asia Pacific Network Information Centre) — Азиатско-тихоокеанский регион

ARIN (American Registry for Internet Numbers) — Североамериканский регион

LACNIC (Regional Latin-American and Caribbean IP Address Registry) — Латинская Америка и некоторые Карибские острова

RIPE NCC (R?seaux IP Europ?ens) — Европа, Ближний Восток и Центральная Азия

Необходимо использовать следующие ресурсы:

узловой компьютер с операционной системой Windows; доступ к командной строке;

подключение к Интернету;

таблицу для трассировки маршрутов для каждого URL назначения. Таблица для трассировки маршрутов прилагается к данной лабораторной работе. Каждый учащийся заполняет свою таблицу для трассировки маршрутов, затем сдает ее преподавателю;

карту мира с подключениями, которая прилагается к данной лабораторной работе; доступ к командной строке ПК.

Шаг 1. Запуск сервисной программы tracert с узлового компьютера

а. Убедитесь, что узловой компьютер подключен к Интернету.

б. Откройте окно командной строки: Пуск > Выполнить, в появившемся окне введите cmd.

Окно командной строки можно открыть также следующим образом: Пуск > Все программы > Стандартные > Командная строка.

в. В командной строке введите команду tracert и название первого веб-сайта назначения.

Выходные данные команды будут выглядеть так, как показано ниже:

г. Сохраните выходные данные команды tracert в текстовом файле следующим образом.

1) Щелкните правой кнопкой мыши в строке заголовка окна командной строки и выберите

Изменить > Выделить все.

2) Еще раз щелкните правой кнопкой мыши на строке заголовка окна командной строки и выберите Изменить > Копировать;

3) Откройте приложение Блокнот: Пуск > Программы > Стандартные > Блокнот.

4) Для вставки выходных данных в приложение Блокнот выберите Правка > Вставить.

5) Выберите Файл > Сохранить как и сохраните файл с помощью программы Блокнот на рабочем столе под названием tracert1.txt.

д. Выполните команду tracert для каждого веб-сайта назначения и сохраните выходные данные в новых файлах, пронумерованных в последовательном порядке.

е. Выполните команду tracert на компьютерах, подключенных к различным компьютерным сетям, например, на компьютере публичной библиотеки или на компьютере друга, которые

подключены к Интернету через различных поставщиков услуг Интернета (например, кабельная сеть вместо DSL). Сохраните выходные данные в файле программы Блокнот и распечатайте для дальнейшего использования.

Шаг 2. Анализ выходных данных команды tracert и определение подключений ISP

Маршруты могут проходить через многие узлы и через различное количество ISP в зависимости от размера сети вашего поставщика, местонахождения вашего узла и местонахождения узла назначения. Например, как видно из выходных данных, показанных на рисунке, пакеты данных

идут от компьютера-источника к локальному шлюзу по умолчанию, в качестве которого выступает маршрутизатор, затем в точку присутствия (POP) ISP, а потом поступают к точке обмена интернет- трафиком (IXP). Затем они проходят через два маршрутизатора ISP второго уровня, а потом через несколько маршрутизаторов ISP первого уровня. Когда они покидают магистраль ISP первого уровня, они снова проходят через ISP второго уровня по пути к серверу назначения www.ripe.net.

а. Откройте первый файл с выходными данными команды traceroute и ответьте на следующие вопросы.

1) Какой IP-адрес у вашего локального маршрутизатора POP?

2) Сколько переходов делает пакет по пути от узлового компьютера к серверу назначения?

3) Сколько различных ISP проходит отслеживаемый пакет по пути от узлового компьютера до сервера назначения?

4) Перечислите IP-адреса и URL-адреса всех устройств, указанных в выходных данных команды tracert в порядке их появления в таблице трассировки маршрутов.

5) В столбце «Владелец сети» таблицы для трассировки маршрутов укажите, какому ISPкакой маршрутизатор принадлежит. Если маршрутизатор принадлежит вашей локальной сети, пишите «LAN». Последние две части URL показывают название ISP. Например, если

URL-адрес содержит «sprint.net», то это значит, что маршрутизатор принадлежит сети ISP с названием «Sprint».

Ответы будут отличаться.

6) Проходил ли маршрут через неопознанный маршрутизатор, расположенный между сетями двух ISP? Это могла быть IXP-точка. Выполните команду whois сервисной программы

или функцию whois программы визуализации трассировки маршрута для определения владельца этого маршрутизатора. Либо посетите веб-сайт http://www.arin.net/whois, чтобы определить, на кого зарегистрирован данный IP-адрес.

б. Заполните таблицу трассировки маршрутов, используя файлы с выходными данными всех URL назначения.

в. Сравните результаты из разных файлов с выходными данными команды tracert. Подключался ли ваш ISP к другим ISP для передачи данных в разные пункты назначения?

г. Если вы выполняли команду tracert в другой сети, проанализируйте также выходные данные в файле для этой сети. Отличалось ли число переходов, которые пакеты должны пройти на пути к тому же месту назначения от сети другого местного ISP? У какого ISP число переходов до места назначения было меньше?

Шаг 3. Построение схемы подключений локального поставщика услуг Интернета

а. Для каждых выходных данных на отдельном листе бумаги нарисуйте схему, в которой покажите, как ваш ISP соединяется с другими, чтобы достичь URL-адреса назначения. Учтите следующее:

1) Покажите все устройства, начиная с вашей сети и заканчивая маршрутизатором URL назначения. Укажите на всех задействованных устройствах их IP-адреса.

2) Обведите локальный POP-маршрутизатор рамкой и обозначьте его словом «POP».

3) Нарисуйте облака ISP, охватывающие все маршрутизаторы каждого соответствующего ISP, и подпишите облака названиями соответствующих ISP.

4) Обведите рамкой все маршрутизаторы точек обмена интернет-трафиком и обозначьте их словом «IXP».

б. Нанесите на карту мира с подключениями только облака ISP и рамки, обозначающие точки обмена интернет-трафиком.

Таблица трассировки маршрутов

Общее количество переходов:

URL назначения:

IP-адрес маршрутизатора

URL маршрутизатора (если имеется)

Владелец сети (LAN, название ISP или IXP)

Карта мира с подключениями

Лабораторная работа

Тема: Оценка плана обновления кабельной системы

Цель занятия: Научиться оценивать план обновления кабельной системы

Краткие теоретические сведения и справочно-информационные материалы по теме занятия.

В дополнение к ранее имевшейся площади на втором этаже офисного здания компания среднего размера недавно приобрела остальную часть второго этажа. Вас попросили изучить существующий поэтажный план и помочь с размещением промежуточного распределительного узла, прокладкой кабеля на новой площади, и определить потребность для этого каких-либо новых устройств.

Эта лабораторная работа может выполняться как индивидуально, так и в группах. Необходимо использовать следующие ресурсы:

поэтажный план здания, предоставляемый клиентом (прилагается).

Шаг 1. Изучение поэтажного плана клиента.

а. Отметьте на плане следующие элементы:

1) точку присутствия (POP);

2) главный распределительный отсек (MDF);

3) промежуточный распределительный отсек (IDF);

4) вертикальные/магистральные кабельные системы;

5) горизонтальные кабельные системы:

б. Кабель какого типа используется в вертикальных/магистральных кабельных системах?

Поясните свой ответ.

Шаг 2. Оценка плана для нового места.

Компания «AnyCompany» недавно приняла на работу небольшую группу веб-дизайнеров и полностью заняла весь второй этаж, чтобы расположить новую группу. Новая площадь показана на правой стороне плана. Было решено для поддержки новых рабочих станций разместить на новой площади второй IDF.

а. Предложите возможное место для нового IDF. Какую комнату/место вы выбрали? Поясните свой ответ.

б.Какой тип кабеля вы предложите для соединения нового IDF с существующим MDF при помощи вертикальных кабельных систем? Поясните свой ответ.

в. На новой площади в основном будут расположены офисы. Допустим, в каждом офисе будет по 2 информационные розетки. Также запланируйте 2 информационные розетки в аудитории, чтобы обеспечить выход в Интернет для презентаций и учебных занятий. Сколько дополнительных информационных розеток необходимо заказать?

г. Вас попросили определить количество необходимых 24-портовых коммутаторов для нового IDF. Не забудьте учесть 25%-ный прирост. Сколько коммутаторов нужно купить данной компании?

д. Сколько горизонтальных кабельных систем будет подключено к коммуникационной панели нового IDF?

Шаг 3. Изучение поэтажного плана и плана прокладки кабелей.

а. Какое оборудование, кроме коммутаторов, вы собираетесь использовать в новом IDF?

б. Какое оборудование, кроме коммутаторов, вы собираетесь использовать в MDF?

в. Возможно ли использовать кабель UTP для подключения устройств в комнате 2.20 или 2.30 непосредственно к коммутатору MDF при данной прокладке кабеля?

Шаг 4. Вопросы для обсуждения

С одним или двумя другими учащимися обсудите следующее:

а. Что является более приемлемым на новой площади: использование IDF или горизонтальной кабельной системы, проложенной от каждого устройства к MDF?

б. Сколько понадобится кабелей от MDF к IDF, чтобы обеспечить работу коммутаторов? Поясните свой ответ.

Лабораторная работа
Тема: Настройка сетевых устройств средствами Linux

Цель занятия: Научиться настраивать сетевые устройства средствами Linux

Краткие теоретические сведения и справочно-информационные материалы по теме занятия.

TCP/IP

Стандартной отправной точкой для изучения стека TCP/IP является общепризнанная модель OSI (Open System Interconnection), определившая семь уровней.

* Прикладной уровень (application layer). На этом уровне осуществляется взаимодействие пользователя с программным обеспечением.

* Уровень представления (presentation layer). Здесь осуществляются преобразования данных, необходимые для предоставления информации, пере- даваемой программами нижележащих уровней, в требуемом для приклад ного уровня виде.

* Сеансовый уровень (session layer). На этом уровне работают программы, обеспечивающие аутентификацию, вход и выход из сеанса.

* Транспортный уровень (transport layer). Программы этого уровня обеспечивают прием/передачу данных с заданной надежностью.

* Сетевой уровень (network layer). Этот уровень определяет адреса сетей и узлов в сети, а также определяет передачи данных между сетями.

* Канальный уровень (data link). На этом уровне обеспечивается передача информации как форматированного потока битов.

* Физический уровень (physical layer) — самый нижний уровень сетевого взаимодействия, обеспечивающий передачу потока битов посредством сетевого

аппаратного обеспечения и физического носителя, связывающего вычислительные системы.

Если отобразить стек протоколов TCP/IP на модель OSI, то окажется, что в нем реализованы лишь четыре уровня сетевого взаимодействия.

* Прикладной. Этот уровень в TCP/IP представлен прикладными протоколами, например: HTTP, FTP, SMTP, POP3 и т. д. С помощью этих протоколов обеспечивается функционирование прикладного программного обеспечения.

* Транспортный. В TCP/IP имеются два транспортных протокола: надежный и ориентированный на соединение протокол TCP (Transmission Con- trol Protocol) и более быстрый, но не надежный, протокол UDP (User Data- gram Protocol).

* Сетевой. Данный уровень представлен протоколом IP (Internet Protocol).

Этот протокол обеспечивает передачу пакетов между узлами и сетями.

* Канальный уровень. Он представлен в TCP/IP протоколами адресации физических устройств, такими, как ARP (Address Resolution Protocol).

Достоинством вертикально структурированных стеков протоколов является то, что при реализации программ для конкретного уровня не требуется учитывать детали реализации программ, принадлежащих другим уровням.

Данные, сформированные программой прикладного уровня, разбиваются на пакеты, которые упаковываются в пакеты нижележащего уровня (инкапсуляция). При приеме этих упакованных пакетов происходит обратный процесс: принятые пакеты распаковываются и извлекаются из более пакетов нижележащего уровня (декапсуляция).

Существуют документы, описывающие функционирование стека протоколов TCP/IP, Интернета и стандартных сетевых служб. Эти документы называются RFC (Request For Comments). Список RFC размещен на сайте IETF (Internet Engineering Task Force) www.ietf.org, www.rfc.net или www.rfc-editor.org.

Список разнообразных протоколов находится в файле /etc/protocols (пример 1).

```
$ sed -n '10,20p' /etc/protocols
ip0IP# internet protocol, pseudo protocol numbericmp
...1ICMP#  internet control message protocol
```

1. Задание

1.1. К какому уровню стека TCP/IP следует отнести протокол IMAP, позволяющий управлять удаленным почтовым ящиком и читать в нем почту?

1.2. Какой транспортный протокол следует предпочесть для передачи TV-трансляции посредством Интернета (например, на стадии проектирования специализированной программы для TV-трансляции)?

1.3. К какому уровню модели OSI можно было бы отнести протокол ICMP (Internet Control Message Protocol)? Он, в частности, позволяет проверить работоспособность и правильность настроек сетевого оборудования.

2. Задание

2.1. К какому классу принадлежит IP-адрес 63.127.33.254?

2.2. Какой широковещательный адрес у этой сети?

2.3. Какая маска у этой сети?

2.4. Запишите указанный выше адрес в шестнадцатеричном формате.

3. Задание

3.1. Выполните команду /sbin/ifconfig. Имеется ли автоматически сконфигурированный адрес IPv6?

3.2. Проверьте соответствие MAC-адреса и IPv6-адреса (MAC-адрес — HWaddr).

4. Задание

4.1. Получите статистику по приему/передаче пакетов.

4.2. Как командой ifconfig можно отключить сетевой интерфейс?

4.3. Остановите сетевой интерфейс и попробуйте выполнить команду ping, направляя пакеты на остановленный интерфейс. Что при этом происходит?

4.4. Какая опция ping позволяет посылать ICMP-пакеты потоком без задержки?

5. Задание

5.1. Установите заведомо неверный адрес маршрутизатора по умолчанию.

5.2. Попробуйте выполнить команду ping, указав в качестве аргумента правильный адрес маршрутизатора. Попробуйте также выполнить предыдущую команду с любым существующим IP-адресом узла сети, находящегося вне вашей сети.

5.3. Измените адрес маршрутизатора по умолчанию на правильный и снова выполните команду ping с адресом любого реального узла вне вашей сети.

5.4. Выполните команду traceroute с этим же адресом.

Лабораторная работа
Тема: Настройка сервисов в сети ОС Linux

Цель занятия: Научиться настраивать сервисы сети интернет в ОС Linux

Краткие теоретические сведения и справочно-информационные материалы по теме занятия.

Идентификация служб сети

Процесс взаимодействия программ в сети проходит в соответствии с требованиями протокола прикладного уровня (Application Layer). В TCP/IP для идентификации служб, которые могут быть запущены на каком-либо узле сети, ис- пользуются номера портов в диапазоне от 0 до 65 535 (шестнадцать битов). Номера портов назначаются IANA (Internet Assigned Numbers Authority).

Многие номера портов, меньшие 1024 и некоторые большие, закреплены за определенными службами сети (Well Known Services). Вот список некоторых:

20 — данные, передаваемые сервисом FTP;
21 — управляющая информация для сервиса FTP;
22 — протокол SSH;
25 — транспортный почтовый протокол SMTP;
23 — удаленный доступ с помощью Telnet;
53 — протокол DNS;
80 — протокол HTTP;
110 — доставка почты по протоколу POP3;
119 — служба доставки новостей NNTP;
139 — протокол NetBIOS;
143 — удаленный доступ к почтовым ящикам по протоколу IMAP;
161 — протокол управления сетью SNMP;
389 — протокол доступа к службам каталогов LDAP.

Список имен служб находится в файле /etc/services (пример 1).

ftp-data 20/tcp ftp 21/tcp fsp 21/udp fspd ssh 22/tcp # SSH Remote Login Protocol ssh 22/udp telnet 23/tcp smtp 25/tcp mail

Службы, номера портов которых меньше 1024, называются привилегированными. Серверные приложения, открывающие данные порты, могут быть запущены лишь суперпользователем. В противоположность привилегированным портам порты с номерами от 1024 до 65 535 называют эфемерными, поскольку большинство из них не закреплено за какими-либо службами сети и используются клиентскими приложениями для связи с серверами.

Для связи между двумя сетевыми приложениями каждое из них должно открыть сокет (socket). Список активных соединений выводит команда netstat.

Если необходимо получить список не только установленных соединений, но и перечень портов, открытых для соединения, то можно использовать опцию -a команды netstat. Ограничить вводимую информацию лишь TCP- или UDP-портами можно, используя опции, соответственно, -t или -u.

Этот пример показывает, что на данном компьютере открыт порт для соединений по протоколу SSH (Secure Shell).

Для открытых портов в поле статуса установлен идентификатор LISTEN. Если соединение установлено, то в поле статуса будет ESTABLISHED.

Обратите внимание, что на клиентском компьютере (в данном случае — ssh) открыт сокет, использующий порт 32 771. Через этот сокет производится обмен информацией с сокетом 22/tcp (служба ssh) на компьютере, где запущен сервер sshd.

Для вывода информации в числовом виде предназначена опция -n команды

netstat.

Открытые, но не используемые порты, представляют собой брешь в системе безопасности, поскольку каждый прослушиваемый порт представляет собой потенциальную цель атаки.

1. Задание

1.1. Для какой службы используется порт 8080 TCP?

1.2. Выполните команду netstat -a. В каком порядке выводится информация об открытых портах в системе?

1.3. Имеются ли какие-либо открытые сокеты в подкаталогах /tmp? Используйте для определения этого команду netstat без аргументов.

1.4. Получите информацию об открытых портах UDP.

1.5. Как получить PID процессов, открывших эти порты (см. опцию –p команды netstat)?

2. Задание

2.1. Определите, используется ли в вашей системе супердемон inetd.

2.2. При использовании в системе inetd активизируйте службу telnet.

3. Задание

3.1. Запретите с помощью /etc/hosts.deny доступ отовсюду ко всем службам, кроме telnet, доступ к которому должен быть разрешен в /etc/hosts.allow. Проверьте конфигурацию с помощью tcpdchk.

3.2. Сделайте это же исключительно с помощью файла /etc/hosts.deny.

3.3. Как запретить доступ к telnet с узлов, имена которых не могут быть получены с помощью обратного преобразования IP-адреса в имя хоста посред- ством DNS?

3.4. Проверьте командой tcpdmatch последовательность фильтрации.

4. Задание

4.1. С помощью xinetd разрешите доступ к echo-udp из вашей локальной сети.

4.2. Настройте разрешение на доступ к этой службе с 9:00 до 10:30.

4.3. Как с помощью xinetd перенаправить обращение службе на другой узел сети? Подсказка: изучите директиву redirect файла конфигурации

4.4. /etc/xinetd.conf.

4.5. Необходимо запустить службу telnet не на порту 23, а на порту 2323. Как это сделать? Подсказка: изучите примеры man xinetd.conf.

Лабораторная работа

Тема: Настройка служб удаленного доступа в ОС Linux

Цель занятия: Научиться получать терминальный доступ к удаленной системе

Краткие теоретические сведения и справочно-информационные материалы по теме занятия.

Служба telnet

Служба telnet позволяет открывать сеанс на удаленном компьютере. Клиентская часть этой службы представлена программой telnet, а серверная – in.telnetd. Сервер telnet по умолчанию прослушивает 23-й порт TCP и за- пускается супердемоном.

В примере 1 приведен файл конфигурации службы telnet для супердемона xinetd.

```
service telnet
{
socket_type    = stream
wait    = no
user    = root
server  = /usr/sbin/in.telnetd log_on_success += DURATION USERID log_on_failure += USERID
disable = yes
}
```

В большинстве дистрибутивов служба telnet по умолчанию не активна (на- стройка disable = yes), поэтому для ее запуска следует активизировать (disable = no) и послать сигнал SIGHUP супердемону.

Для входа в сеанс на удаленной машине с помощью telnet необходимо выполнить команду telnet, указав имя или адрес удаленной машины (пример 2).

```
$ telnet note.class.edu Trying 192.168.11.25...
Connected to note.class.edu. Escape character is '^]'.
Connection closed by foreign host.
```

В данном примере сеанс связи с сервером telnet был закрыт, о чем было получено сообщение "Connection closed by foreign host". В данном случае это вызвано настройкой only_from = 127.0.0.1 в файле конфигурации xinetd (пример 3).

```
service telnet
{
...
only_from      = 192.168.11.0/25
disable = no
}

$ telnet note.class.edu Trying 192.168.11.25...
Connected to note.class.edu. Escape character is '^]'.
Welcome! (note.class.edu) note.class.edu login: apox Password:
Last login: Wed Jun 30 22:34:19 on :0
```

В примере 3 явно разрешено устанавливать соединения со службой telnet, запущенной на данном узле с любых узлов сети 192.168.11.0/25.

Сервер telnet вывел строку сообщения из файла /etc/issue.net – "Welcome! (note.class.edu)" и приглашение ввести имя пользователя и пароль для аутентификации пользователя. После успешной аутентификации был запущен удаленный сеанс. В нем можно выполнять любые разрешенные для данного пользователя команды на удаленном компьютере.

При необходимости можно временно выйти из терминального режима работы клиента telnet в командный (пример 4). Для этого следует ввести escape-последовательность, указанную при запуске сеанса: <Ctrl>+<]>.

```
apox@note apox $
```

<Cntl>+<]>
telnet> help
Commands may be abbreviated. Commands are: close close current connection
logout forcibly logout remote user and close the connection display display operating parameters
mode try to enter line or character mode ('mode ?' for more) open connect to a site
quit exit telnet
send transmit special characters ('send ?' for more) set set operating parameters ('set ?' for more) unset unset operating parameters ('unset ?' for more) status print status information
toggle toggle operating parameters ('toggle ?' for more) slc change state of special charaters ('slc ?' for more) z suspend telnet
! invoke a subshell
environ change environment variables ('environ ?' for more)
? print help information telnet> quit
Connection closed.

Для выхода из удаленного сеанса можно либо воспользоваться обычными средствами завершения работы в оболочке (например, exit), либо ввести команду quit.

В силу того, что использование telnet не предусматривает никаких средств криптографической защиты средствами самого протокола telnet, то настоятельно рекомендуется не использовать telnet для связи в сетях, не являющихся доверенными. Вместо этой службы следует использовать SSH (Secure Shell).

Клиентская часть службы telnet, тем не менее, исключительно удобна для тестирования разнообразных служб, работающих с собственными протоколами. Далее приведен пример проверки возможности связаться с сервером SSH, работающим с 22-м портом TCP (пример 5).

$ telnet note.class.edu 22 Trying 192.168.11.25...
Connected to note.class.edu. Escape character is '^]'.
SSH-1.99-OpenSSH_3.7.1p2
^]
telnet> quit Connection closed.

В примере 5 продемонстрировано, что клиент telnet способен устанавливать соединение по порту, указанному в командной строке. Здесь указан порт 22 – SSH.

1. Задание

1.1. Установите и запустите сервер telnet. Настройте супердемон так, чтобы соединения с вашей машиной могли быть установлены из вашей сети.

1.2. Подключитесь с помощью telnet к SMTP-серверу на вашей машине (порт 25 TCP).

2. Задание

2.1. Сконфигурируйте xinetd для активизации r-служб.

2.2. Настройте доверительный вход и проверьте работоспособность r-команд.

2.3. Влияет ли наличие файла .rhosts на поведение команды rexec?

2.4. Какая опция rcp позволяет копировать файлы рекурсивно?

3. Задание

3.1. Запустите службу SSH.

3.2. Проверьте работоспособность команд ssh и scp.

3.3. Создайте пару ключей RSA и поместите публичный ключ на желаемый сервер. Оставьте парольную фразу пустой – в таком случае при успешном обмене ключами вводить пароль для доступа к удаленному узлу не потребуется.

Лабораторная работа

Тема: Настройка службы FTP, сервера Samba в ОС Linux

Цель занятия: Научиться настраивать службу FTP, сервер Samba в ОС Linux

Краткие теоретические сведения и справочно-информационные материалы по теме занятия.

Как работает служба FTP

Служба FTP реализует одноименный протокол для передачи файлов с одного узла сети на другой (FTP – File Transfer Protocol). Сервер FTP позволяет по запросу клиента FTP передавать требуемые файлы на клиентский узел.

При запуске FTP-сервера он открывает порт TCP 21, предназначенный для инициации FTP-соединения и передачи управляющей информации. При инициации клиентом FTP-соединения происходит аутентификация пользователя, при успешном прохождении которой запускается сеанс FTP. После этого пользователь получает возможность копирования файлов между удаленным и локальным компьютерами. Передача данных производится в отдельном TCP-соединении по порту 20.

Таким образом, при работе службы FTP открываются сразу два TCP-соединения:

* первое инициируется клиентским узлом с порта источника с номером выше 1024 (обычно более 30 000) и портом назначения 21 на серверной стороне; это соединение используется для передачи управляющей информации;

* второе инициируется серверным узлом для обмена данными, использующим 20-й порт источника на серверном узле и порт назначения с номером выше 1024 на клиентском узле; причем клиент предварительно информирует сервер о номере открытого для передачи данных порта.

Данная схема описывает работу активного FTP-соединения, вызывающего трудности при организации работы IP-фильтра, поскольку порт назначения

для передачи данных на клиентской машине заранее неизвестен. Для обхода описанной проблемы используется пассивный режим FTP. В этом случае соединение для передачи данных инициируется не сервером с порта 20 TCP, а клиентом с порта выше 1024 на порт сервера с номером выше 1023. Номер порта на сервере для передачи данных заранее сообщается клиенту.

В настоящее время в GNU/Linux используется множество различных программ, реализующих FTP-серверы. Среди них: BSD ftpd, wuftpd, proftpd и vsftpd. Большинство из них может работать как в самостоятельном режиме (stand-alone), так и с помощью супердемона. Имеется также множество реализаций FTP-клиентов. Наиболее популярны: ftp, lftp, nftp и wget.

Часто серверы FTP предоставляют возможность анонимного использования. Для этих целей используются специальные имена анонимных пользователей: anonymous или ftp. При анонимном доступе к FTP-серверу вместо пароля вводят почтовый адрес или вообще ничего. Большинство анонимных FTP- серверов сконфигурировано только для копирования данных с них (download), но имеются и поддерживающие загрузку файлов на них (upload). В последнем случае следует предпринимать особые меры предосторожности, т. к. анонимный сервер с возможностью загрузки файлов на него – отличная цель для атак и иной незаконной деятельности.

По историческим причинам протокол FTP различает два режима передачи файлов: текстовый (ascii) и бинарный (binary). Передача бинарного файла в текстовом режиме приведет к искажению передаваемой информации.

Состав пакета SAMBA

Пакет SAMBA представляет собой набор программ, реализующий сервер SMB/CIFS (Server Message Block) в UNIX/Linux-системах. Протокол SMB и его дальнейшее развитие – CIFS (Common Internet File System) являются наследниками протокола NetBIOS, разработанного в IBM. Эти протоколы лежат в основе функциональности сетей MS Windows, поэтому пакет SAMBA обеспечивает возможности интеграции GNU/Linux-систем в Windows-сети.

Используя SAMBA, работающая с GNU/Linux система способна использовать и предоставлять ресурсы для Windows-сети. В настоящий момент реализованы два вида разделяемых в сети Windows ресурсов: файловые ресурсы и разделяемые принтеры.

В распространенных дистрибутивах GNU/Linux пакет SAMBA разделен на несколько пакетов: samba, samba-server, samba-client и т. д. Важнейшие программы SAMBA 3.4.x:

* smbd – сервер SMB/CIFS;
* nmbd – сервер разрешения NetBIOS-имен;
* smbclient – клиентская программа для обращения к ресурсам сети;
* testparm – утилита, для проверки правильности конфигурации SAMBA;
* smbstatus – программа, выводящая статус SAMBA;
* nmblookup – утилита, позволяющая проверять разрешение имен NetBIOS;
* smbpasswd – команда для установки и изменения паролей пользователей;
* mount.cifs – команда монтирования сетевых файловых ресурсов SMB/CIFS;
* smbtar – сценарий для архивирования файловых ресурсов;
* winbindd – демон, позволяющий получать информацию от серверов Windows;
* wbinfo – программа, позволяющая запрашивать информацию от winbindd;
* findsmb – скрипт Perl для получения списка SMB-машин в сети;
* smbcontrol – посылает сигналы демонам smbd и nmbd;
* smbspool – посылает задания на печать на SMB-сервер печати;
* pdbedit – программа для управления SAMBA-пользователями;
* swat – программа для настройки и управления SAMBA с Web-интерфейсом.

1. Задание

1.1. Определите, какие программы FTP установлены в вашей системе.

1.2. Какие конфигурационные файлы используются сервером FTP в вашей системе?

1.3. Поддерживают ли имеющиеся клиенты FTP пассивный режим?

2. Задание

2.1. Настройте vsftpd для разрешения реальным пользователям входить в сеанс с возможностью загружать файлы на сервер.

3. Задание

3.1. Получите свежую версию wget, используя саму команду wget.

4. Задание

4.1. Определите версию SAMBA, установленную в вашей системе.

4.2. Проверьте, установлена ли программа mount.cifs. Из какого пакета?

5. Задание

5.1. Какая настройка security требуется в системе, которая должна предоставлять общедоступный гостевой файловый ресурс на запись без пароля?

5.2. Создайте файл настроек для такого доступа и проверьте его правильность.

5.3. Предположим, что в примере 25.1 требуется разрешить доступ к ресурсу BUX группе users. Как это сделать?

Лабораторная работа

Тема: Настройка DNS и DHCP в ОС Linux

Цель занятия: Научиться настраивать протокол DNS и DHCP в ОС Linux

Краткие теоретические сведения и справочно-информационные материалы по теме занятия.

Организация DNS

Аббревиатура DNS расшифровывается как служба доменных имен (Domain Name Service). Она пришла на смену файлу, устанавливающему соответствия имен компьютеров их адресам, который использовался на заре ARPANET (сейчас он называется /etc/hosts). DNS во многом решила проблему конфликтов имен. Конфликт возникает в случае, когда узлы с разными адресами претендуют на одно и то же имя в сети.

В системе DNS все пространство имен разбито на домены, имена узлов в которых должны быть уникальны. В то же время в разных доменах могут использоваться одинаковые имена узлов. Имена www.bamboo.be и www.bamboo.de различны, т. к. находятся в разных доменах – bamboo.be и bamboo.de.

Сервер DNS BIND (Berkeley Internet Name Daemon) является де-факто стандартным сервером DNS в Интернете. Он предоставляет требуемую инфраструктуру для организации иерархической распределенной базы данных DNS, хранящей информацию о соответствии имен хостов их IP-адресам. База данных DNS является распределенной, поскольку информация о различных доменах может находиться на разных серверах DNS. Нет ни одного сервера DNS, который бы имел полную информацию о соответствии всех имен компьютеров в сети их адресам. Пространство имен в DNS организовано в виде дерева, корень которого имеет имя "точка" (.). Этот домен (точка) содержит поддомены, называемые доменами верхнего уровня (TLDs, Top Level Domains). Они условно подразделяются на три типа:

* исходные (generic) – com, gov, mil, edu, net, org, int;
* территориальные (geographic) – ru, su, be, uk и т. д.;
* дополнительные, например – biz, news и info.

Корневые домены содержат поддомены, называемые доменами второго уровня. Так, например, class.edu – это домен второго уровня, являющийся поддоменом корневого домена edu. В доменах второго уровня также могут быть созданы поддомены. Так, может быть создан поддомен tjumen.class.edu.

Множество имен компьютеров, входящих в домен, за исключением имен всех компьютеров, входящих во все поддомены этого домена, называется зоной. Каждая зона должна обслуживаться сервером имен, который сопоставляет имена компьютеров их адресам. При этом сервер имен обычно может обслуживать сразу несколько зон, но каждая зона должна обладать хотя бы одним сервером имен.

Обычно для обеспечения надежности системы DNS и деятельности сервера имен, сопоставляющего имена компьютеров их адресам в некоторой зоне, устанавливаются подчиненные (slave) серверы. Сервер имен зоны, являющийся первоисточником информации о соответствии имен компьютеров их адресам, называется мастером (master). Информация о зонах находится на мастер-сервере в специальных текстовых файлах, содержащих так называемые записи о ресурсах (Resource Records, RR).

Подчиненные (slave) серверы получают информацию о зоне с мастер-сервера (master) с помощью копирования файлов ресурсов. Операция копирования файлов ресурсов называется трансфером зоны (zone transfer).

Информация, получаемая от мастер-серверов и подчиненных серверов, считается клиентской частью DNS одинаково достоверной (хотя это далеко не всегда соответствует истине). Поэтому ответы, получаемые от мастер- серверов и подчиненных серверов, называются авторитетными.

В процессе разрешения имени, производимого сервером по поручению клиента, сервер может обращаться с запросами к корневым серверам и серверам поддоменов, рекурсивно углубляясь в дерево доменных имен. При этом в кэше сервера обычно фиксируются результаты выполнения промежуточных запросов.

Серверы, способные углубляться в дерево доменных имен, в процессе получения ответа на запрос клиента, работают в рекурсивном режиме и кэшируют промежуточные результаты запросов. Серверы, обслуживающие корневые домены (root servers), работают в нерекурсивном режиме и не кэшируют информацию в целях защиты от DNS-подлогов (DNS spoofing).

Время, в течение которого DNS-сервер может пользоваться кэшированной информацией, называется временем жизни записи (time to live, TTL).

В процессе обслуживания запроса клиента в кэше какого-либо сервера DNS может оказаться информация, требуемая клиенту. Уровень доверия к такой информации ниже, чем к авторитетной, т.к. она может устареть и не соответствовать истине. Поэтому такие ответы называются неавторитетными, и в них содержится дополнительная информация клиенту о том, где (вероятно) может быть получена авторитетная информация по данному запросу.

Сервер DNS может быть запущен в рекурсивном режиме, кэшируя информацию, необходимую для повторных запросов клиентов, но при этом не содержать описания зон (исключая зоны для соответствия имени localhost адресу

127.0.0.1 и наоборот). Такой сервер называется исключительно кэширующим (cache only). Кэширующие серверы используются для минимизации нагрузки на авторитетные серверы.

Процедура регистрации доменного имени заключается в выборе доменного имени и фиксации адресов серверов, являющихся авторитетными для регистрируемой зоны. Считается, что для надежности каждая зона должна обслуживаться не менее, чем двумя серверами (мастером и подчиненным), находящимися в разных IP-сетях.

Ранее доменами второго уровня централизованно управлял Network Information Center (NIC), на сегодняшний момент управление децентрализовано, и домен второго уровня можно зарегистрировать у коммерческих регистраторов. В территориальных доменах регистрация обычно осуществляется национальными регистраторами. Для создания поддомена домена второго уровня достаточно всего лишь обратиться к администратору данного домена.

Процесс передачи прав авторитетности для какой-либо зоны другому серверу имен называется делегированием. Так, например, право вести записи о ресурсах поддомена может быть делегировано серверу DNS, запущенному на одной из машин, принадлежащих поддомену.

В системе BIND основой является демон named, отвечающий на запросы о преобразовании имен машин в IP-адреса и наоборот.

Файлы конфигурации BIND позволяют настраивать работу демона named так, чтобы он являлся мастер-сервером имен зоны и был одновременно подчиненным сервером для других зон.

Разделяют два типа зон:

* зоны прямого отображения, в которых имена узлов сопоставляются их IP-адресам;

* зоны обратного отображения, сопоставляющие IP-адреса узлов именам узлов.

Зоны обратного отображения всегда являются поддоменами специального домена in-addr.arpa. Имена зон обратного отображения формируются из IP- адреса сети, переписанного наоборот. Так, отображение IP-адресов узлов сети 192.168.0.0 на имена узлов задается в зоне 0.168.192.in-addr.arpa. Такая непривычная форма записи имен зон обратного отображения позволяет производить и прямое, и обратное отображение с помощью одних и тех же программ.

Обычно на DNS-сервере имеется специальный файл указателей на корневые серверы, что позволяет серверу обращаться к ним.

Работа DHCP

Администрирование сети становится исключительно неудобным, если количество рабочих станций со статическими IP-адресами приближается к не- скольким десяткам. Даже в небольших сетях гораздо удобнее автоматически настраивать сетевые интерфейсы и передавать клиентам настройки DNS, маршрутизатора по умолчанию, сервера точного времени и т. п. Протокол DHCP является усовершенствованием протокола BOOTP (Bootstrap protocol).

Последовательность взаимодействия DHCP-сервера и клиента такова:

1. Клиент посылает широковещательный запрос DHCPDISCOVER.

2. Сервер отвечает на запрос пакетом DHCPOFFER, в котором клиенту предлагаются сетевые настройки.

3. Все полученные ответы DHCPOFFER анализируются клиентом, затем клиент посылает выбранному DHCP-серверу запрос DHCPREQUEST.

4. DHCP-сервер подтверждает получение запроса и гарантирует предложенные настройки, высылая подтверждение DHCPACK.

Сервер DHCP предоставляет клиентам сетевые настройки на ограниченное время, называемое lease time. По истечении этого срока клиент может запросить продления действия настроек.

Сервер DHCP также предоставляет возможность зафиксировать за определенным клиентом его сетевые настройки так, чтобы он получал их всегда. Это делается с помощью привязки по MAC-адресу клиента.

Обычные клиентские запросы включают:

* сетевые настройки:
* IP-адрес и сетевая маска;
* IP-адрес маршрутизатора;
* доменное имя компьютера;
* настройки DNS;
* настройки приложений:
* сервер печати;
* сервер времени;
* сервер загрузки TFTP (Trivial File Transfer Protocol);
* сервер WINS

и т. д.

Имеются два обычных пути предоставления клиентам информации сервером DHCP:

* на основе MAC-адреса. В таком случае можно обеспечить постоянство параметров конфигурации, предоставляемых клиенту;

* с помощью пула адресов. При таком подходе клиент получает IP-адрес динамически по принципу обычной очереди "первый пришел – первый обслужен". Когда клиент не работает в течение заданного периода времени, его конфигурация освобождается и может быть использована сервером для настройки другого клиента.

В распространенных дистрибутивах GNU/Linux всегда имеются два разных пакета: один содержит клиентскую часть (обычно называется dhclient), другой – серверную. Исполняемый файл сервера DHCP – dhcpd.

1. Задание

1.1. Какие преимущества и недостатки имеются у кэширующих серверов?

1.2. Почему мастер-серверы и подчиненные серверы должны быть в разных IP сетях?

2. Задание

2.1. Предположим, что требуется установить сервер BIND для сети 172.16.0.0, имена узлов в ней – comp1.cheremiska.ru, comp2.cheremiska.ru и т. д. до comp254.cheremiska.ru. IP-адреса узлов соответствуют числу в их имени. Какие зоны должны быть описаны в named.conf?

2.2. Как бы вы назвали файлы описания зон в таком случае?

2.3. Создайте соответствующий заданным выше требованиям файл конфигурации и проверьте его синтаксис с помощью команды named-checkconf.

3. Задание

3.1. Составьте необходимые файлы описания зон для реализации задания из предыдущего раздела (cheremiska.ru).

3.2. Проверьте синтаксис этих файлов с помощью named-checkzone.

3.3. Получите обновленный файл db.root с официального сайта.

4. Задание

4.1. Запустите BIND и проверьте его статус.

4.2. Определите, на какие сигналы и как реагирует сервер BIND.

4.3. Остановите сервер BIND с помощью передачи ему соответствующего сигнала.

4.4. Удается ли теперь стартовать BIND с помощью сценария в /etc/init.d?

4.5. Если сервер не стартует – изучите проблему и запустите сервер.

4.6. Изучите работу rndc-confgen. Включите полученный текст в файлы /etc/named.conf (удалив комментарии) и /etc/rndc.conf.

4.7. Опробуйте rndc.

5. Задание

5.1. Проверьте правильность работы сервера DNS с помощью nslookup, host

5.2. и dig.

5.3. Проверьте трансфер зоны.

5.4. Можно ли проверить трансфер зоны средствами dig?

6. Задание

6.1. Настройте журналирование по примеру 26.23.

6.2. Выполните любой запрос к серверу. Записывается ли информация в журнал запросов? Как включить запись запросов?

6.3. Какие сообщения записываются в канал common?

6.4. Настройте канал common так, чтобы сообщения передавались службой syslog от имени local0 (facility), и создайте журнал syslog для записи этих сообщений.

7. Задание

7.1. Определите настройки для DHCP-сервера: пул адресов, маршрутизатор, DNS и т. п.

7.2. Создайте файл настроек для заданных настроек.

7.3. Запустите сервер DHCP, проверьте, получают ли клиенты IP-адреса и другую информацию с сервера.

Лабораторная работа
Тема: Настройка Web-сервра Apache в ОС Linux

Цель занятия: Научиться настраивать Web – сервер Apache в ОС Linux

Краткие теоретические сведения и справочно-информационные материалы по теме занятия.

Конфигурационный файл Apache

Apache – это целое семейство различных проектов, первым из которых был Web-сервер. Web-сервер представлен демоном httpd, поэтому проект Apache по разработке Web-сервера называется httpd.

Конфигурационные файлы Web-сервера httpd в GNU/Linux в различных дистрибутивах размещаются в разных каталогах: /etc/httpd/conf/, или /etc/apache2, или

ином. Главный конфигурационный файл называется httpd.conf, причем часто выделенные для каких-либо групп настроек индивидуальные конфигурационные файлы подключаются к httpd.conf с помощью директивы include.

В целом, настройки httpd можно разделить на три основные категории:

* секция глобальных настроек;

* настройки для главного сервера;

* настройки для виртуальных узлов.

Кроме этих секций можно выделить настройки для обработки заданных типов файлов, MIME-расширений и спецификаций обработки национальных языков.

К глобальным настройкам сервера относятся те из них, которые влияют на работу сервера Apache в целом. Далее приводятся основные глобальные настройки:

* ServerRoot – базовый каталог установки, относительно которого в файловой системе GNU/Linux размещаются конфигурационные файлы Apache, а также некоторые файлы, необходимые в его работе;

* PidFile – файл, в который при запуске сервера Apache заносится PID главного процесса сервера;

* LoadModule – команда загрузить модуль расширения Apache, скомпилированный в виде разделяемой библиотеки;

* Timeout – количество секунд перед посылкой сигнала о потере соединения;

* KeepAlive – разрешение или запрет поддержки долгоживущих соединений, доступных в рамках протокола HTTP/1.1, позволяющих оставлять соединение в неразорванном состоянии после отправки сервером требуемой информации;

* KeepAliveTimeOut – количество секунд ожидания следующего запроса, по прошествии которого долгоживущее соединение будет разорвано;

* MaxKeepAliveRequests – максимально возможное количество запросов, разрешенное для долгоживущих соединений;

* StartServers – количество дочерних процессов httpd, которые стартуют при запуске сервера Apache;

* MinSpareServers – минимальное количество ждущих соединения дочерних процессов httpd (при появлении соединений запускается столько копий httpd, чтобы количество ожидающих соединения дочерних процессов было не меньше этой величины);

* MaxSpareServers – максимальное количество ждущих соединения дочерних процессов httpd (лишние процессы останавливаются);

* MaxClients – ограничение на максимальное количество дочерних процессов httpd, определяющее возможное количество соединений;

* MaxRequestsPerChild – максимальное количество запросов, которое разрешено обслуживать одному дочернему процессу httpd, при достижении которого он гарантированно останавливается для исключения возможных утечек памяти.

1. Задание

1.1. Какая версия Apache установлена в вашей системе? Проверьте, как описаны настройки StartServers и MinSpareServers в вашей системе.

1.2. Предположим, что сервер Apache скомпилирован и установлен непривилегированным пользователем в подкаталог bin его домашнего каталога. Каковы условия, необходимые для запуска Apache непривилегированным пользователем?

2. Задание

2.1. Проверьте ваш файл конфигурации Apache на наличие директив, позволяющих получить информацию о статусе сервера.

2.2. Имеются ли в вашем конфигурационном файле Apache директивы, позволяющие использовать модуль mod_info.c? Как обратиться к его обработчику?

2.3. С помощью каких директив в вашем файле конфигурации устанавливается запрет доступа к файлам, имена которых начинаются с .ht?

3. Задание

3.1. Изучите команду apache2ctl. Как с ее помощью получить статус сервера?

3.2. Проверьте правильность конфигурации Apache.

3.3. Запустите сервер и проверьте его статус.

3.4. Обратитесь к серверу с помощью браузера для проверки его работоспособности.

4. Задание

4.1. Зарегистрируйте пользователя с первичной группой apache (или иной – в зависимости от GID запуска демона httpd в вашей системе), имеющего домашний каталог. Создайте в его домашнем каталоге подкаталог public_html с группой владельцев http. На домашний каталог пользователя установите права 750, а на public_html – 2750 (установлен SGID).

4.2. От имени только что зарегистрированного пользователя создайте файл index.html (или воспользуйтесь любым существующим в системе) в каталоге public_html. Получите доступ к нему с помощью браузера.

4.3. Разместите в каталоге public_html несколько любых файлов и удалите

4.4. index.html. Что надо сделать для получения доступа к ним?

4.5. Разместите в каталоге public_html символические ссылки на файлы из домашнего каталога. Удается ли пользоваться ими с помощью браузера?

5. Задание

5.1. Защитите личную страницу пользователя, зарегистрированного в предыдущем разделе, от неавторизованного доступа.

5.2. Как сделать так, чтобы к личной странице пользователя имели доступ только члены группы users?

6. Задание

6.1. Предположим, что у вашей машины имеются два доменных имени, связанных с ее адресом: www.machine.com и site.machine.com. Установите соответствующие настройки в файле конфигурации Apache для организации виртуального хостинга на основе имен.

6.2. Перенесите директивы конфигурации виртуального хостинга в отдельный файл.

6.3. Настройте парольный доступ к site.machine.com.

Лабораторная работа

Изучение протоколов высших уровней модели OSI

Цель работы: ознакомиться с принципами работы текстовых протоколов высших уровней на примере протоколов электронной почты.

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.

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.

Протокол Telnet

Протокол Telnet (от слов telecommunicationnetwork − телекоммуникационная сеть) обеспечивает возможность входа в удаленную систему. Он позволяет пользователю одного компьютера зарегистрироваться на удаленном компьютере, расположенном в другой части сети. При этом пользователю кажется, что он работает за терминалом удаленного компьютера. Telnet может оказаться полезным, если вы, работая на медленном компьютере, хотите воспользоваться вычислительными ресурсами более мощной машины, а также если на удаленном компьютере имеется необходимое вам программное обеспечение.

Работу Telnet обеспечивает специальная программа (сервер), запущенная на компьютере, к которому вы подключаетесь, и обрабатывающая поступающие запросы. На вашем компьютере выполняется программа Telnet, которая обращается к серверу. В процессе установления соединения компьютеры договариваются о режиме эмуляции терминала в данном сеансе работы.

Для начала сеанса работы Telnet необходимо ввести доменное имя или IP-адрес удаленного компьютера. После установления соединения удаленная система обычно запрашивает имя пользователя и пароль, хотя это зависит от типа операционной системы и программного обеспечения Telnet, установленных на удаленном компьютере.

После установления соединения ваш компьютер играет роль терминала удаленной машины. Все вводимые вами команды выполняются на удаленном компьютере. Telnet лишь осуществляет обработку и передачу ваших команд на удаленный компьютер. Telnet автоматически заканчивает свою работу, когда вы выходите из удаленной системы.

Синтаксис команды TELNET следующий:

TELNETадрес_сервера [порт]

Если порт не указан, используется 23 - стандартный порт протокола TELNET

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

Протокол SMTP

SMTP (англ. SimpleMailTransferProtocol — простой протокол передачи почты) — это широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.

SMTP впервые был описан в RFC 821 (1982 год); последнее обновление в RFC 5321 (2008) включает масштабируемое расширение — ESMTP (англ. Extended SMTP). В настоящее время под «протоколом SMTP», как правило, подразумевают и его расширения. Протокол SMTP предназначен для передачи исходящей почты с использованием порта TCP 25.

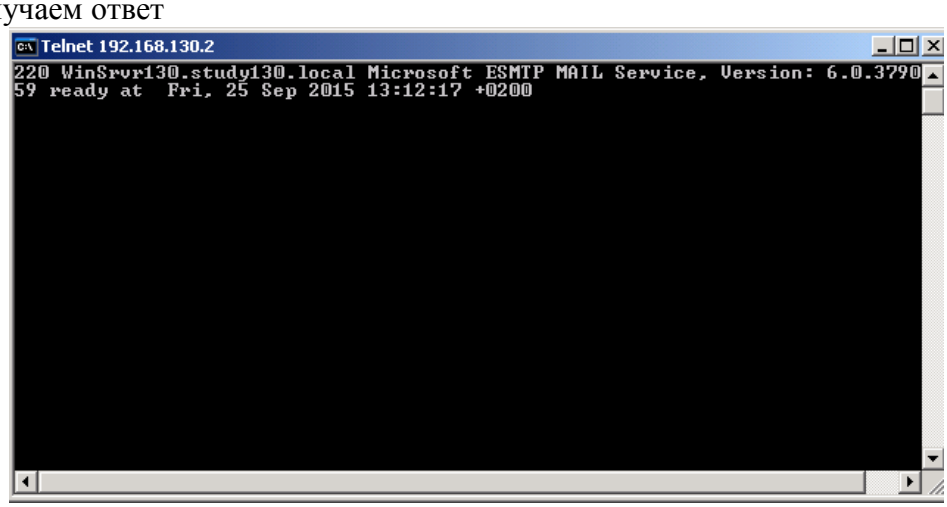
В то время, как электронные почтовые серверы и другие агенты пересылки сообщений используют SMTP для отправки и получения почтовых сообщений, работающие на пользовательском уровне клиентские почтовые приложения обычно используют SMTP только для отправки сообщений на почтовый сервер для ретрансляции. Для получения сообщений клиентские приложения обычно используют либо POP (англ. PostOfficeProtocol — протокол почтового отделения), либо IMAP(англ. InternetMessageAccessProtocol), либо патентованные системы (такие как MicrosoftExchangeиLotusNotes/Domino) для доступа к учётной записи своего почтового ящика на сервере.

Для наглядности команды пользователя выделены *курсивом синего цвета*, ответы сервера –красным цветом.

В командной строке даем команду на подключение:

telnet 192.168.130.2 25

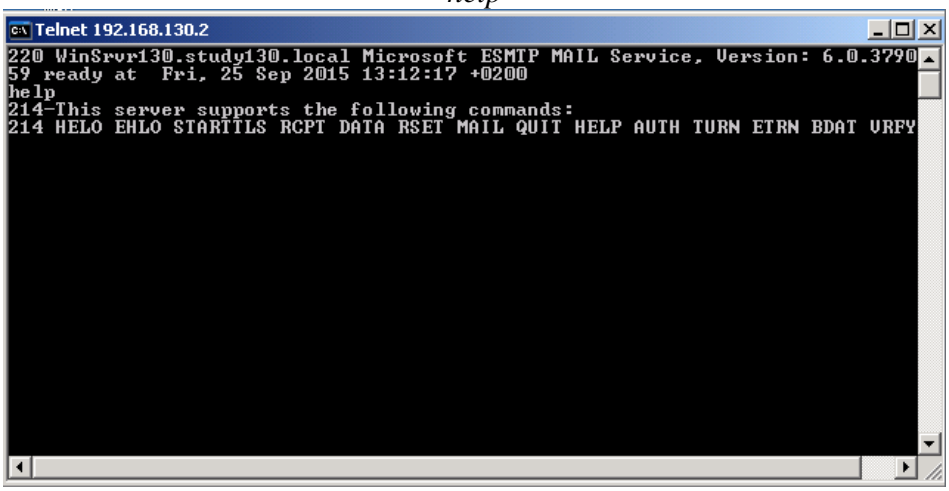
Получаем ответ



Работает! 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.

help



Список команд, которые поддерживает данный сервер:

- EHLO (устаревшая HELO) - Открывает приглашение от клиента;
- STARTTLS - Позволяет создать зашифрованное соединение;
- MAIL - Определяет отправителя сообщения;
- RCPT - Определяет получателей сообщения;
- DATA - Определяет начало сообщения;
- RSET - Сброс SMTP-соединения;

- ETRN - Борьба с проблемами безопасности команды TURN;
- VRFY - Проверяет имя пользователя системы;
- HELP - Запрашивает список команд;
- QUIT - Остановить сеанс SMTP;
- TURN - Реверс ролей в SMTP (клиент становится сервером);
- AUTH - Показывает серверу механизм аутентификации.

Дадимсерверунеправильныйзапрос.

abrakadabra

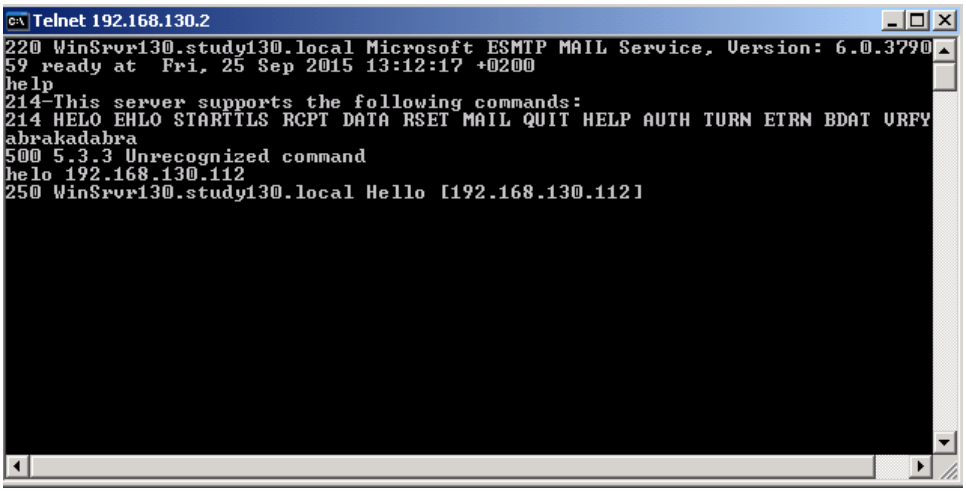
500 5.3.3 Unrecognizedcommand

Список NDR-кодов (NonDeliveryReport) можно просмотреть здесь и здесь.

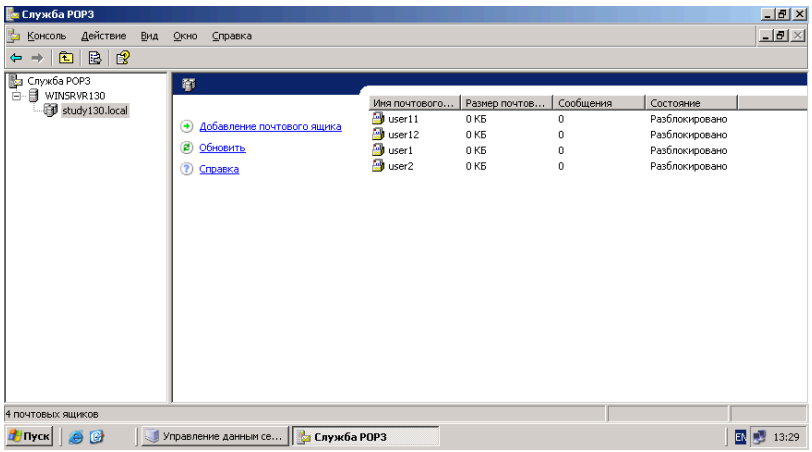
Попробуем написать письмо.

Поздороваемся ☺. Для этого воспользуемся командой HELO, указывая адрес своего компьютера в качестве аргумента.

helo192.168.130.112



Создадим на сервере пользователей***(если работаете на домашнем компьютере с доступом на сервер).***Для этого открываем Пуск → Управление данным сервером →Почтовый сервер (POP3, SMTP) → Управление этим почтовым сервером. В меню слева находим наш сервер и добавляем новые почтовые ящики



Имя почтового ящика выбирается по инициалам студента. Например, Иванов Иван Иванович – iii.

В данном случае добавили два почтовых ящика: user1 (пароль user_1)и user2 (пароль user_2).

ИЛИ подойдите к преподавателю, чтобы вам завели почтовый ящик, если лабораторную работу выполняете в университете!

Продолжаем работу в командной строке.

Укажем отправителя письма:

mailfrom: user1@study130.local

Укажем получателя письма:

rcptto: user2@study130.local

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:

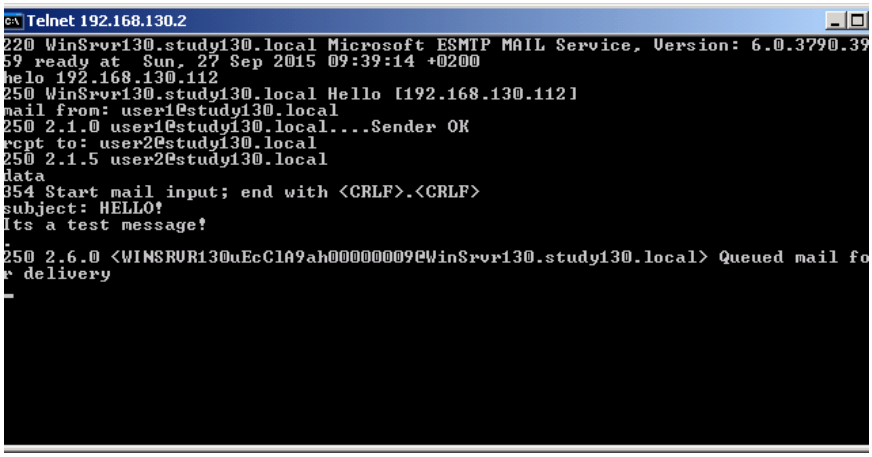
Date: Tue, 22 Nov 2005 19:55:07 +0200
Дата создания по GMT и часовой пояс
From: User user1@home.my
Откого
Reply-To: User user1@home.my
Кому отвечать
To: user2@home.my
Кому
Subject: Test
Темаписьма
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

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

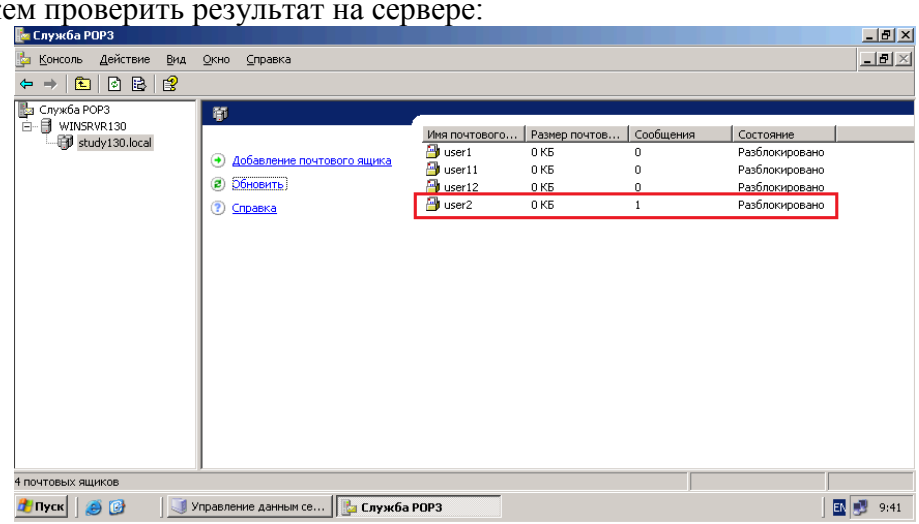
Вводим тест сообщения и не забываем про точку в конце.

SubjectHELLO!
It’s a test message!
.



Письмо принято!

Можем проверить результат на сервере:



Теперьвыходим:

quit

221 Подключение к узлу утеряно.

Протокол POP3

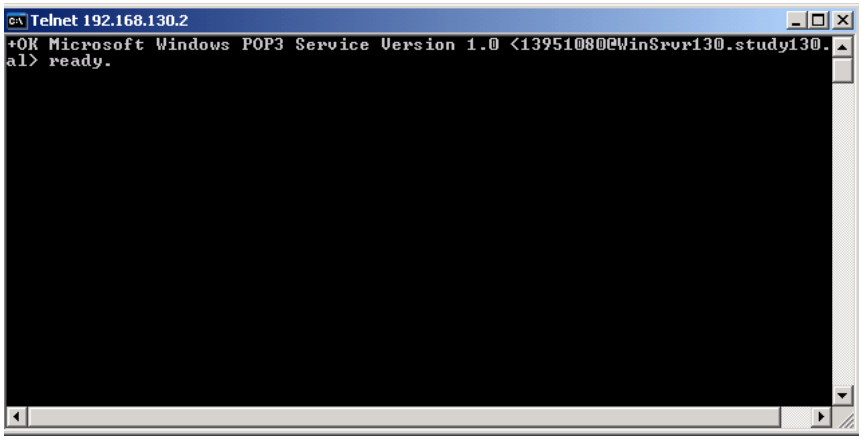
POP3 (англ. PostOfficeProtocolVersion 3 — протокол почтового отделения, версия 3) — стандартный интернет-протокол прикладного уровня, используемый клиентами электронной почты для получения почты с удаленного сервера по TCP/IP-соединению.

POP и IMAP (InternetMessageAccessProtocol) — наиболее распространённые интернет - протоколы для извлечения почты. Практически все современные клиенты и серверы электронной почты поддерживают оба стандарта. Протокол POP был разработан в нескольких версиях, нынешним стандартом является третья версия (POP3). Большинство поставщиков услуг электронной почты (Hotmail, Gmail и Yahoo!,Mail) также поддерживают IMAP и POP3. Предыдущие версии протокола (POP, POP2) устарели.

Альтернативным протоколом для сбора сообщений с почтового сервера является IMAP.

Поработаем с протоколом POP3. Обычно он работает, используя порт 110.

telnet 192.168.130.2 110



Работает, но трехсимвольного кода ответа нет!

Попробуемhelp:

help

-ERRUnacceptablecommand

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

Залогинемся:

useruser2@study130.local

+OK

pass user_2

+OK User successfully logged on

Воспользуемся командой LIST, чтобы получить информацию обо всех сообщениях, находящихся в почтовом ящике.

list

+OK 1 messages (452 octets)

1 452

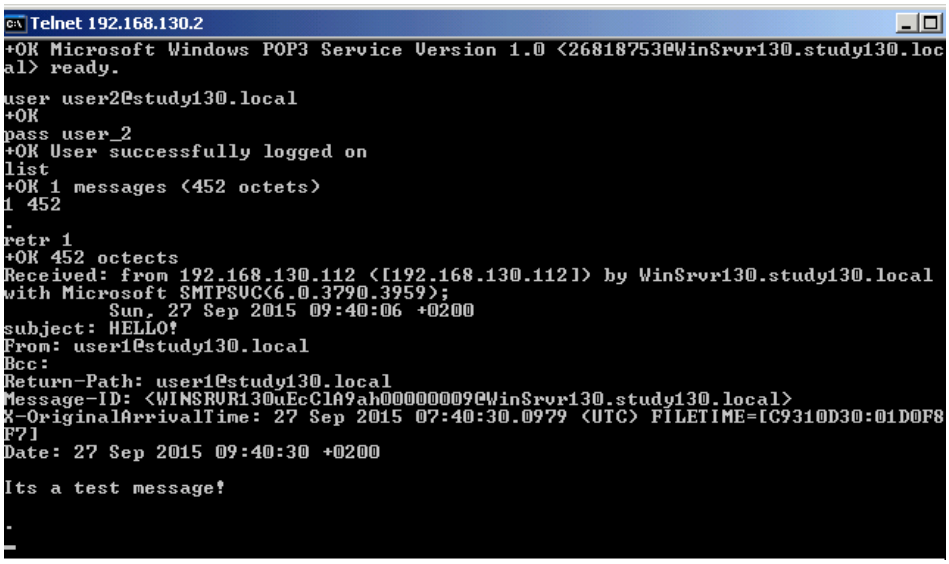
.

У нас одно письмо в 452 символа. 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 получим первое письмо (см. рисунок ниже) с помощью команды RETR, которая передает сообщение с указанным номером.

retr 1

+OK 452 octets



Как мы видим, служебных полей стало больше – их добавил сервер.

Теперь удалим письмо с сервера с помощью команды DELE.Сервер помечает указанное сообщение для удаления. Сообщения, помеченные на удаление, реально удаляются только после закрытия транзакции (закрытие транзакций происходит обычно после посыла команды QUIT, кроме этого, например, на серверах закрытие транзакций может происходить по истечении определённого времени, установленного сервером).

dele 1

+OKMessage marked as deleted

Проверим, есть ли что еще:

list

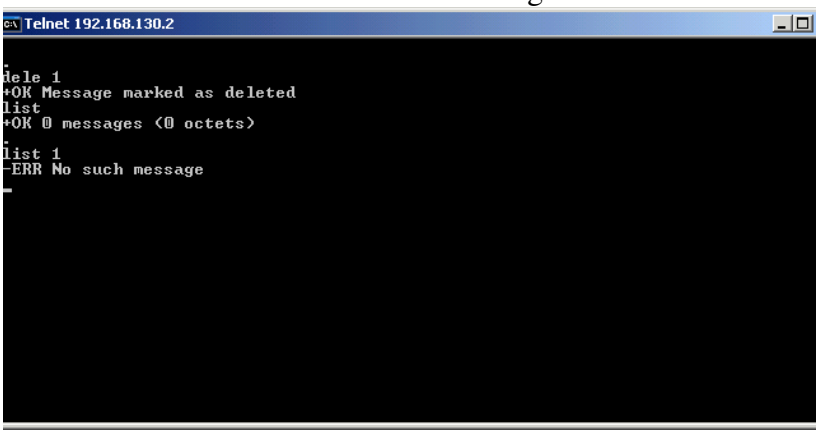
+OK 0 messages (0 octets)

.

Ничегонет. А можно проверить и так, для программы это будет более удобным:

list 1

-ERRNo such message



Ну, итеперьвыходим:

quit

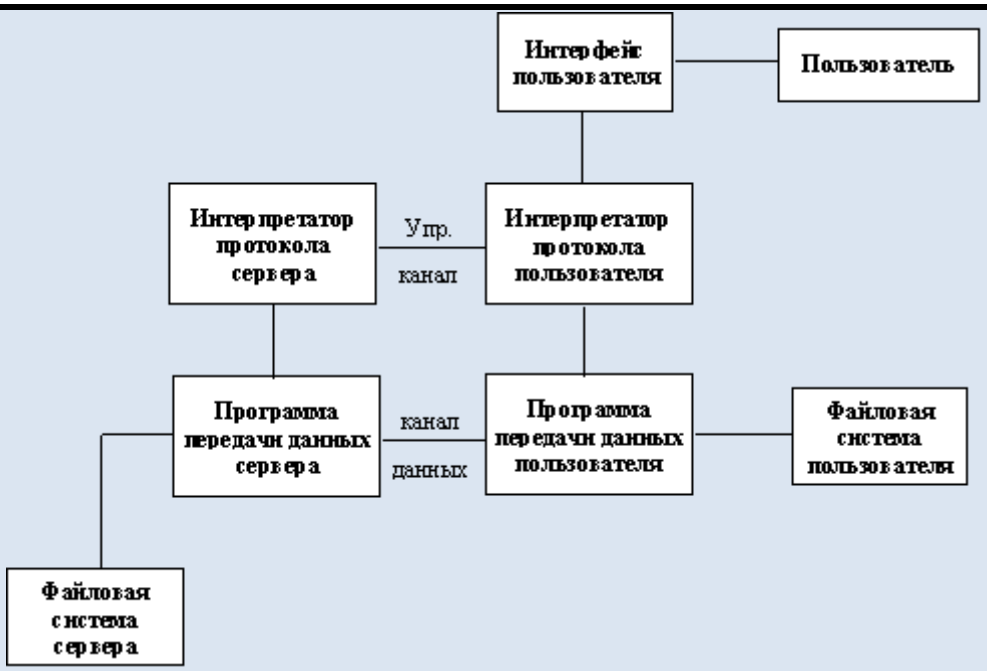
Подключение к узлу утеряно

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.

Протокол FTP

В отличие от Telnet, протокол FTP (FileTransferProtocol) предназначен не для работы на удаленном компьютере, а для передачи файлов между подключенными к сети компьютерами. Так же как и Telnet, сервис FTP основан на совместном использовании двух программ — программы-сервера, которая выполняется постоянно в фоновом режиме на удаленном компьютере, и программы-клиента, которую вы должны запустить на своем компьютере, чтобы начать сеанс работы по протоколу FTP. Программа сервер занимается обработкой всех запросов, приходящих к ней от программы-клиента, поэтому если программа-сервер не предоставляет каких-либо возможностей вроде докачки и т.д., то каким бы навороченным клиентом вы ни пользовались все равно данные возможности так и останутся недоступными для вас. Протокол FTPпозволяет передавать файлы, как в текстовом, так и в двоичном формате между совершенно различными платформами.

Модель протокола FTP:



Алгоритм работы протокола FTP состоит в следующем:

1. Сервер FTP использует в качестве управляющего соединение на TCP порт 21, который всегда находится в состоянии ожидания соединения со стороны пользователя FTP.

2. После того как устанавливается управляющее соединение модуля “Интерпретатор протокола пользователя” с модулем сервера — “Интерпретатор протокола сервера”, пользователь (клиент) может отправлять на сервер команды. FTP-команды определяют параметры соединения передачи данных:

роль участников соединения (активный или пассивный),

порт соединения (как для модуля “Программа передачи данных пользователя”, так и для модуля “Программа передачи данных сервера”),

тип передачи,

тип передаваемых данных,

структуру данных и управляющие директивы, обозначающие действия, которые пользователь хочет совершить (например, сохранить, считать, добавить или удалить данные или файл и другие).

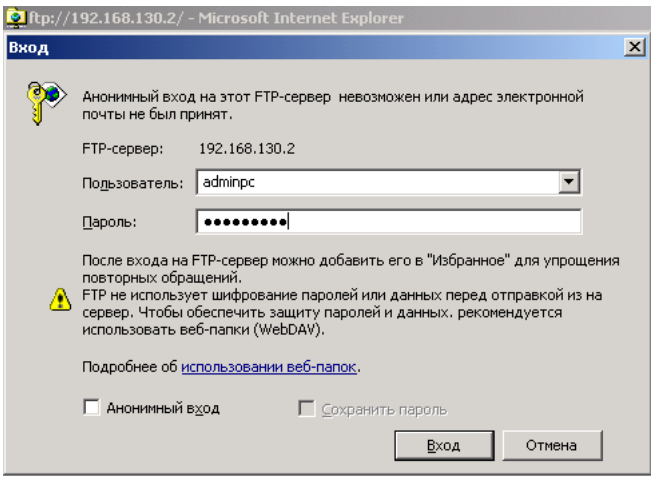
3. После того как согласованы все параметры канала передачи данных, один из участников соединения, который является пассивным (например, “Программа передачи данных пользователя”), становится в режим ожидания открытия соединения на заданный для передачи данных порт. После этого активный модуль (например, “Программа передачи данных сервера”) открывает соединение и начинает передачу данных.

4. После окончания передачи данных, соединение между “Программой передачи данных сервера” и “Программой передачи данных пользователя” закрывается, но управляющее соединение “Интерпретатора протокола сервера” и “Интерпретатора протокола пользователя” остается открытым. Пользователь, не закрывая сессии FTP, может еще раз открыть канал передачи данных.

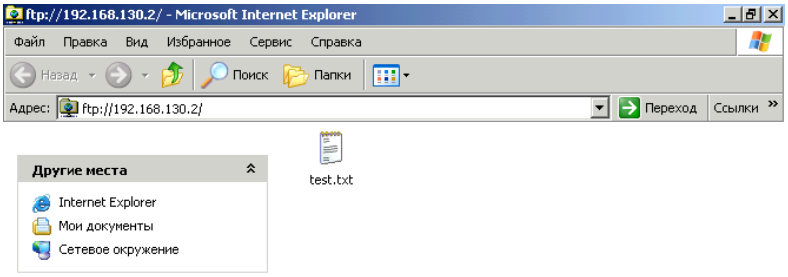
Войдем на FTP-сервер через браузер. Открываем браузер и в адресной строке указываем:

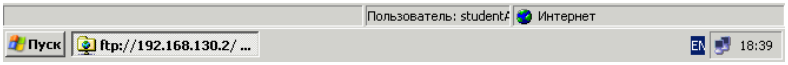
ftp://192.168.130.2

Нажимаем Enter. Появилось окно следующего вида:

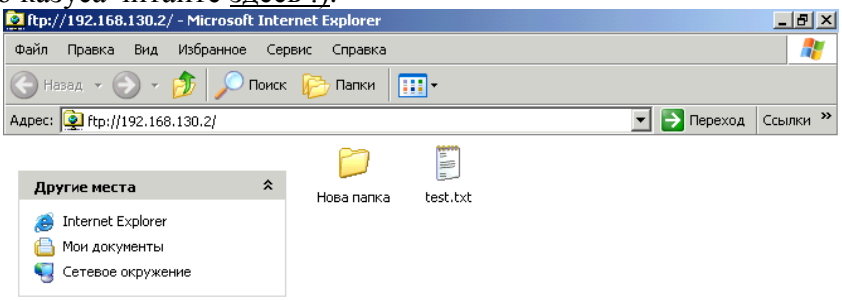


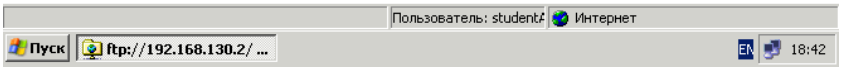
Указываем логин и пароль. Логин: ***adminStudy***пароль: ***locAdmin1.***
Вошли!





Пробуем создать новую папку. Выдаст ошибку, но не обращайте внимание. Нажимайте «ОК» и обновляйте страницу. Как видите – папка «Нов*а* папка» создана. Описание этого казуса читайте здесь :).



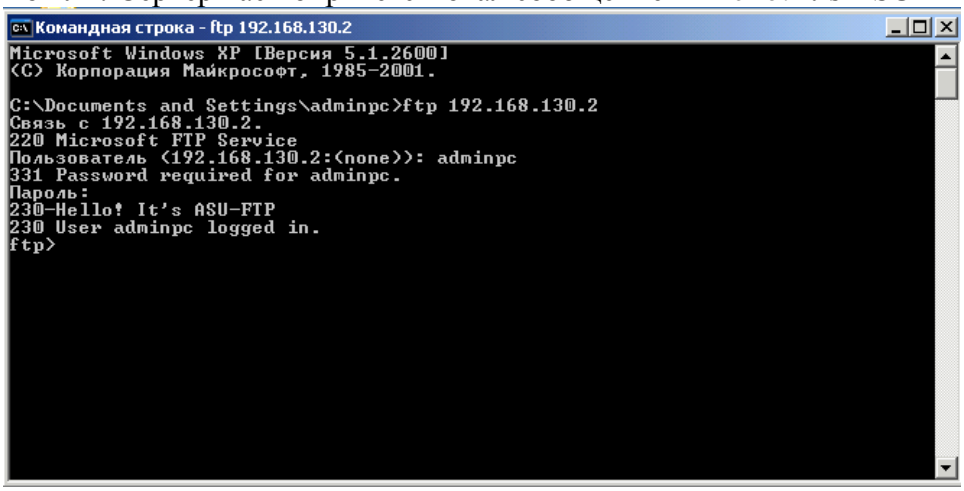


Для удобства сразу переименуйте папку «dir».
Теперь зайдем на FTP-сервер через командную строку.

ftp 192.168.130.2

Залогинемся (не пугайтесь, пароль при вводе остается невидимым, будто мы ничего и не вводим).

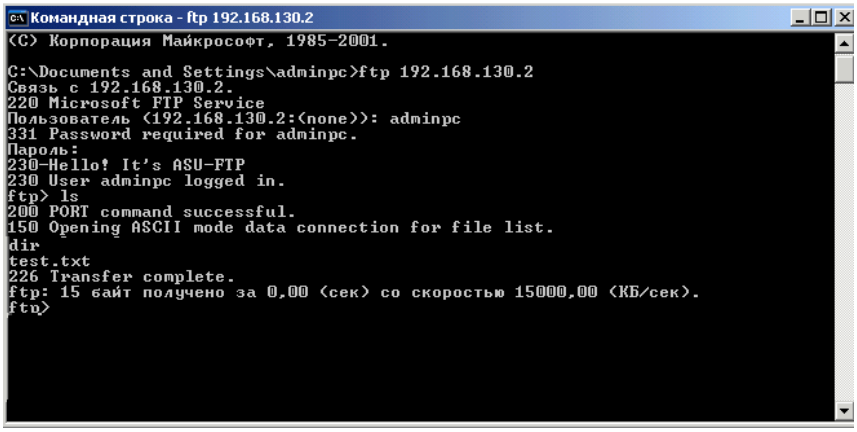
Вошли! Сервер нас поприветствовал сообщением «Hello! It's ASU-FTP».



Описание действующих команд можно узнать здесь.

Введем командуLS, чтобы отразить список файлов и папок в удаленным каталоге.

ls

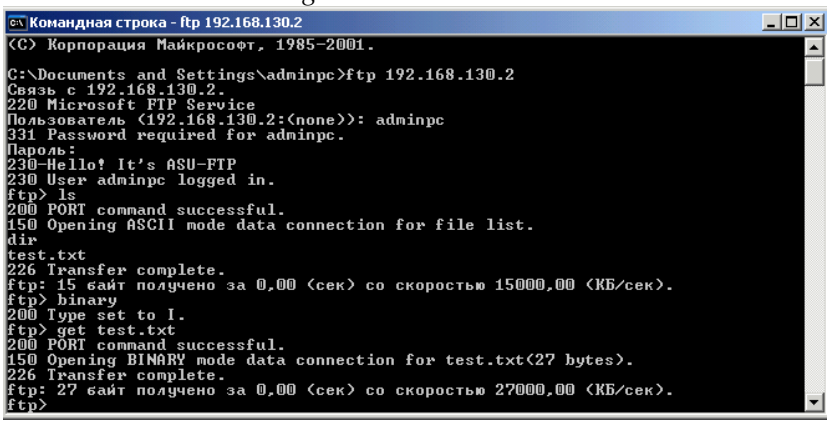


Получим файл test.txt, установив перед этим режим передачи файлов в двоичном формате с помощью команды BINARY:

binary

200 Type set to I

get test.txt



По умолчанию файл скопирован в папку C:\DocumentsandSettings*username*. Можно сменить текущий локальный каталог с помощью команды LCD. Напоминаю, описание действующих команд можно узнать здесь.

Протокол HTTP

HTTP — широко распространённый протокол передачи данных, изначально предназначенный для передачи гипертекстовых документов (то есть документов, которые могут содержать ссылки, позволяющие организовать переход к другим документам).

Аббревиатура HTTP расшифровывается как HyperTextTransferProtocol, «протокол передачи гипертекста». В соответствии со спецификацией OSI, HTTP является протоколом прикладного (верхнего, 7-го) уровня. Актуальная на данный момент версия протокола, HTTP 1.1, описана в спецификации RFC 2616.

Протокол HTTP предполагает использование клиент-серверной структуры передачи данных. Клиентское приложение формирует запрос и отправляет его на сервер, после чего серверное программное обеспечение обрабатывает данный запрос, формирует ответ и передаёт его обратно клиенту. После этого клиентское приложение может продолжить отправлять другие запросы, которые будут обработаны аналогичным образом.

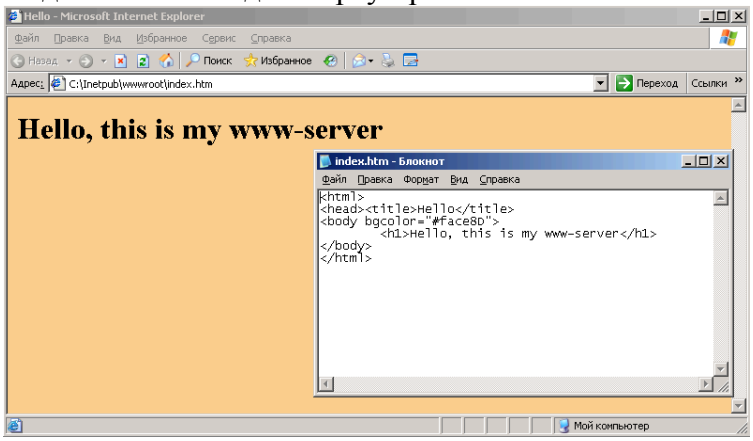
Задача, которая традиционно решается с помощью протокола HTTP — обмен данными между пользовательским приложением, осуществляющим доступ к веб-ресурсам (обычно это веб-браузер) и веб-сервером. На данный момент именно благодаря протоколу HTTP обеспечивается работа Всемирной паутины.

Также HTTP часто используется как протокол передачи информации для других протоколов прикладного уровня, таких как SOAP, XML-RPC и WebDAV. В таком случае говорят, что протокол HTTP используется как «транспорт».

API многих программных продуктов также подразумевает использование HTTP для передачи данных — сами данные при этом могут иметь любой формат, например, XML или JSON.

Как правило, передача данных по протоколу HTTP осуществляется через TCP/IP-соединения. Серверное программное обеспечение при этом обычно использует TCP-порт 80 (и, если порт не указан явно, то обычно клиентское программное обеспечение по умолчанию использует именно 80-й порт для открываемых HTTP-соединений), хотя может использовать и любой другой.

Поработаем с протоколом HTTP. Обычно он работает, используя порт 80.Наша цель – получить исходный HTMLкод без браузера.



Для этого введем в командной строке команду:

telnet 192.168.130.2 80

Если вы видите пустой черный экран и мигающий курсор - все в порядке. Подключение прошло успешно, сервер ждет нашего запроса.

Запросимглавнуюстраницу:

GET /index.htm HTTP/1.1

enter

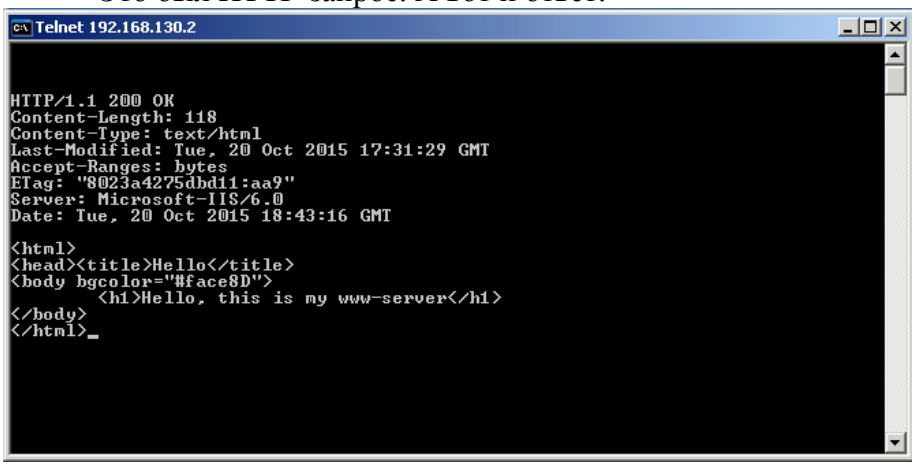
host:192.168.130.2

enter

enter

Enter 2 раза означает конец заголовков.

Это был HTTP-запрос. А вот и ответ:



Так, мы подключились к серверу через 80-ый порт (стандартный для HTTP), отправили запрос, состоящий из стартовой строки и одного заголовка, и получили ответ, состоящий из стартовой строки, семи заголовков и тела.

В стартовой строке запроса необходимо указать HTTP метод, URI документа и версию HTTP. В заголовке Host − имя хоста. Это был минимальный запрос. Если убрать заголовок Host, сервер скажет "Badrequest".

Ответ начинается со стартовой строки "HTTP/1.1 200 OK", что означает, что наш запрос обработан успешно. Нам присылают желанный документ, содержимое которого находится в теле HTTP ответа. Именно его мы увидим, если нажмем в браузере кнопку "Исходный код страницы". Среди заголовков, обратите внимание на Content-Length − здесь указан размер тела сообщения в байтах.

Пустая строка означает, что заголовки закончились и начинается тело сообщения. Именно поэтому мы нажимали Enter дважды в конце запроса.

ЗАДАНИЕ

1. Получить у преподавателя адрес сервера электронной почты, имена и пароли пользователей. Создать на сервере свои почтовые ящики. Имя почтового ящика выбирается по инициалам студента (например, Иванов Иван Иванович – iii).
2. С помощью программы TELNETпоработать с SMTP, отправить сообщение, используя команды протокола.
3. Посмотреть сообщение с помощьюPOP3, также используя программу TELNET.
4. Определить, является ли протокол FTP текст-ориентированным и поддерживает ли он трехсимвольные коды ответов.
5. Подключиться к FTP-серверучерез браузер и через командную строку. Попробовать передать и считать данные двумя способами.
6. Получите HTMLкод через командную строку.

   Все действия фиксировать с помощью скриншотов и предоставить в отчете.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Почему протоколы называются протоколами высших уровней?
2. Что такое TELNETи для чего он предназначен?
3. Для чего нужны протоколы SMTPи POP3, что они из себя представляют?
4. Перечислите возможные состояния для протокола POP3.
5. Расскажите формат сообщения RFC 822 (электронная почта).
6. Почему прием и передача электронной почты производятся по разным протоколам?
7. Какие команды протокола SMTPвы знаете?
8. Что является альтернативным протоколом для SMTP?
9. Какая комбинация означает конец ввода данных в протоколе SMTP?
10. Почему POP3требует обязательной аутентификации, а SMTP нет?

11. Что такое FTPпротокол? Объясните принцип его работы.
12. Какая спецификация определяет FTP модель в терминах модели «пользователь-сервер»?
13. Объясните, что такое HTTP протокол и для чего он предназначен.
14. Что необходимо указать при минимальном HTTP-запросе?
15. Какие порты используют вышеназванные протоколы?
16. Почему для работы со стандартными протоколами используют специальные программы?

Лабораторная работа
Настройка безопасности почтового клиента

Цель работы: Ознакомиться с настройками почтового клиента, например Outlook Express для передачи сообщений с электронной цифровой подписью.

Краткие теоретические сведения:

Почтовый клиент- это программа, предназначенная для приема – отправки электронной почты. Примером такой программы является программа Outlook Express. Для работы с электронной почтой почтовый клиент должен поддерживать протоколы SMTP (исходящая почта) и POP3 (входящая почта).

Одну из реальных угроз в современных глобальных сетях представляют электронные письма с вложенными программами-вирусами (прикрепленные файлы). Именно посредством электронной почты были проведены последние глобальные сетевые атаки. В связи с этим защита компьютера при работе с электронной почтой приобретает особую актуальность. Аналогично вопрос конфиденциальности и безопасности электронной почты с течением времени не только не теряет своей актуальности, но и становится всё более остро. Отправляя конфиденциальную информацию по электронной почте, необходимо иметь уверенность в том, что сообщение не перехватывалось и не подделывалось.

Outlook Express позволяет использовать цифровые идентификаторы или цифровые удостоверения, для защиты электронной почты, в частности, для шифрования почтовых сообщений. По умолчанию Outlook Express автоматически добавляет сертификаты, которые приходят по почте, в адресную книгу Windows.

Цифровой идентификатор состоит из открытого ключа, личного ключа и цифровой подписи. Когда пользователь подписывает отправляемые им сообщения, он добавляет в состав сообщения свою цифровую подпись и открытый ключ. Комбинация цифровой подписи и открытого ключа называется сертификатом.

Цифровая подпись отправителя подтверждает получателю подлинность полученных сообщений. Открытый ключ отправителя получатель может использовать для отправки ему зашифрованной почты, расшифровать которую он сможет с помощью своего личного ключа. Таким образом, чтобы отправить зашифрованное сообщение в чей-либо адрес, необходимо включить в адресную книгу цифровые идентификаторы, ассоциированные с получателями. Благодаря этому при помощи открытых ключей получателей Вы сможете зашифровывать отправляемые ими сообщения. Каждый получатель расшифрует полученное сообщение с помощью своего личного ключа.

Задание: Разработать систему правил по управлению входящими сообщениями в Outlook Express и настроить Outlook Express для передачи сообщений с электронной цифровой подписью.

Алгоритм выполнения работы:

a. Создание системы правил по обработке входящих сообщений электронной почты.

Расширенные правила управления сообщениями поддерживают большое количество критериев действий, включая блокирование отправителей сообщения и новые правила для групп новостей. Для создания правила по обработке входящих сообщений электронной почты выполните следующие действия.

1. Откройте программу Outlook Express.
2. Последовательно выполните команды меню Сервис - Правила для сообщений – Почта.
3. В результате откроется диалоговое окно (рис. 1). Создать правило для почты.
4. Выберите условие создаваемого правила (например для защиты от заражения компьютера вложенными в электронное письмо файлами можно выбрать условие **Искать сообщение с вложениями**, рис. 2).

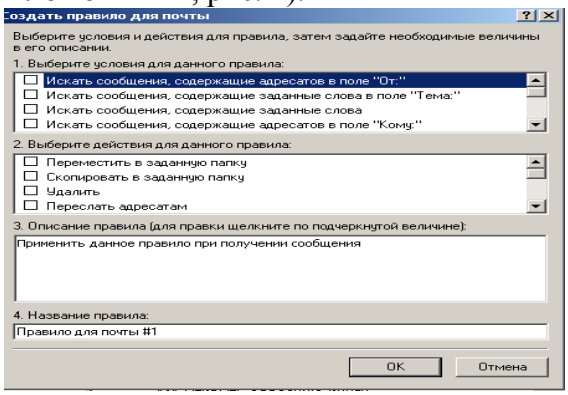


Рис. 1

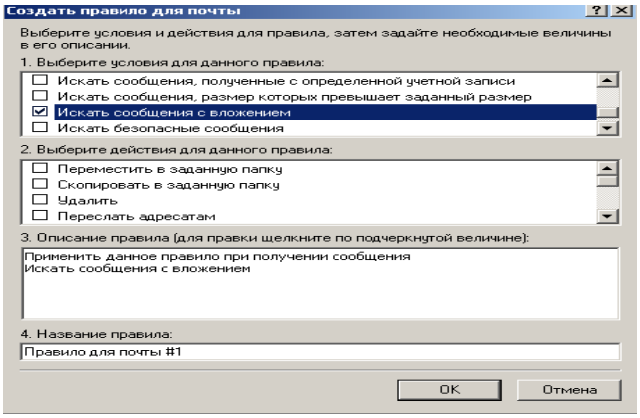


Рис. 2

5. Выберите действия для данного правила (например, **Удалить с сервера,** рис. 3).

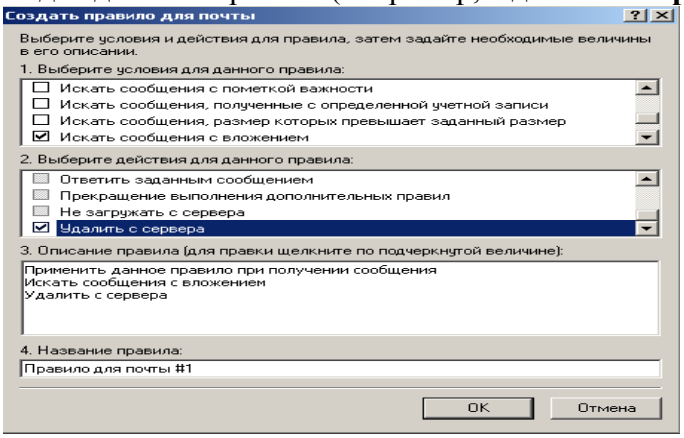


Рис. 3

6. Обратите внимание, что в поле 3 приводится описание созданного правила. После создания этого правила, все письма содержащие вложения будут удалены с сервера.
7. Для завершения создания правила введите его имя в поле 4 – **Название правила**.

8. Для успешного создания правила нужно задать хотя бы одно условие. Если задано составное условие (т.е. несколько условий), то по умолчанию должно выполниться хотя бы одно из простых условий; в поле “Описание правила”.
9. Пример составного условия показан на рис. 4. В результате выполнения этого правила с сервера будут удалены все письма с вложениями, в которых ёщё в поле «Тема» содержится слово «вирус» (можно задать произвольное слово).

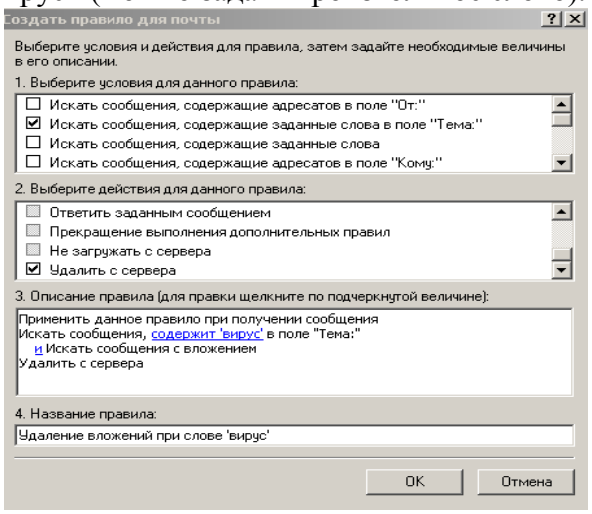


Рис. 4

10. Таким образом, комбинируя правила управления входящими сообщениями, можно существенно повысить защищенность компьютера при работе с электронной почтой.

b. Получение цифрового идентификатора.
Прежде чем отправлять сообщения, подписанные цифровой подписью и зашифрованные, необходимо получить цифровой идентификатор.

1. Для получения цифрового идентификатора необходимо заполнить заявку на получение цифрового идентификатора в организации, уполномоченной представлять этот сервис.
2. Для этого в окне Параметры (меню Сервис – Параметры) на вкладке Безопасность нажмите кнопку Получить сертификат.
3. В результате запустится веб-браузер, который обратится к странице на веб-узле Microsoft, где приводится перечень организаций, уполномоченных предоставлять этот сервис (например, у компании VeriSign можно бесплатно получить временный (на два месяца) цифровой идентификатор, позволяющий опробовать все режимы безопасности программы Outlook Express).
4. После заполнения формы с запросом на предоставление цифрового идентификатора Вы получите (через несколько минут) почтовое сообщение от VeriSign с инструкциями по установке полученного цифрового идентификатора.
5. Раскройте и прочтите письмо. В точности выполните приведенные в нем инст рукции.
6. Подтвердите установку цифрового идентификатора.

c. Использование цифровой электронной подписи.

1. Для отправки сообщения, которое требуется подписать цифровой подписью, создайте новое сообщение (**Сообщение – Создать сообщение**).
2. Выберите в меню **Сервис** команду **Цифровая подпись.** В результате напротив поля **Кому** появится символ  подтверждающий включение электронной цифровой подписи (рис. 5).

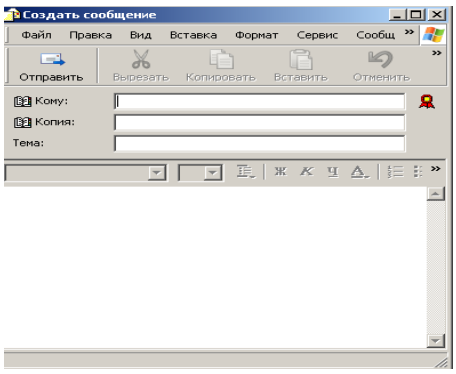


Рис. 5

3. Если отправляемое сообщение требуется также зашифровать, выберите в меню **Сервис** команду **Зашифровать.** В случае включения шифрования появится символ  напротив поля **Копия** (рис. 6).

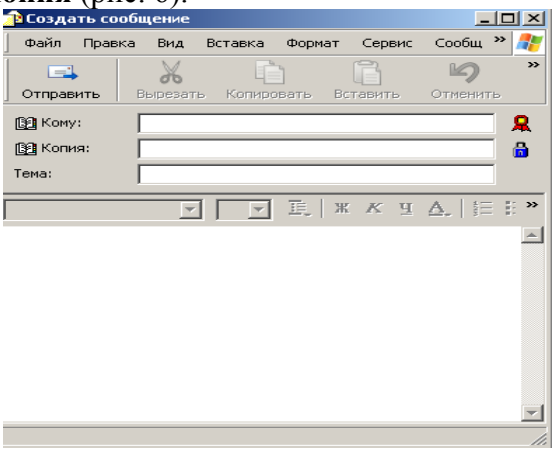


Рис. 6

d. Настройка опций обмена защищенной почтой.

1. Чтобы настроить работу с защищенными почтовыми сообщениями, выберите в меню **Сервис** команду **Параметры** и перейдите на вкладку **Безопасность** (рис. 7).

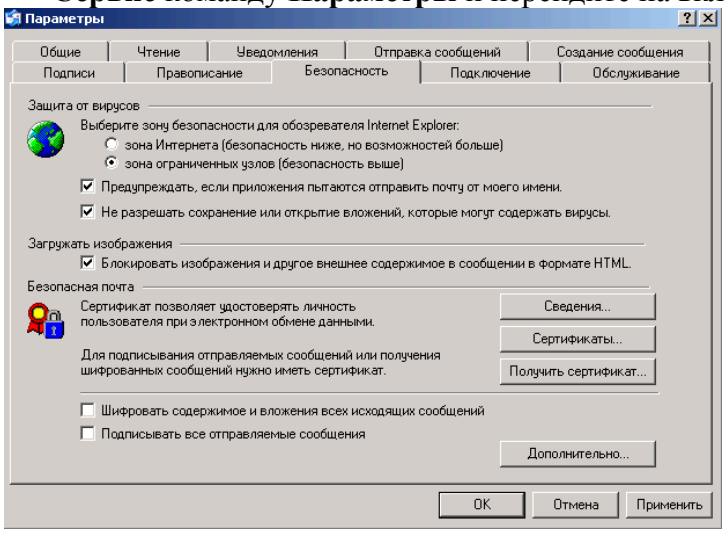


Рис. 7

2. Параметры, необходимые для настройки обмена защищенной почтой, находятся в группе **Безопасность – Дополнительно,** перейдите на вкладку **Дополнительные параметры безопасности** (рис. 8).

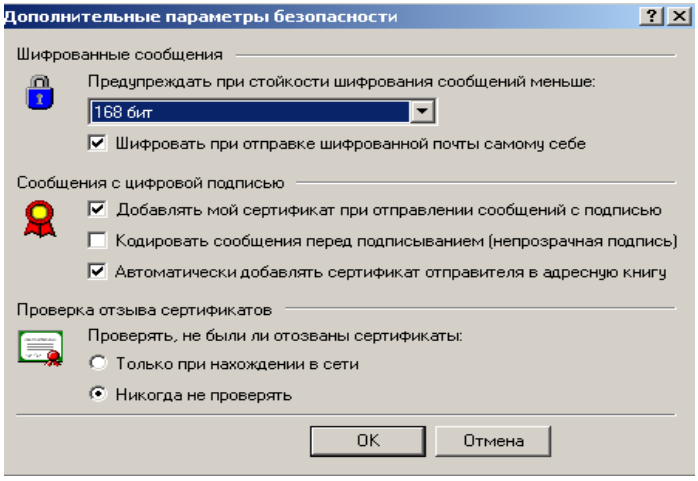


Рис. 8

Задание для самостоятельной работы

1. Выполните задания a-d
2. Создайте три новых правила (произвольных) управления сообщениями электронной почты и опишите их безопасные свойства, т.е. как и от каких угроз можно ими защитить компьютер. Составьте отчет.

Контрольные вопросы:

1. Для чего используется механизм электронной цифровой подписи?
2. Что понимается под сертификатом?
3. Какой метод шифрования использует электронная цифровая подпись?

Лабораторная работа
Настройка параметров аутентификации

Цель работы: Ознакомиться с механизмами аутентификации и идентификации, локальными политиками безопасности, встроенными в ОС Windows XP.

Краткие теоретические сведения:

В соответствии с сертификационными требованиями к системам безопасности операционных систем при подключении пользователей должен реализовываться механизм аутентификации и/или идентификации. Идентификация и аутентификация применяются для ограничения доступа случайных или незаконных субъектов (пользователей, процессов) к информационной системе, объектам – ресурсам (аппаратным, программным, информационным).

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он сам себя выдаёт.

Настройка параметров аутентификации в ОС Windows XP выполняется в рамках локальной политики безопасности. Вкладка «Локальная политика безопасности» используется для изменения политики учетных записей и локальных политик безопасности на компьютере. При помощи вкладки «Локальная политика безопасности» можно определить:

- Кто имеет доступ к компьютеру;
- Какие ресурсы могут использовать пользователи на компьютере;

- Включение и выключение записи действий пользователей или группы пользователей в журнале событий.

Задание: Настроить параметры локальной политики безопасности операционной системы Windows XP.

Алгоритм выполнения работы:

Для просмотра и изменения параметров аутентификации пользователей выполните следующие действия:

1. Выберите кнопку Пуск на панели задач.
2. Откройте меню Настроить – Панель управления.
3. В открывшемся окне выберите ярлык Администрирование – Локальная политка безопасности (рис. 1).

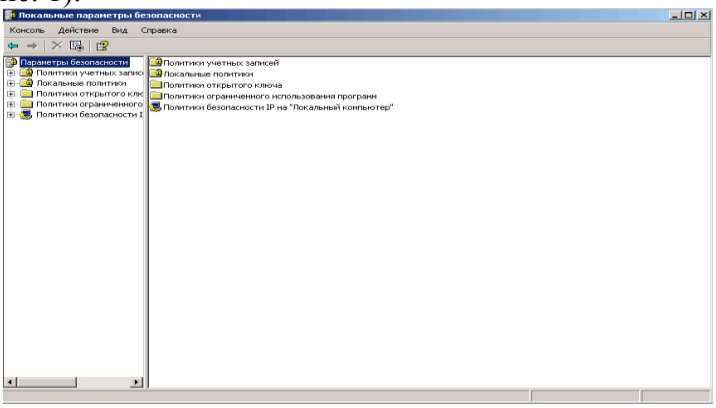


Рис. 1

4. Выберите пункт **Политика учетных записей** (этот пункт включает два подпункта: **Политика паролей** и **Политика блокировки учетной записи**).
5. Откройте подпункт Политика паролей. В правом окне появится список настраиваемых параметров (рис. 2).

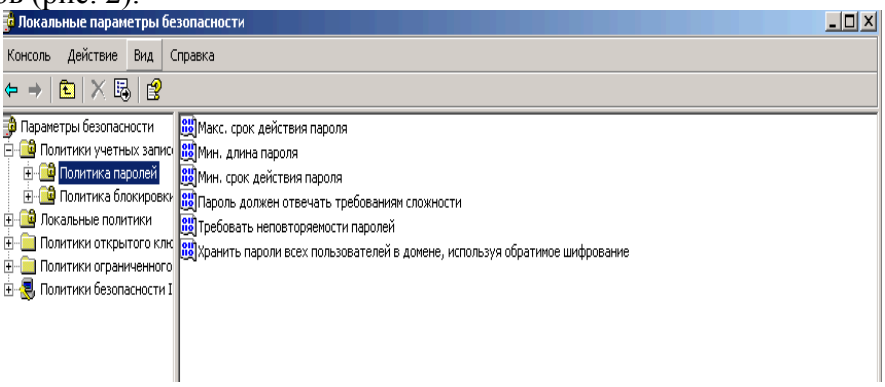


Рис. 2

6. В показанном примере политика паролей соответствует исходному состоянию системы безопасности после установки операционной системы, при этом ни один из параметров не настроен. Возможные значения параметров приведены в таблице №1.

Таблица №1

Значения параметров Политики паролей

Параметр	Значение
Требовать повторяемости паролей	Определяет число новых паролей, которые должны быть сопоставлены учетной записи пользователя, прежде чем можно будет снова использовать старый пароль. Это значение должно принадлежать диапазону от 0 до 24.
Максимальный срок действия пароля	Определяет период времени (в Днях), в течение которого можно использовать пароль, чем система потребует от пользователя заменить его. Можно задать значение в диапазоне от 1 до 999 дней или снять всякие ограничения срока действия, установив число дней равным 0.
Минимальный срок действия пароля.	Определяет период времени (в Днях), в течение которого можно использовать пароль, чем система потребует от пользователя заменить его. Можно задать значение в диапазоне от 1 до 999 дней или снять всякие ограничения срока действия, установив

	число дней равным 0.
Минимальная длина пароля.	Определяет наименьшее число символов, которые может содержать пароль учетной записи пользователя. Можно задать значение в диапазоне от 1 до 14 символов или отменить использование пароля, установив число символов равным 0
Пароль должен отвечать требованиям сложности	Определяет, должны ли отвечать пароли требованиям сложности. Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям. ➢ Пароль не может содержать имя учетной записи пользователя или какую-либо его часть; ➢ Пароль должен состоять не менее чем из 6 символов; ➢ В пароле должны присутствовать символы трех категорий из числа следующих четырех: 1. Прописные буквы английского алфавита от A до Z; 2. Строчные буквы английского алфавита от A до Z;
Параметр	Значение
	3. Символы не принадлежащие алфавитно-цифровому набору (например, !,$,#,%). Проверка соблюдения этих требований выполняется при изменении или создании паролей.
Хранить пароли всех пользователей в домене, используя обратимое шифрование.	Определяет, следует ли в системах Windows 2000, Windows XP хранить пароли, используя обратимое шифрование. Эта политика обеспечивает поддержку приложений, использующих протоколы, которым для проверки подлинности нужно знать пароль пользователя. Хранить пароли, зашифрованные обратимыми методами, это всё равно, что хранить их открытым текстом. Поэтому данную политику следует использовать лишь в исключительных случаях, если потребности приложения оказываются важнее, чем защита пароля.

7. Ознакомитесь со свойствами всех параметров.
8. Для изменения требуемого параметра выделите его и вызовите его свойства из контекстного меню после нажатия правой кнопки мыши (или дважды щёлкните на изменяемом параметре).
9. В результате этого действия появится одно из окон, показанных на рис. 3.

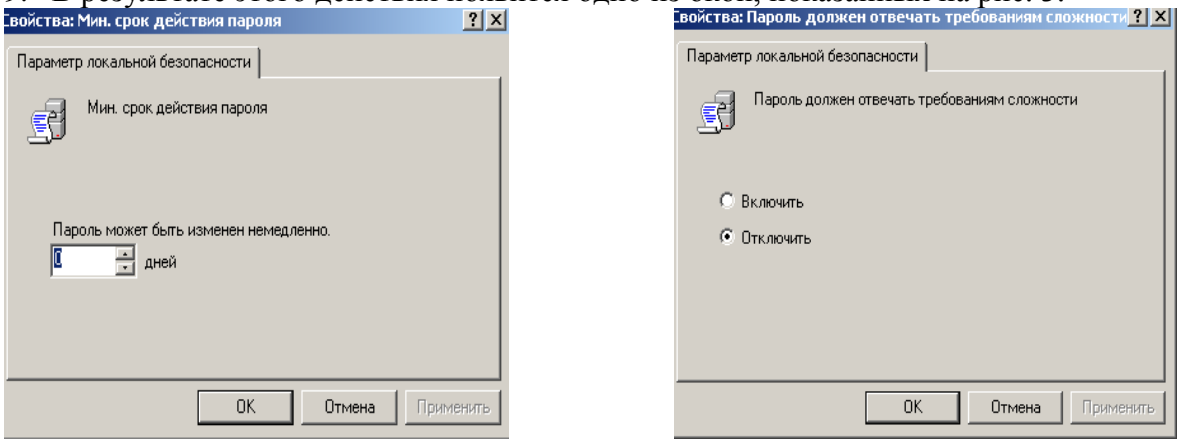


Рис. 3

10. Измените, значение параметра и нажмите Ок.
11. Например (обязательно выполнить и сохранить), выберите параметр Требовать неповторяемости паролей и измените его значение на 1.
12. Для настройки Политики блокировки учетной записи выберите этот подпункт и откройте его.
13. Значения параметров данного подпункта Политики учетной записи приведены в таблице №2.

Таблица №2

Параметр	Значение
Пороговое значение блокировки	Определяет число неудачных попыток входа в систему, после которых учетная запись пользователя блокируется. Блокированную учетную запись нельзя использовать до тех пор, пока не будет сброшена администратором или пока не истечёт её интервал блокировки. Можно задать значение в диапазоне от 1 до 999 или запретить блокировку данной учетной записи, установив значение 0.
Блокировка учетной записи на	Определяет число минут, в течении которых учетная запись остаётся блокированной, прежде чем будет автоматически разблокирована. Этот параметр может принимать значения от 1 до 99999 минут. Если установить
Параметр	Значение
	Значение 0, учетная запись будет блокирована на всё время до тех пор, пока администратор не разблокирует её явным образом. Если пороговое значение блокировки определено, данный интервал блокировки должен быть больше или равен интервалу сброса.
Сброс счетчика блокировки через	Определяет число минут, которые должны пройти после неудачной попытки входа в систему, прежде чем счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99999 минут. Если определено пороговое значение блокировки, данный интервал сброса не должен быть больше интервала Блокировка учетной записи на.

14. Ознакомитесь со свойствами всех параметров.
15. Для изменения параметров воспользуйтесь алгоритмом, описанным в пунктах 8-10.

Задания для самостоятельной работы:

1. Измените параметр «**Пароль должен отвечать требованиям сложности**» **Политики паролей** на «**Включен**» (рисунок 3) и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения Вашего задания.
2. После успешного выполнения первого задания, измените пароль Вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.
3. Проведите эксперименты с другими параметрами **Политики учетных записей.**

Контрольные вопросы:

1. Что такое аутентификация и идентификация?
2. Для чего применяются эти механизмы?
3. Что можно настроить с помощью вкладки **Локальные политики безопасности**?

Лабораторная работа
Шифрующая файловая система EFS и управление сертификатами

Цель работы: Познакомиться с механизмами управления шифрованием файлов шифрующей файловой системой EFS.

Краткие теоретические сведения:

Шифрующая файловая система EFS позволяет пользователям хранить данные на диске в зашифрованном виде.

Шифрование – это процесс преобразования данных в формат не доступный для чтения другими пользователями. После того как файл будет зашифрован, он автоматически остаётся зашифрованным в любом месте хранения, на любом диске.

Расшифровка – это процесс преобразования данных из зашифрованной формы в исходный формат. При работе с шифрующей файловой системой EFS следует учитывать следующие требования и рекомендации.

1. Могут быть зашифрованы только файлы и папки, находящиеся на томах NTFS.
2. Сжатые файлы и папки не могут быть зашифрованы. Если шифрование выполняется для сжатого файла или папки, файл или папка преобразуются к состоянию без сжатия.
3. Зашифрованные файлы могут стать расшифрованными, если файл копируется или перемещается на том, не являющийся томом **NTFS.**
4. При перемещении незашифрованных файлов в зашифрованную папку они автоматически шифруются в новой папке. Однако обратная операция не приведет к автоматической расшифровке файлов. Файлы необходимо явно расшифровать.
5. Не могут быть зашифрованы файлы с атрибутом **«Системный»** и файлы в структуре папок системный корневой каталог.
6. Шифрование файла или папки не защищает их от удаления. Любой пользователь, имеющий права на удаление, может удалить зашифрованные файлы или папки.
7. Процесс шифрования является прозрачным для пользователя.

Примечание: *Прозрачное шифрование означает, что перед использованием файл не нужно расшифровывать. Можно как обычно открыть файл и изменить его. В системах прозрачного шифрования (шифрования «на лету») криптографические преобразования осуществляются в режиме реального времени незаметно для пользователя. Например, пользователь записывает подготовленный в текстовом редакторе документ на защищенный диск, а система защиты в процессе записи выполняет его шифрование.*

Использование EFS сходно с использованием расширений для файлов и папок. Оба метода используются для ограничения доступа к данным. Но злоумышленник, получивший несанкционированный физический доступ к зашифрованным файлам и папкам, не сможет их прочитать. При попытке открыть или скопировать зашифрованный файл или папку появится сообщение, что доступа нет.

Шифрование и расшифровывание файлов выполняется установкой свойств шифрования для папок и файлов, как устанавливаются другие атрибуты, например, **«только чтение», «сжатый»** или **«скрытый».** Если шифруется папка, все файлы и подпапки, созданные в зашифрованной папке автоматически шифруются. Рекомендуется использовать шифрование на уровне папки. Шифрующая файловая система использует алгоритм шифрования Data Encryption Standard (DESX).

Задание: Включить и отключить шифрование файлов шифрующей файловой системой EFS. Экспортировать сертификат с ключами для расшифровки файлов на другом компьютере.

Алгоритм выполнения работы:

a. Для включения режима шифрования выполните следующие действия.

1. Укажите файл или папку (например, создайте файл шифр.doc в папке Мои документы), которую требуется зашифровать, нажмите правую кнопку мыши и выберите в контекстном меню команду **Свойства.**
2. В появившемся окне свойств на вкладке Общие нажмите кнопку Другие. Появится окно диалога Дополнительные атрибуты.
3. В группе **Атрибуты сжатия и шифрования** установите флажок **Шифровать содержимое для защиты данных** и нажмите кнопку «**Ок**».
4. Нажмите кнопку ОК в окне свойств зашифровываемого файла или папки, в появившемся окне диалога укажите режим шифрования: **только к этой папке или к этой папке и всем вложенным папкам и файлам.**

Внимание! *После выполнения этих действий файл с Вашей информацией будет автоматически зашифровываться. Просмотр его на другой ПЭВМ будет невозможен.*

b. Для выключения режима шифрования выполните следующие действия.

1. Выделите файл шифр.doc в папке **Мои документы**.
2. Нажмите правую кнопку мыши и выберите пункт **Свойства.**
3. На вкладке **Общие** нажмите кнопку **Другие.**

4. В открывшемся окне диалога в группе атрибуты сжатия и шифрования сбросьте флажок **Шифровать содержимое для защиты данных**.

Внимание! *После Выполнения тих действий файл с Вашей информацией не будет зашифровываться.*

c. Создание резервной копии Сертификата средствами ОС Windows XP.

Примечание: *Резервная копия сертификата необходима для расшифровки данных после переустановки операционной системы или для просмотра зашифрованной информации на другой ПЭВМ.*

Для создания резервной копии сертификата выполните следующие действия.

1. Выберите кнопку Пуск в панели задач.
2. Перейдите к вкладке Выполнить.
3. В открывшемся окне в поле ввода введите команду **mmc.**
4. В результате откроется консоль управления **mmc.**

Примечание: *Консоль ММС – это средство для создания, сохранения и открытия наборов средств администрирования, называемых консолями. Консоли содержат такие элементы, как оснастки, расширения оснасток, элементы управления , задачи, мастера и документацию, необходимые для управления многими аппаратными, программными и сетевыми компонентами системы Windows.Можно добавлять элементы в существующую консоль ММС, а можно создавать новые консоли и настраивать их для управления конкретными компонентами системы.*

5. В меню консоль выберите команду **Добавить или удалить оснастку** (рис. 1) и нажмите кнопку **Добавить.**

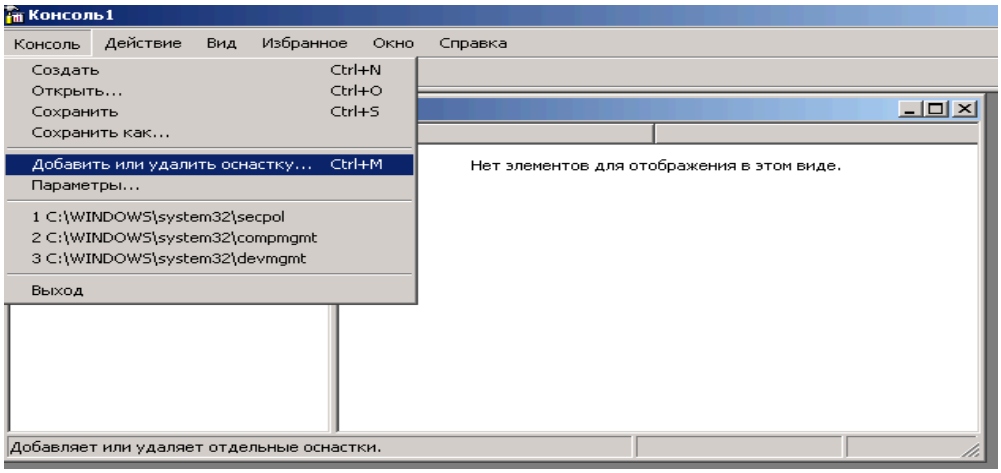


Рис. 1

6. В поле **Оснастка** дважды щелкните **Сертификаты** (рис. 2), установите переключатель в положение **учетной записи компьютера** и нажмите кнопку **Далее.**

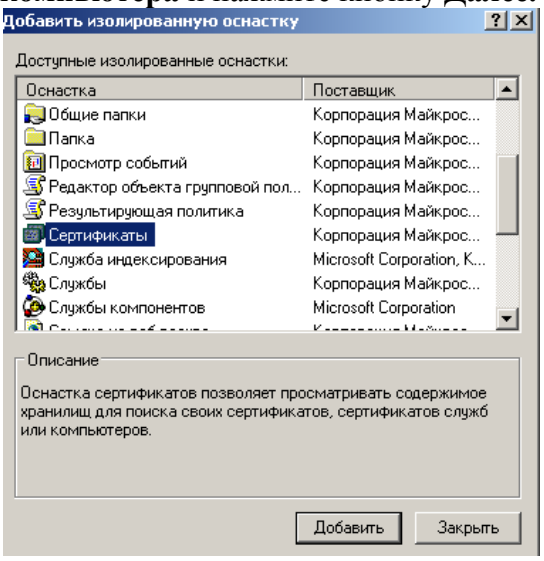


Рис. 2

7. Выполните одно из следующих действий.

- Чтобы управлять сертификатами локального компьютера, установите переключатель в положение **локальным компьютером** и нажмите кнопку **Готово.**
- Чтобы управлять сертификатами удаленного компьютера, установите переключатель в положение **другим компьютером** и введите имя компьютера или нажмите кнопку **Обзор** для выбора компьютера, затем нажмите кнопку **Готово**.

8. Нажмите кнопку **Закрыть.**
9. В списке выбранных оснасток для новой консоли появиться элемент **Сертификаты** (имя_компьютера).
10. Если на консоль не нужно добавлять другие оснастки, нажмите кнопку **ОК.**
11. Чтобы сохранить эту консоль, в меню **Консоль** выберите команду **Сохранить** и укажите имя оснастки **Сертификаты.**
12. Закройте окно **Консоли** и выберите команду **Пуск** и далее **Все программы.**
13. Найдите пункт **Администрирование** и выберите подпункт **Сертификаты** (теперь оснастка с **Сертификатами** доступна в меню **Пуск**).
14. В левом подокне оснастки Сертификаты откройте папку Доверенные коренные сертификаты, а затем папку Сертификаты. В правом подокне появиться список сертификатов.
15. Укажите переносимый сертификат (например, первый в списке, рис. 3) и щелкните правой кнопкой мыши . В появившемся контекстном меню выберите команду Все задачи и далее выберите команду **Экспорт.**
16. В результате запустится **Мастер экспорта сертификатов** (рис. 4).
17. Нажмите кнопку Далее.
18. В следующем окне мастера выберите опцию **Да,** экспортировать закрытый ключ.
19. Затем нажмите кнопку **Далее.**
20. В следующем окне мастера доступен только один формат (PFX), предназначенный для персонального обмена информацией. Нажмите кнопку **Далее**.

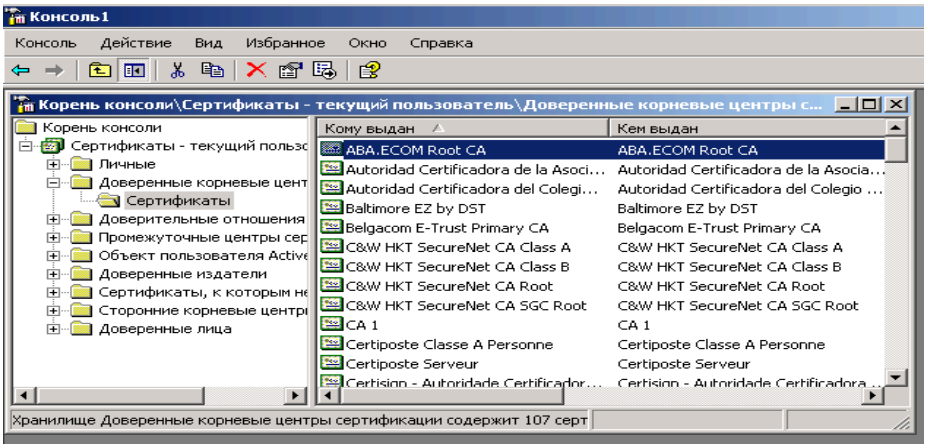


Рис. 3

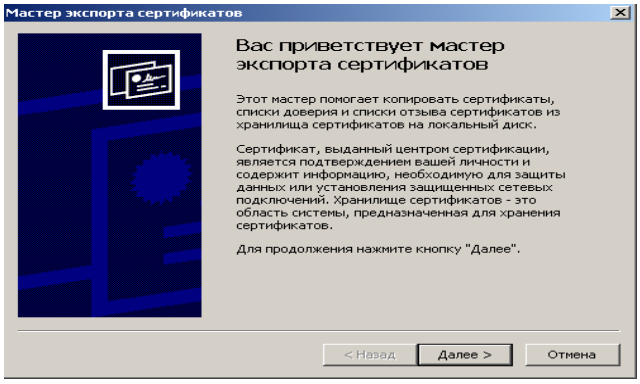


Рис. 4

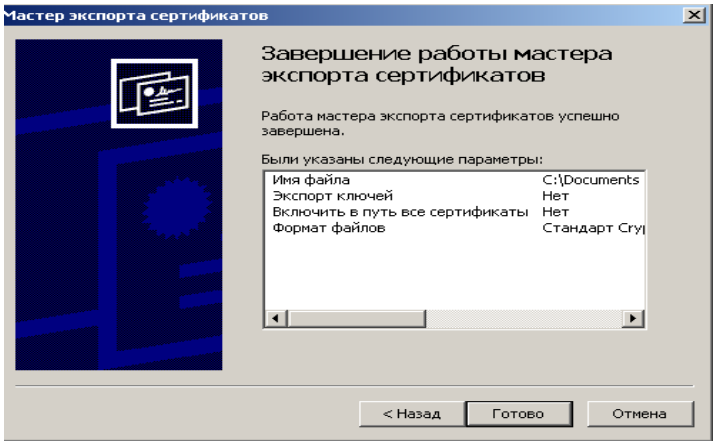


Рис. 5

21. В следующих окнах сообщите пароль (например 11), защищающий данные файла сертификат.pfx, а также путь сохранения файла (запишите путь к папке, в которой Вы сохранили копию сертификата) сертификат. Pfx.
22. Нажмите кнопку **Далее.**
23. Отобразиться список экспортируемых ключей и сертификатов. Нажмите кнопку **Готово** (рис. 5).
24. Завершите работу Мастера экспорта сертификата нажатием кнопки **ОК** в окне диалога, сообщением об успешном выполнении процедуры экспорта. В результате сертификат и секретный ключ будут экспортированы в файл с расширением сертификат.pfx, который может быть скопирован на гибкий диск и перенесен на другой компьютер или использован после переустановки операционной системы.

d. **Для восстановления сертификата из резервной копии выполните следующие действия.**

1. Перенесите созданный на предыдущем этапе файл с расширением сертификат.pfx на компьютер (**Вам необходимо вспомнить путь к копии Сертификата**).
2. Запустите оснастку сертификаты, для этого выберите кнопку **Пуск** панели задач и далее **Все программы/Администрирование/Сертификаты**.
3. В окне структуры оснастки **Сертификаты** откройте папку **Доверенные корневые сертификаты**, затем папку **Сертификаты**. В правом подокне появиться список Ваших сертификатов.
4. Щелкните правой кнопкой мыши на пустом месте правого подокна.
5. В появившемся контекстном меню выберите команду **Все задачи.**
6. В её подменю выберите команду **Импорт.**
7. Запуститься **Мастер импорта** сертификатов.
8. Следуйте указаниям мастера – укажите местоположение файла сертификат.pfx и сообщите пароль защиты данного файла.
9. Для начала операции импорта нажмите кнопки **Готово** и **ОК.**
10. После завершения процедуры импорта нажмите кнопку **ОК** и закройте окно **Мастера импорта**. В результате Ваших действий текущий пользователь или Вы сами получите возможность работать с зашифрованными данными на этом компьютере.

Задания для самостоятельной работы:

1. Экспортируйте сертификат №2 из папки **Промежуточные центры сертификации Root Agency** (сохраните иллюстрации для отчета).
2. Импортируйте экспортированный сертификат в папку **Личные** (сохраните иллюстрации для отчета).

Контрольные вопросы:

1. Что входит в криптосистему?
2. Сравните методы шифрования с открытым и закрытым ключом (симметричное и асимметричное шифрование).
3. Что такое mmc?
4. Назначение файловой системы EFS.

Лабораторная работа
Назначение прав пользователей при произвольном управлении доступом

Цель работы: Научиться создавать учетные записи пользователей, локальных групп, блокировать учетные записи пользователей и.т.д.

Краткие теоретические сведения:

После выполнения аутентификации идентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы. Обычно полномочия субъектов представляются списком ресурсов, доступным пользователю и правами по доступу к каждому ресурсу из списка.

При разграничении доступа по спискам задаются соответствия: каждому пользователю – список ресурсов и прав доступа к ним или каждому ресурсу – список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Задание: Создать учетную запись и локальную группу, изменить принадлежность пользователя к локальной группе и блокировать учетную запись.

Алгоритм выполнения работы:

A. **Создание учетной записи**.

1. Откройте оснастку **Настройка** – **Панель управления** – **Администрирование** (рис. 1) – **Управление компьютером** (рис. 2).

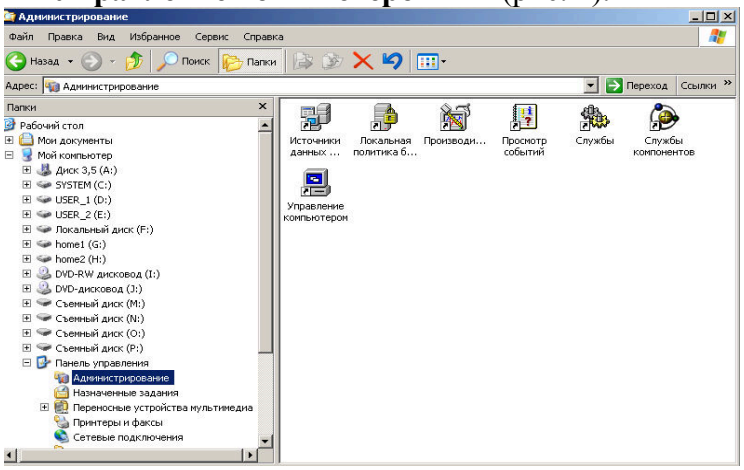


Рис. 1

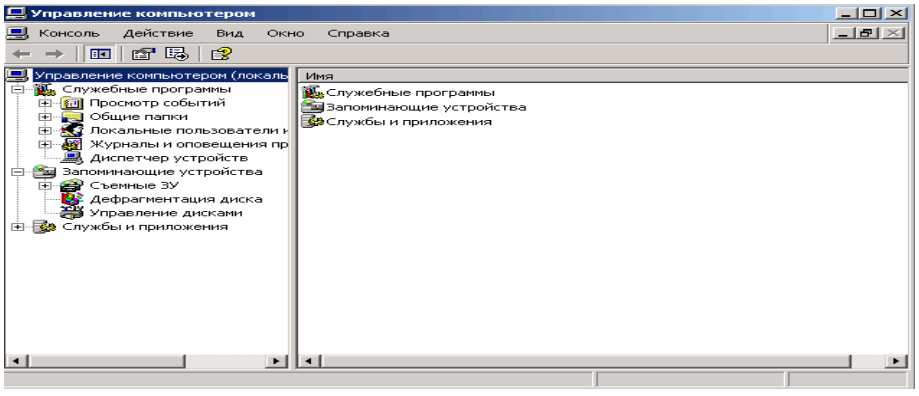


Рис. 2

2. В оснастке **Локальные пользователи и группы** установите указатель мыши на папку Пользователи и нажмите правую кнопку.
3. В появившемся контекстном меню выберите команду **Новый пользователь** (рис. 3). Появиться окно диалога **Новый пользователь** (рис. 4).

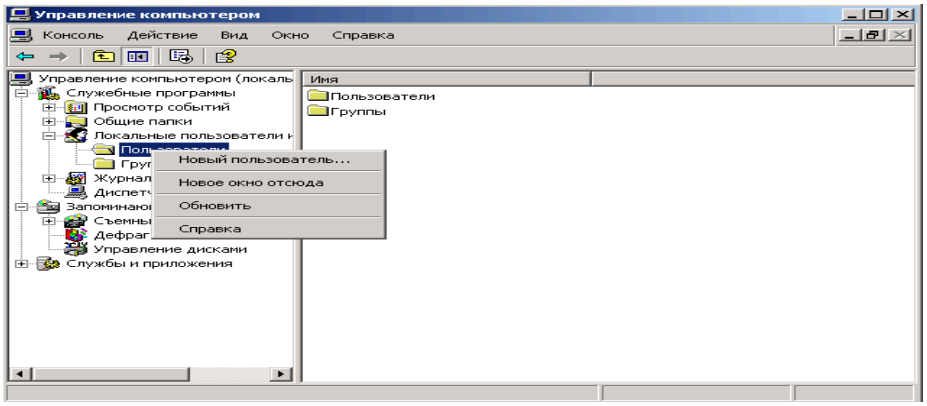


Рис. 3

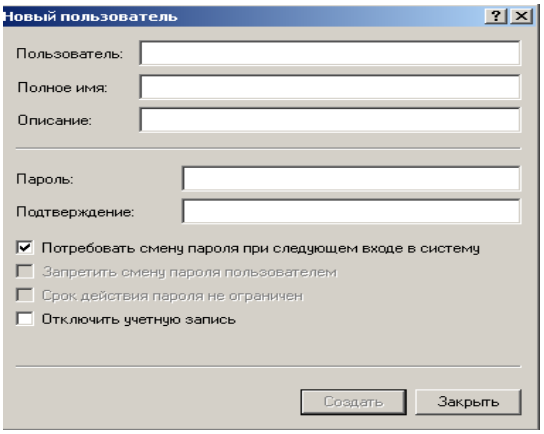


Рис. 4

4. В поле **Пользователь** введите имя создаваемого пользователя, например, свою фамилию.

Примечание: Имя пользователя должно быть уникальным для компьютера. Оно может содержать до 20 символов верхнего и нижнего регистра. Ниже приведены символы, применение которых в имени пользователя недопустимо:*[];:=.,<>? Имя пользователя не может состоять целиком из точек и пробелов.

5. В поле **Полное имя** введите полное имя создаваемого пользователя.
6. В поле **Описание** введите описание создаваемого пользователя или учетной записи, например, «*студент ……*».
7. В поле **Пароль** введите пароль пользователя и в поле **Подтверждение** подтвердите его правильность вторичным вводом.

Примечание: Длина пароля не может превышать 14 символов.

8. Установите или снимите флажки:
    - Потребовать смену пароля при следующем входе в систему
    - Запретить смену пароля пользователем
    - Срок действия пароля не ограничен
    - Отключить учетную запись
9. Чтобы создать ещё одного пользователя, нажмите кнопку **Создать** и повторите шаги с 1 по 8. Для завершения работы нажмите кнопку **Создать** и затем **Закрыть**.

B. Создание локальной группы.

1. В окне оснастки **Локальные пользователи и группы** установите указатель мыши на папке **Группы** и нажмите правую кнопку.
2. В появившемся контекстном меню выберите команду **Новая группа**.
3. В поле **Имя группы** (рис. 5) введите имя новой группы, например, **Студенты.**

Примечание: Имя локальной группы должно быть уникальным. Оно сможет содержать до 256 символов в верхнем и нижнем регистрах.

4. В поле **Описание** введите описание новой группы.
5. В поле **Члены группы** можно сразу добавить пользователей и группы, которые войдут в новую группу: для этого нужно нажать кнопку **Добавить** и выбрать их в списке. Для завершения нажмите кнопку **Создать** и затем **Закрыть**.

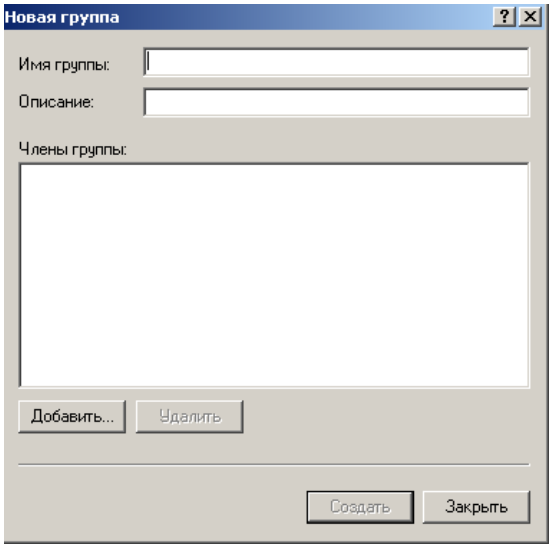


Рис. 5

C. **Изменение членства в локальной группе**.

1. В окне оснастки **Локальные пользователи и группы** щелкните на папке **Группы.**
2. В правом подокне установите указатель мыши на модифицируемую группу и нажмите правую кнопку.
3. В появившемся контекстном меню выберите команду **Добавить** в группу или Свойства.
4. Для того чтобы добавить новые учетные записи в группу, нажмите кнопку **Добавить** (рис. 6)

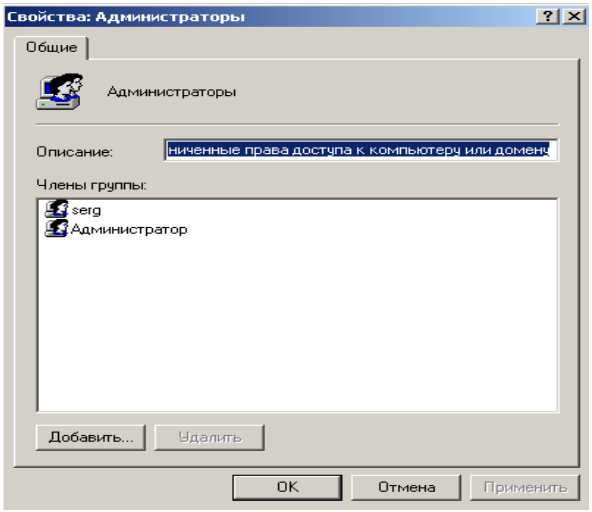


Рис. 6

5. Далее следуйте указателям окна диалога **Выбор: Пользователи или группы.**
6. Для того, чтобы удалить из группы некоторых пользователей, в поле **Члены группы** (рис. 6) окна свойств группы выберите одну или несколько учетных записей и нажмите кнопку **Удалить.**

Примечание*: В локальную группу можно добавлять как локальных пользователей, созданных на компьютере, так и пользователей и локальные группы, созданные в домене, к которому принадлежит компьютер, или в доверяемых доменах. Встроенные группы не могут быть удалены. Удаленные группы не могут быть восстановлены. Удаление группы не отражается на входящих в неё пользователей.*

D. **Временная блокировка учетной записи.**

1. Откройте оснастку **Управление компьютером.**
2. Для этого либо выберите на **Рабочем столе** ярлык **Мой компьютер** и нажмите правую кнопку мыши, после этого выберите пункт контекстного меню **Управление**, либо воспользуйтесь разделом **Администрирование в Панели управления**.
3. В открывшейся оснастке выберите пункты **Служебные программы/Локальные пользователи и группы** (рис. 3).
4. Откройте папку пользователи и выберите учетную запись **Гость.**

5. Нажмите правую кнопку мыши и выберите пункт свойства.
6. В открывшемся окне снимите отметку пункта **Отключить** учетную запись (рис. 7).
7. Нажмите кнопку **ОК** и сделайте вывод о состоянии учетной записи.
8. Выполните пункт 5 и отметьте пункт **Отключить учетную запись**.

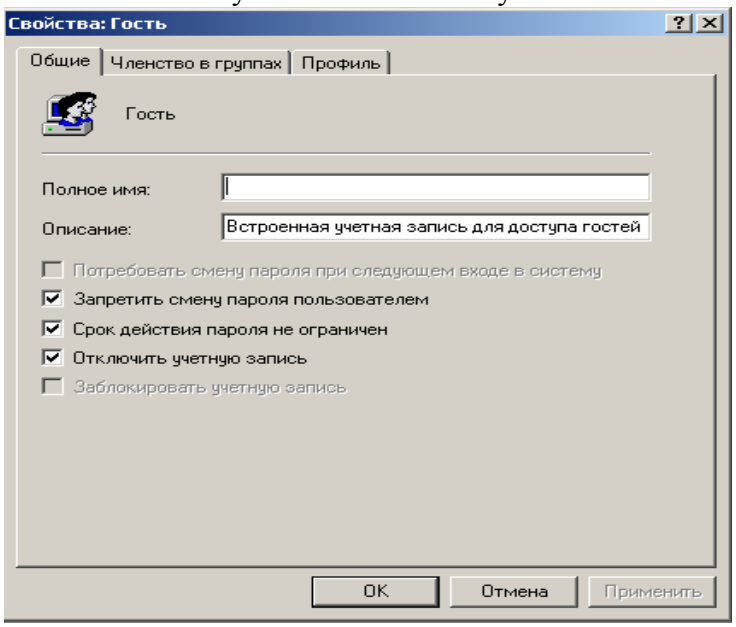


Рис. 7

Задание для самостоятельной работы:

1. Создайте учетную запись с именем ПЗ-6, используя команду Print Screen клавиатуры, сохраните копию экрана со списком пользователей Вашего компьютера(для чего после нажатия клавиши Print Screen вставьте скопированное изображение в новый документ Word) для представления в качестве отчета.
2. Создайте группу **Информационная безопасность** и, как в первом задании, сохраните окно со списком групп Вашего компьютера для отчета.
3. Заблокируйте учетную запись ПЗ-6 и после этого удалитею

Контрольные вопросы:

1. Какие методы управления доступом Вам известны?
2. Чем отличается мандатное управление доступом от дискретного?
3. Допустимо ли имя пользователя П38/44? Почему?

Лабораторная работа

Тема: Использование прикладного протокола FTP

Цели работы: научиться осуществлять поиск FTP-ресурсов с помощью специальных списков размещенных в сети, получать доступ к FTP ресурсам через Web – браузер и специализированный FTP-клиент, организовывать пересылку файлов на FTP-сервер.

Теоретическая часть

FTP (File Transfer Protocol– протокол передачи файлов) – один из первых прикладных протоколов для обмена данными между компьютерами.

Для хранения файлов в Интернет используются специальные FTP-серверы. Многие серверы открыты для свободного доступа, их часто называют анонимными. Другие доступны только для ограниченного круга зарегистрированных пользователей и требуют при подключении ввода идентификатора (*login* – входное имя) и пароля (*password*).

Первые клиентские FTP-приложения были интерактивными инструментами командной строки, реализующими стандартные команды и синтаксис. Графические пользовательские интерфейсы с тех пор были разработаны для многих используемых по сей день операционных

систем. Среди этих интерфейсов как программы общего веб-дизайна вроде Microsoft Expression Web, так и специализированные FTP-клиенты (например, FileZilla).

Сейчас большинство Web-Браузеров обеспечивают доступ к FTP-серверам без использования специальных программ – FTP-клиентов. Установка связи с FTP-сервером происходит точно так же, как и установка связи с сайтом HTTP, только вместо префикса http:// в поле ввода адреса нужно напечатать префикс ftp://.

Ход работы

1. Поиск FTP-ресурсов.

1.1. С помощью поисковой машины в сети Internet найдите каталоги FTP-ресурсов.

1.2. В каталоге FTP-ресурсов, расположенному по адресу _____ _____ найдите анонимный FTP – сервер на котором находятся дистрибутив FTP-клиента FileZilla.

2. Работа с FTP - сервером через web – браузер.

2.1. Запустите web – браузер. В адресной строке введите адрес, найденного FTP-сервера ftp:// _____.

2.2. Запишите иерархическую структуру публичной части FTP – сервера:

_____
_____
_____
_____
_____

1.1. Скачайте дистрибутив FileZilla. Установите данное программное обеспечение.

1.2. Для пересылки своего файла на FTP-сервер, если у Вас есть на это права, можно воспользоваться приемом буксировки файла из окна Проводника на своем компьютере в окно Браузера, настроенного на нужную папку FTP-сервера. Перешлите любой свой файл на анонимный FTP-сервер.

2. Доступ к FTP – специализированный FTP-клиент.

2.1. Запустите FileZilla и произведите те же действия, что и в Web-браузере.

2.2. Запишите последовательность действий:

_____
_____
_____
_____
_____
_____

Вывод:

_____
_____
_____
_____.

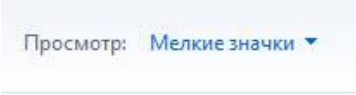
Лабораторная работа

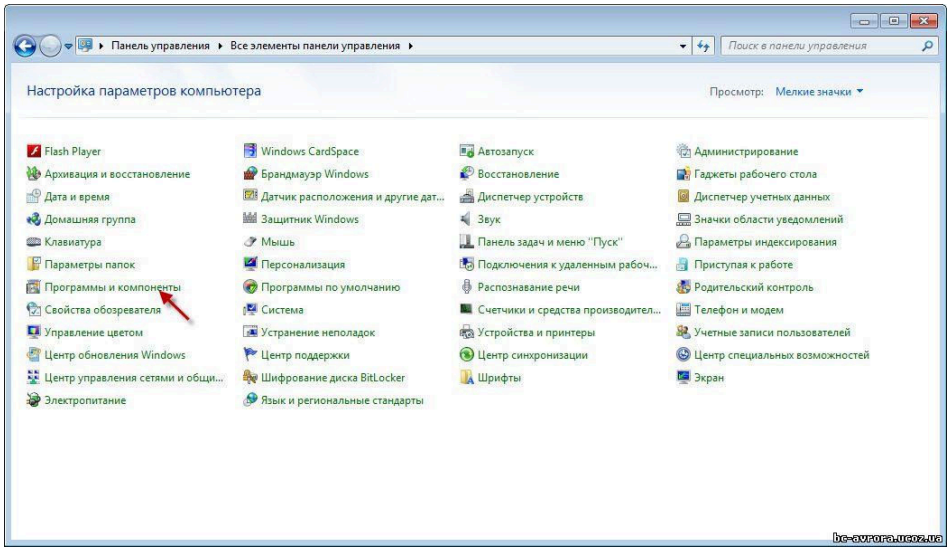
Тема: Анализ пакетов протокола FTP**.**

Цели работы: научиться создавать FTP-сервер, анализировать его состояние и администрировать его.

Ход работы

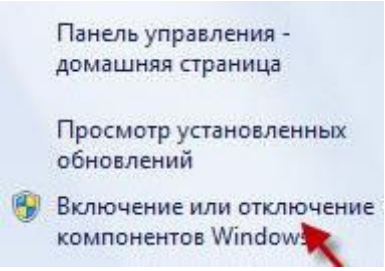
Переходим в Пуск>Панель управления
В Просмотр выбираем "Мелкие значки"

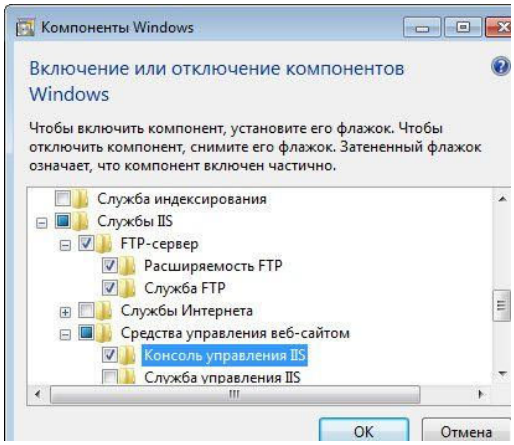




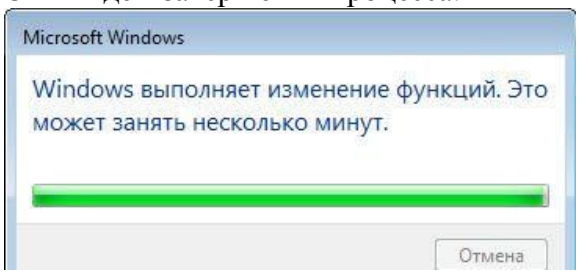
Далее выбираем "Программы и компоненты"

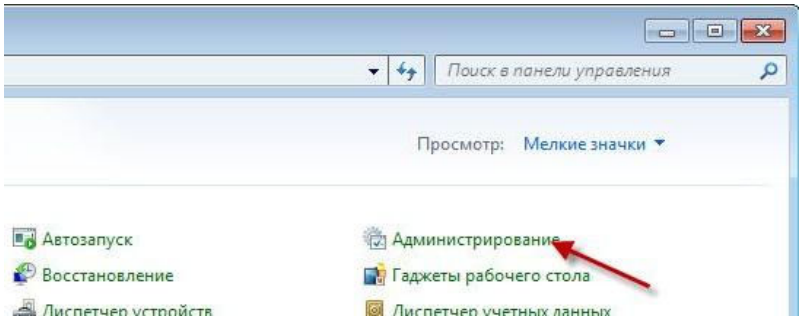
Выбираем "Включение или отключение компонентов Windows"



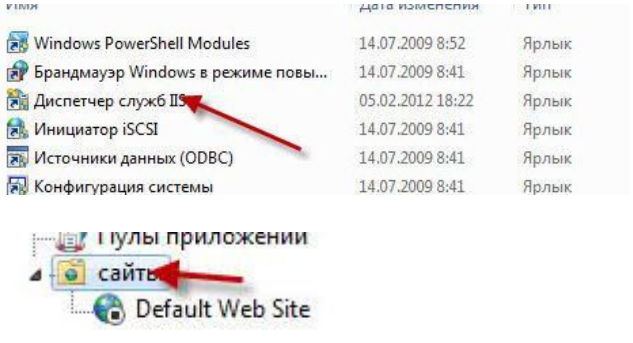


Выбираем "Расширяемость FTP", "Служба FTP" и "Консоль управления IIS". Нажимаем ОК и ждем завершения процесса.

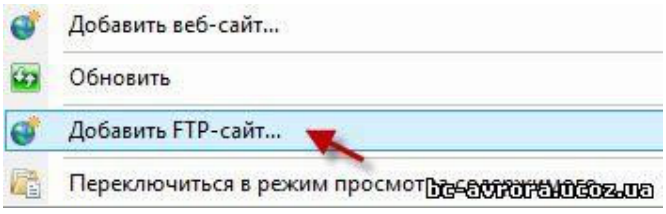


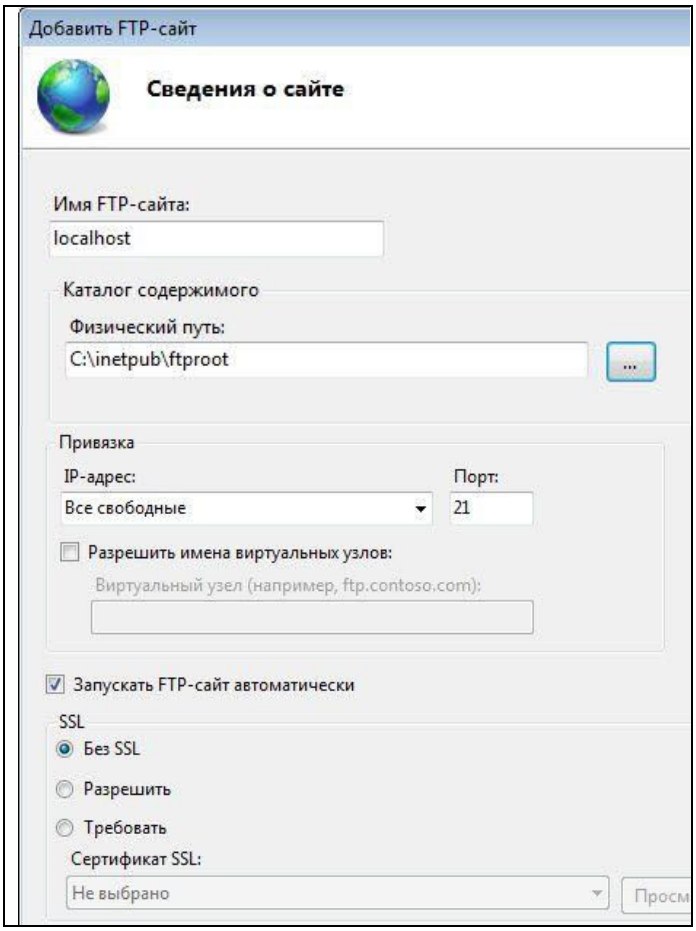


Переходим в Панель управления>Администрирование



Выбираем "Диспетчер служб IIS" Нажимаем правую кнопку мыши и в выпадающем меню выбираем "Добавить FTP сайт"

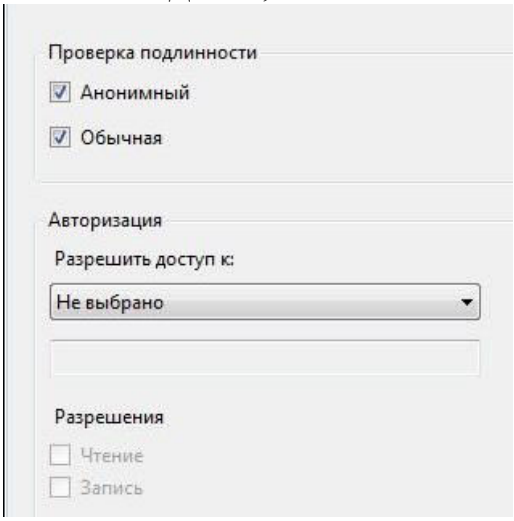




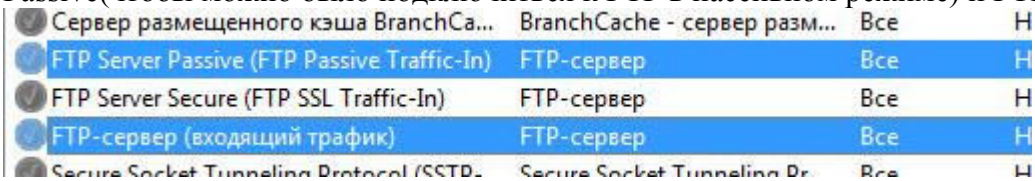
Указываем название сайта и расположение (по умолчанию "C:\inetpub\ftproot")

Нажимаем "Далее". Указываем параметры запуска FTP ("Если вам не нужен автоматический запуск FTP, снимите галочку "Запускать FTP сайт автоматически"").
В разделе "SSL" устанавливаем "Без SSL"

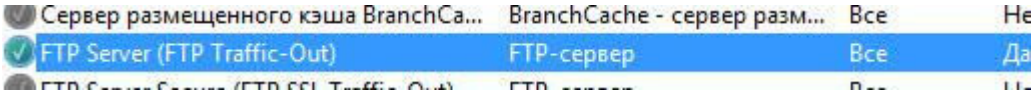
Нажимаем "Далее", потом "Готово".



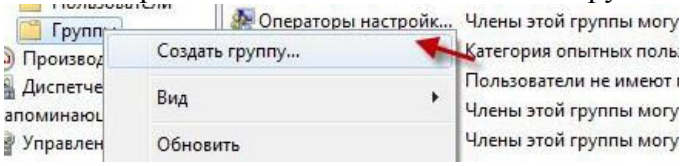
Сайт создан. Далее переходим в Панель управления>Брандмауэр>Дополнительные параметры>Правила для входящих соединений. Выбираем и активируем пункты FTP Server Passive(чтобы можно было подключиться к FTP в пассивном режиме) и FTP сервер.



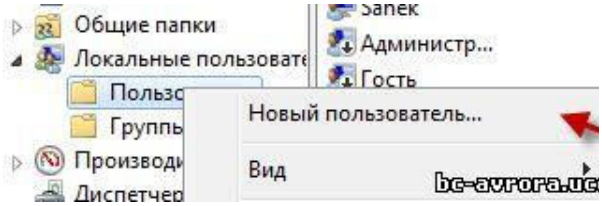
Переходим в раздел "Правила для исходящих соединений" и активируем пункт "FTP Server"



Далее переходим Панель управления>Администрирование>Управление компьютером>Локальные пользователи>Группы>(правая кнопка мыши)>Создать группу

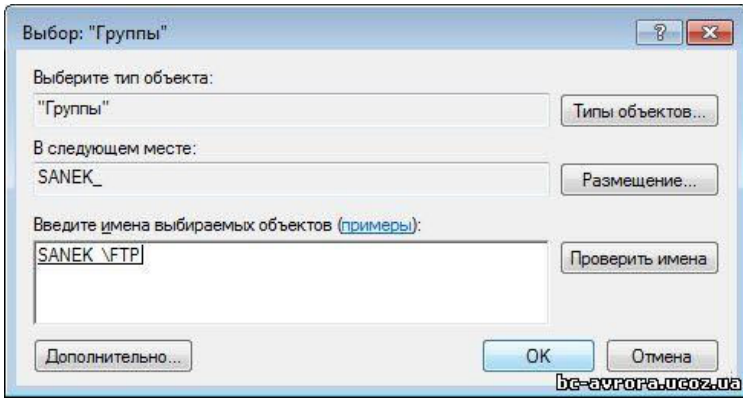


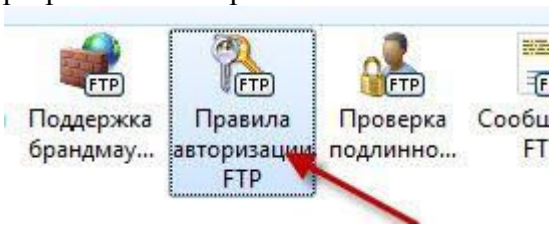
Указываем название группы "FTP" и нажимаем "Создать".



Далее переходим в Пользователи. Клик правой кнопкой мыши>Новый пользователь
Указываем имя пользователя, пароль (не менее 8 символов). Устанавливаем галочки напротив "Запретить смену пароля пользователем" и "Срок действия пароля неограничен". Нажимаем создать

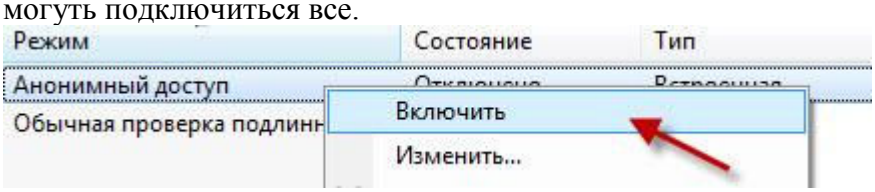
Далее выбираем пользователя, правый клик мыши, "Свойства", "Членство в группах". Нажимаем "Добавить" и выбираем группу "FTP", нажимаем "ОК". Еще раз нажимаем "ОК".
Переходим в каталог, который мы указали для FTP сервера (смотри "Указываем название сайта и расположение"). Правая кнопка мыши> Свойства> Безопасность> Изменить. Далее "Добавить", указываем название группы и "ОК". Устанавливаем разрешения "Разрешить все"

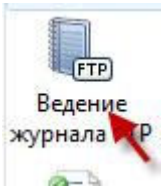




Переходим в Панель управления > Администрирование > Диспетчер служб IIS и выбираем наш FTP.
Переходим в "Правила авторизации FTP". Выбираем "Добавить разрешающее правило" и указываем нашу группу "FTP". Ставим галочки напротив "Чтение" и "Запись". Нажимаем "ОК"
Если хотите разрешить доступ всем пользователям, снова "Добавить разрешающее правило" и указываем "Все анонимные пользователи". Устанавливаем галочку только напротив "Чтение"!
Переходим в "Проверка подлинности FTP"

Выбираем "Анонимный доступ", правая кнопка мыши, "Включить". Теперь к FTP серверу могуть подключиться все.





Переходим в "Ведение журнала FTP". Устанавливаем максимальный размер лога или отключаем вообще.

Все. FTP сервер создан и настроен. Чтобы проверить его функционирование, используйте любой FTP клиент (например FileZilla).

Лабораторная работа
Система безопасности Microsoft SQL Server

Цель: научить использовать системные хранимые процедуры для управления именами входа MS SQL Server и пользователями баз данных, а также разрешать и запрещать выполнение определенных действий некоторому пользователю.

Теоретический материал: перед выполнением лабораторной работы рекомендуется изучить лекцию №6 «Система безопасности в базах данных», в которой подробно рассмотрены вопросы управления учетными записями и правами пользователя.

Требования к отчету: по результатам работы представить отчёт со скриншотами, содержащими SQL-команды и результаты их выполнения для каждой задачи из раздела «Самостоятельная работа».

Задание 1. Подключитесь к серверу *MyServ* с помощью утилиты *Management Studio*.

Указания к выполнению:

1. Запустите *SQL Server Management Studio* через меню **Пуск –Программы – Microsoft SQL Server 2008**.

2. Выберите тип аутентификации: *SQL Server Authentication*. Укажите *User name*: ***sa,*** и *Password*: пустой и нажмите кнопку **Connect**.

Задание 2. Определите список ролей сервера.

Указания к выполнению:

1. Создайте новый запрос или через команду меню **File – New – Query with Current Connection** или при помощи кнопки **New Query** на панели инструментов.

2. Во вкладке *SQLQuery1.sql* выполните команду **sp_helpsrvrole** (см. рис. 5.1).

Results | Messages

	ServerRole	Description
1	sysadmin	System Administrators
2	securityadmin	Security Administrators
3	serveradmin	Server Administrators
4	setupadmin	Setup Administrators
5	processadmin	Process Administrators
6	diskadmin	Disk Administrators
7	dbcreator	Database Creators
8	bulkadmin	Bulk Insert Administrators

Рис. 5.1. Серверные роли MS SQL Server

Замечание. Для более наглядного представления данных используйте способ отображения информации в виде таблицы (кнопки **Results to Grid/Results to Text** на панели инструментов или через команды меню **Query – Results To**).

Задание 3. Создайте и настройте новую учетную запись *TempUser* для входа в SQL Server.

Указания к выполнению:

1. Для добавления учетной записи используйте хранимую процедуру **sp_addlogin:**

sp_addlogin 'TempUser', 'Password!'

Замечание. Для получения справки по командам Transact-SQL и хранимым процедурам можно воспользоваться утилитой *SQL Server Management Studio*. Для этого необходимо выделить имя оператора и нажать клавишу **F1**.

2. Убедитесь, что учетная запись была добавлена при помощи хранимой процедуры **sp_helplogins** (см. рис. 5.2).

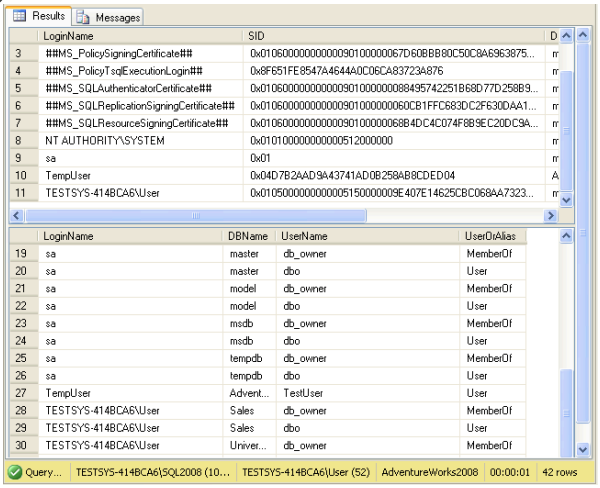


Рис. 5.2. Список имен пользователей MS SQL Server

3. Попробуйте войти на сервер под созданной учетной записью.

4. Зайдите снова под учетной записью **sa**, т.к. для дальнейших действий снова потребуются права администратора.

5. Для присвоения учетной записи для входа встроенной серверной роли используется процедура:

sp_addsrvrolemember ‘TempUser’, ‘securityadmin’

Задание 4. Определите список ролей базы данных *AdventureWorks2008* и членов роли *db_owner*.

Указания к выполнению:

1. Выполните хранимую процедуру **sp_helprole** для получения списка как встроенных, так и определенных пользователем ролей базы данных.

2. При помощи команды **sp_helprolemember ‘db_owner’** определите членов роли *db_owner* (см. рис. 5.3).

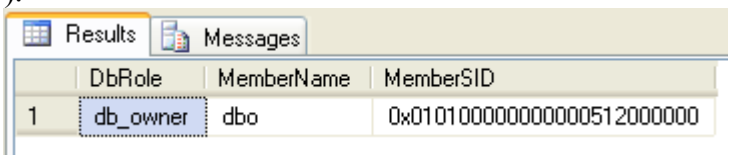


Рис. 5.3. Список членов роли *db_owner*

Задание 5. Создайте нового пользователя базы данных для логина *TempUser*.

Указания к выполнению:

1. При помощи хранимой процедуры добавьте пользователя:

sp_adduser 'TempUser', ‘MyFirstUser’

2. При помощи процедуры **sp_helpuser** убедитесь, что пользователь был добавлен. Какая роль ему была присвоена?

3. Добавьте пользователю роль *db_datareader:*

sp_addrolemember 'db_datareader, ‘MyFirstUser’

Задание 6. Настройте права доступа пользователю *Andy*: предоставьте явным образом право только для выборки из таблицы *Product* и обновления только полей *Name* и *ListPrice* этой таблицы.

Указания к выполнению:

1. С помощью следующей команды пользователю *TestUser* базы данных ***AdventureWorks2008*** предоставляются права выборки и изменения данных таблицы *Orders* этой базы данных:

GRANT select, update on AdventureWorks2008.Production.WorkOrder to TestUser

2. Следующая команда предоставляет пользователю *Andy* права только выборки данных полей *Name* и *ListPrice* таблицы *Product* базы данных ***AdventureWorks2008****:*

GRANT select on AdventureWorks2008.Production.Product (Name, ListPrice) to Andy

Задание 7. Изучите выполнение вышеупомянутых функций при помощи графического интерфейса утилиты *Management Studio*.

Указания к выполнению:

1. Просмотр списка имеющихся учетных записей и их параметров осуществляется выбором группы *Logins* в папке **Security** сервера.

2. Для создания новой учетной записи для входа необходимо выполнить команду **New Login…** контекстного меню узла **Logins,** в появившемся диалоговом окне указать:

- вкладка *General*: имя пользователя, тип аутентификации (при аутентификации средствами MS SQL Server – задать пароль), базу данных, к которой пользователь подключается автоматически, язык по умолчанию;
- вкладка *Server Roles*: роли сервера, в которые будет входить создаваемая учетная запись;
- вкладка *User Mapping*: доступ к одной из созданных на сервере базе данных, в поле *User* ввести имя пользователя базы данных и включить создаваемого пользователя в одну существующих ролей.

Замечание. Для изменения параметров существующей учетной записи пользователя для входа необходимо выбрать ее из списка и выполнить команду контекстного меню **Properties**, для удаления – **Delete.**

3. Для отображения списка ролей сервера необходимо выбрать группу *Server Roles* в папке **Security** сервера. Просмотр пользователей, входящих в эту роль и разрешений, присвоенный ей, осуществляется выполнением команды контекстного меню **Свойства.**

Замечание. Встроенные роли сервера не могут быть удалены из системы, и нельзя изменить определенные для них разрешения. Также запрещено создавать и собственные серверные роли.

4. Для просмотра и управления параметрами пользователей некоторой базы данных предназначена группа *Security/Users* этой базы. Учетные записи отображаются в поле *User Name*, а в поле *Login Name* – соответствующие им учетные записи для входа.

Для создания нового пользователя базы данных необходимо выполнить команду **New User…,** затем в поле *User name* ввести имя пользователя, а в списке *Login Name* выбрать соответствующую учетную запись для входа. Можно также включить пользователя в роли базы данных.

Замечание. Для изменения параметров учетной записи служит команда **Properties,** а для удаления – **Delete.**

5. Для отображения списка ролей базы данных используется группа *Roles*. Для просмотра пользователей, входящих в эту группу, необходимо выполнить команду **Properties.**

6. Чтобы назначить полномочия объекту безопасности необходимо выбрать его в группе *Users* (для изменения разрешения конкретного пользователя базы данных) или в группе *Roles* (для разрешений определенной роли). Для этих целей используется вкладка **Securables**.

В появившейся вкладке перечислены все объекты базы данных, с возможными правами доступа. Можно установить одно из трех состояний доступа: *предоставление* (галочка), *запрещение* (крестик) и *неявное отклонение* (пустое поле) – в соответствующем поле.

Задание 8. Отмените присвоение роли учетной записи и удалите учетную запись *TempUser*.

Указания к выполнению:

1. Отмена присвоенной пользователю роли может быть выполнена с помощью процедуры:

sp_droprolemember ‘db_datareader’, ‘MyFirstUser’

2. Для удаления пользователя БД используются процедуры:

sp_dropuser ‘MyFirstUser’

3. Отмена присвоения учетной записи определенной роли выполняется с помощью хранимой процедуры:

sp_dropsrvrolemember 'TempUser', ‘securityadmin’

4. Для удаления учетной записи выполните хранимую процедуру:

sp_droplogin 'TempUser'

Самостоятельная работа

1. Определите список всех ролей сервера и действия, разрешенные пользователям роли *dbcreator*.
2. Установите, какая серверная роль присвоена системной учетной записи ***sa***.
3. Определите, пользователь какой роли имеет возможность создания и удаления учетных записей для входа.
4. Изменение пароля учетной записи пользователя для входа выполняется с помощью процедуры *sp_password*.
5. Создайте собственную учетную запись для входа с подключением к базе данных ***AdventureWorks2008***, докажите правильность выполненных действий. Созданной учетной записи присвойте права на создание и изменение баз данных, докажите правильность выполненных действий. Подключитесь к MS SQL Server, используя созданную учетную запись, и создайте еще одну учетную запись пользователя для входа, результат объясните.
6. Создайте пользователя *manager* базы данных ***AdventureWorks2008*** на основе созданной ранее учетной записи для входа. Докажите правильность выполненных действий.
7. Пользователю *manager* присвойте роль, обладающую только возможностью просмотра содержимого базы данных ***AdventureWorks2008***.

Замечание. Для проверки правильности выполненных действий можно выполнить произвольный запрос к этой базе данных, например, отображающий содержимое таблицы *Production.WorkOrder*:

SELECT * FROM Production.WorkOrder.

8. Пользователю *manager* запретите просмотр данных БД ***AdventureWorks2008***, присвоив необходимую роль. Как доказать правильность внесенных изменений?
9. Какое количество пользователей базы данных может быть создано на основе одной учетной записи пользователя для входа? Ответ обоснуйте.
10. Средствами *SQL Server Management Studio* создайте учетную запись пользователя для входа на основе аутентификации SQL, подключающегося по умолчанию к базе данных ***AdventureWorks2008***, имеющего права серверной роли *diskadmin*.
11. Определите список пользователей, входящих в роль *diskadmin* и ее разрешения.
12. В базе данных ***AdventureWorks2008*** создайте пользователя на основе созданной ранее учетной записи для входа.
13. Для созданного ранее пользователя базы данных ***AdventureWorks2008*** определите, членом какой роли он является и каково ее назначение. Имеет ли данный пользователь право выборки данных из таблицы *Production.Product* этой базы данных? Ответ обоснуйте и проверьте, выполнив извлечение данных командой SELECT * *from Production.Product*.
14. В базе данных ***AdventureWorks2008*** создайте роль *managers*. Для этой роли определите право выборки данных из таблицы *Production.Product* базы данных ***AdventureWorks2008***. Присвойте роль *managers* созданному ранее пользователю. Имеет ли теперь этот пользователь право выборки данных? Проверьте сделанный вывод. К каким еще объектам базы данных ***AdventureWorks2008*** имеет право доступа этот пользователь? Обоснуйте и проверьте вывод.
15. Создайте пользователя, имеющего доступ к базе данных ***AdventureWorks2008*** и принадлежащего роли *clerks*. Для этой роли определите возможность выборки данных из таблицы *Production.Location* только для полей *Name* и *Availability.* Для проверки правильности выполненных действий выполните команды:
    - SELECT * *from Production.Location* – чтение данных из всех полей таблицы *Authors*;
    - SELECT *Name, Availability from Production.Location* – чтение данных таблицы *Production.Location* только из указанных полей.

Для роли *clerks* запрещена выборка данных из таблицы *Production.WorkOrder* базы данных ***AdventureWorks2008***. Пользователь *Andy* принадлежит пользовательской роли *clerks* и системной роли *db_datareader*. Может ли этот пользователь получить данные из этой таблицы

Лабораторная работа
Настройка параметров регистрации и аудита

Цель работы: Изучить механизмы аудита и регистрации ОС Windows XP.

Краткие теоретические сведения:

Регистрация является одним из механизмов обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения безопасности, фиксации всех событий, касающихся безопасности. Эффективность системы безопасности существенно повышается в случае дополнения механизма регистрации механизмом аудита. Это позволяет оперативно выявлять нарушения и слабые места в системе защиты, анализировать работу системы, выявлять различные нарушения, оценивать работу пользователей и.т.д.

Аудит- Это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, один раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Практическими средствами аудита являются:

- Различные системные утилиты и прикладные программы
- Регистрационный (системный или контрольный) журнал.

Первое средство обычно является дополнением к мониторингу, осуществляемому администратором систем. Комплексный подход к протоколированию и аудиту обеспечивается при использовании регистрационного журнала.

Регистрационный журнал – это хронологически упорядоченная совокупность записей результатов деятельности объектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакциях с целью контроля конечных результатов.

Задание:

Активизировать механизмы регистрации и аудита ОС Windows XP, настроить параметры просмотра аудита папок и файлов.

Алгоритм выполнения работы:

А. Активизация механизма регистрации и аудита с помощью оснастки Локальные политики безопасности.

1. Выберите кнопку **Пуск** панели задач.
2. Откройте меню **Настроить/Панель управления**.
3. В открывшемся окне выберите ярлык **Администрирование/Локальная политика безопасности.**
4. Выберите пункт **Политика аудита** (рис. 1).
5. Для включения/отключения параметров аудита выберите требуемый параметр и дважды щелкните левой клавишей мышки.
6. Для каждого параметра можно задать аудит успехов или отказов, либо вообще отключить аудит данного типа (рис. 2).
7. Значения параметров аудита приведены в таблице №1.
8. По умолчанию все параметры политики аудита выключены.
9. Включите аудит успеха и отказа для всех параметров.
10. Для этого выполните пункт 5.
11. Нажмите кнопку **ОК.**

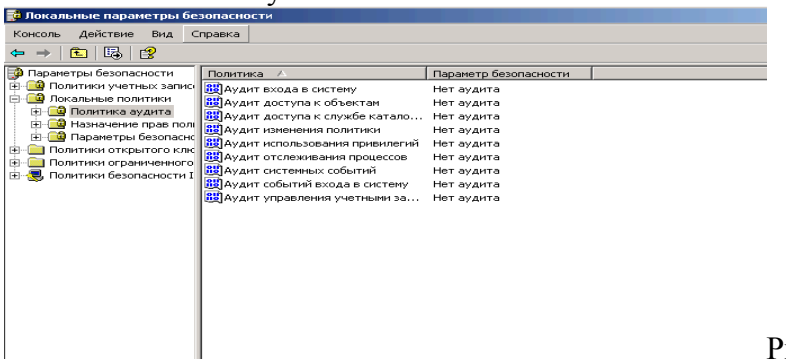


Рис. 1

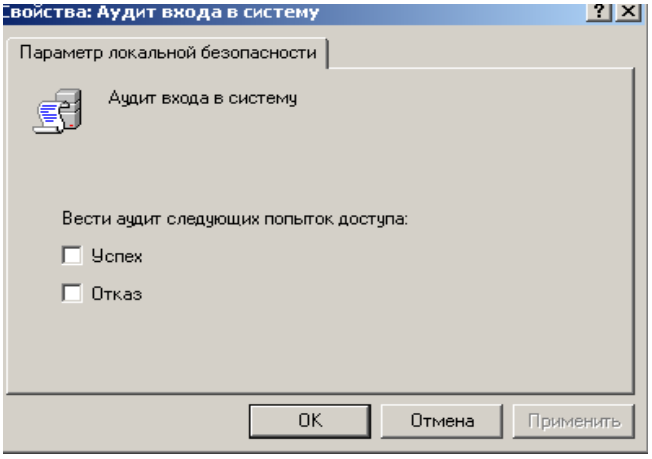


Рис. 2

Таблица №1

Значения параметров аудита системы

Параметр	Значение
Аудит событий Входа в систему	Определяет, подлежит ли аудиту каждая попытка пользователя войти в систему или выйти из неё на другом компьютере при условии, что данный компьютер используется для проверки подлинности учетной записи. Если этот параметр политики определен, можно задать аудит успехов или отказов, либо вообще отключить аудит событий данного типа. Аудит успехов означает создание записей аудита для каждой неудачной попытки входа в систему.
Аудит управления Учетными записями	Определяет подлежат ли аудиту все события, связанные с управлением учетными записями на компьютере. К таким событиям относятся следующие события: • Создание, изменение или удаление учетной записи пользователя или группы • Переименование, отключение или включение учетной записи пользователя • Задание или изменение пароля.
Параметр	Значение
Аудит доступа к службе каталогов	Определяет, подлежит ли аудиту событие доступа пользователя к объекту каталога Active Directory, для которого задана собственная системная таблица управления доступом.
Аудит входа в систему	Определяет, подлежит ли аудиту каждая попытка пользователя войти в систему либо выйти из неё на данном компьютере, или подключиться к нему через сеть.
Аудит доступа к объектам	Определяет, подлежит ли аудиту событие доступа пользователя к объекту – например, к файлу папке, разделу реестра, принтеру и т.п. – для которого задана собственная системная таблица управления доступом.
Аудит изменения политики	Определяет, подлежит ли аудиту каждый факт изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.
Аудит использования привилегий	Определяет, подлежит ли аудиту каждая попытка пользователя воспользоваться предоставленным ему правом.
Аудит отслеживания процессов	Определяет, подлежат ли аудиту такие события, как активизация программы, завершение процесса, повторение дескрипторов и косвенный доступ к объекту.
Аудит системных событий	Определяет, подлежат ли аудиту такие события, как перезагрузка или отключение компьютера, а также события, влияющие на системную безопасность или на журнал безопасности.

B. Просмотр и настройка аудита папок и файлов (доступно только на томах NTFS).

1. Установите указатель мыши на папку или файл, для которой следует выполнить аудит, и нажмите правую кнопку мыши.
2. В появившемся контекстном меню выберите команду **Свойства**.
3. В окне свойств папки или файла перейдите на вкладку **Безопасность.**
4. На вкладке **Безопасность** нажмите кнопку **Дополнительно** и затем перейдите на вкладку **Аудит.**
5. Если Вы хотите настроить аудит для нового пользователя или группы, на вкладке **Аудит** нажмите кнопку **Добавить**
6. Появиться диалоговое окно **Выбор**: **Пользователь**, **Компьютер** или **Группа.**

7. Выберите имя нужного пользователя или группы и нажмите кнопку **ОК**. Откроется окно диалога **Элемент аудита для**. Здесь Вы сможете ввести все необходимые параметры для аудита.
8. В списке **Применять** укажите, где следует выполнять аудит (это поле доступно только для папок).
9. В группе **Доступ** следует указать, какие события следует отслеживать: окончившиеся успешно (**Успех**), неудачно (**Отказ**) или **оба типа событий**.
10. Применять этот аудит к объектам и контейнерам только внутри этого контейнера – определяет, распространяются ли введенные Вами настройки аудита на файлы и папки, находящиеся ниже по дереву каталогов файловой системы (флажок не установлен). В обратном случае, установите флажок (или выберите в списке) **Применять** опцию **Только для этой папки**. Это позволит не выполнять аудит для тех объектов файловой системы, которые не представляют интереса.
11. После завершения настройки аудита для папки или файла нажмите несколько раз кнопку ОК, чтобы закрыть все окна диалога.
12. Если Вы хотите просмотреть или изменить настройки аудита для уже существующего пользователя или группы, нажмите кнопку **Показать/Изменить**. Появиться окно диалога **Элемент аудита для. Здесь** Вы сможете выполнить все необходимые изменения параметров аудита для выбранного Вами пользователя или группы. По окончанию внесения изменений нажмите кнопку ОК.

Примечание: *После включения Аудита операционная система Windows XP начинает отслеживать события , связанные с безопасностью. Полученную информацию можно просмотреть с помощью оснастки* ***Просмотр событий****. При просмотре журнала событий можно выяснить, кто предпринял попытку выполнения неразрешенных ему действий. Для того, чтобы иметь возможность настраивать аудит для файлов или папок, необходимо иметь права администратора.*

C. **Просмотр событий в журнале событий.**

1. Выберите кнопку **Пуск** панели задач**.**
2. Откройте меню Настроить/Панель управления.
3. В открывшемся окне выберите ярлык **Администрирование** и далее параметр **Просмотр событий.**
4. В открывшемся окне выберите пункт Безопасность (рис. 3).

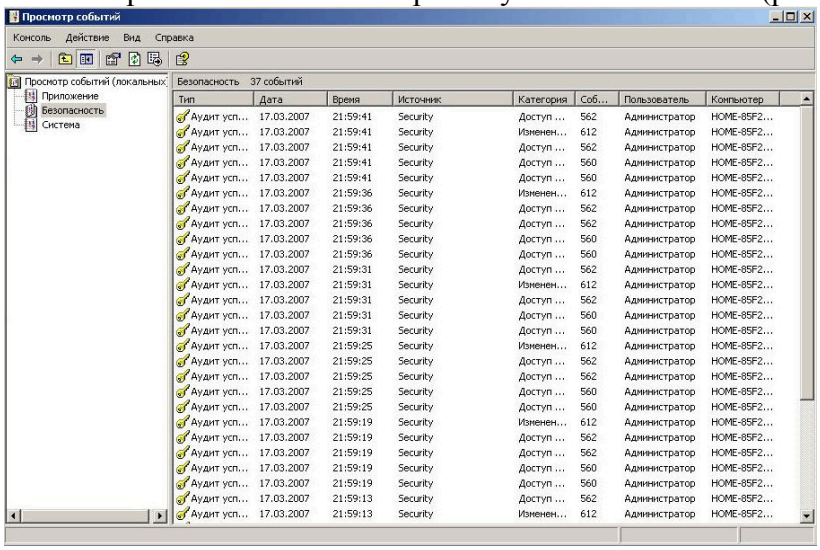


Рис. 3

5. В правой половине открытого окна появиться список всех зарегистрированных событий.
6. Для просмотра требуемого события вызовите его свойства из контекстного меню или дважды щелкните по его названию левой клавишей мыши.
7. В результате появится окно, как показано на рис. 4.
8. В показанном примере зафиксирован успех входа в систему пользователя Администратор.

9. Таким образом просмотр журнала событий позволяет в полной мере проанализировать действия пользователей и процессов.

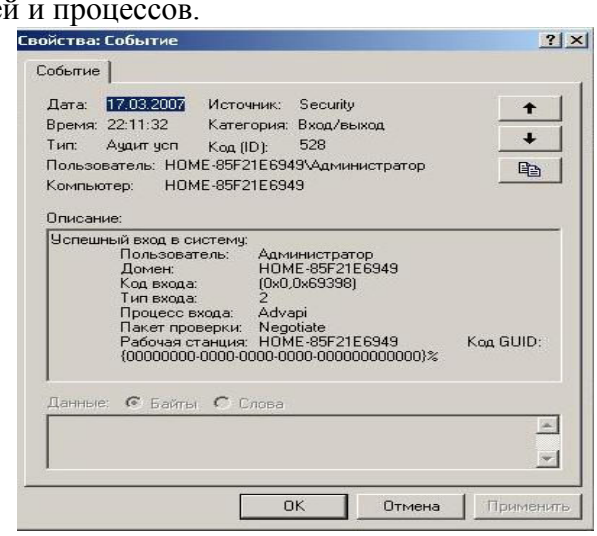


Рис. 4

Задания для самостоятельной работы:

1. Включите аудит успеха и отказа всех параметров (используйте задание А).
2. Выйдите из системы и предпримите попытку входа в операционную систему с неверным паролем. Откройте журнал событий, найдите соответствующую запись и скопируйте в буфер обмена для отчета (клавиша Print Screen).
3. Удалите раннее созданную учетную запись ПЗ-6 и зафиксируйте все события системного журнала, связанные с этим действием для отчета.

Контрольные вопросы:

1. Чем отличаются термины регистрация и аудит?
2. Что является средствами регистрации и аудита?
3. Какие события фиксируются в системном журнале?
4. Что фиксирует система при регистрации событий?

Лабораторная работа
Управление шаблонами безопасности

Цель работы: Научиться работать с редактором шаблонов безопасности, создавать их, редактировать и сохранять.

Краткие теоретические сведения:

Управление шаблонами безопасности в ОС Windows XP осуществляется с помощью Редактора шаблонов безопасности, реализованного в виде оснастки MMC. Он предназначен для создания и редактирования текстовых файлов конфигурации безопасности ОС Windows XP. Такие файлы значительно легче переносятся с одной системы на другую, чем соответствующие им базы безопасности.

Созданные при помощи оснастки Шаблоны безопасности текстовые файлы хранятся на жестком диске и при необходимости могут быть импортированы в базу данных безопасности. В этом случае все хранимые настройки безопасности начнут действовать.

Значения параметров безопасности заносятся в текстовые файлы с расширения .inf, называемые Шаблонами безопасности.

Примечание: *Новые шаблоны безопасности не изменяют все старые настройки параметров системы безопасности, они лишь дополняют их, увеличивая (инкрементируя) степень защищенности компьютера.*

Задание: Загрузить редактор Шаблона безопасности, редактировать шаблон безопасности и сохранить его под новым именем.

Алгоритм выполнения работы.

А. Загрузка оснастки Шаблона безопасности.

1. Выберите кнопку Пуск панели задач.

2. Перейдите к пункту Выполнить.
3. В открывшемся поле ввода введите команду mmc.
4. В результате откроется консоль управления mmc.
5. В меню Консоль выберите команду Добавить или удалить оснастку (рис. 1) и нажмите кнопку Добавить.
6. В поле Оснастка дважды щелкните Шаблоны безопасности.
7. Нажмите кнопку Закрыть.

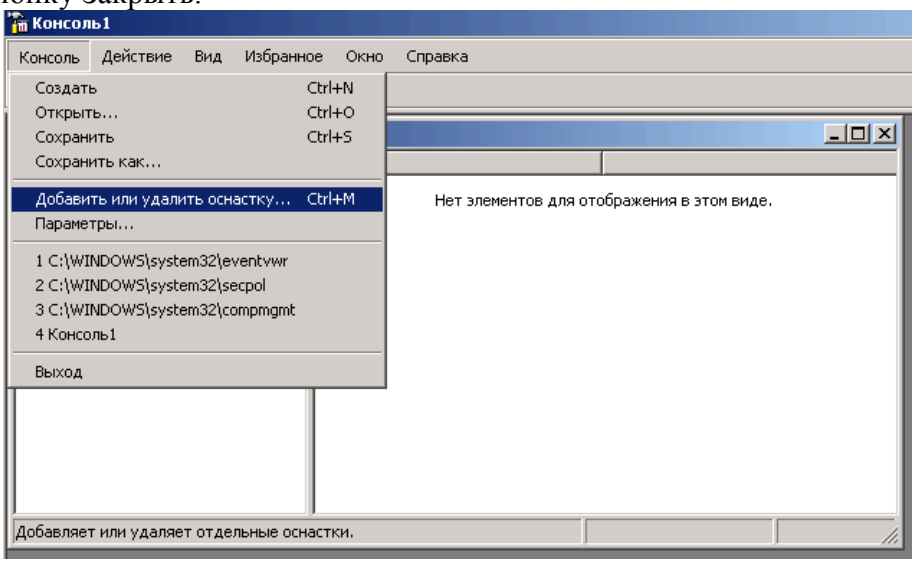


Рис. 1

8. В списке выбранных оснасток для новой консоли появиться элемент Шаблоны безопасности.
9. Если на консоль не нужно добавлять другие оснастки, нажмите кнопку ОК.
10. Чтобы сохранить эту консоль, в меню консоль выберите команду Сохранить и укажите имя оснастки Шаблоны безопасности.
11. Закройте окно Консоли и выберите команду Пуск и далее Все программы.
12. Найдите пункт Администрирование и выберите подпункт Шаблоны безопасности (Теперь оснастка Шаблоны безопасности доступна из меню Пуск).
13. Для просмотра значений имеющихся шаблонов в окне оснастки откройте, например, узел Шаблоны безопасности, щелчком выберите шаблон безопасности compatws (рис. 2) и просмотрите его папки Политика учетных записей, Локальная политика и др.
14. Помимо раскрытого шаблона безопасности compatws.inf существуют и другие стандартные шаблоны, конфигурации которых позволяют получить различные по надежности системы безопасности.

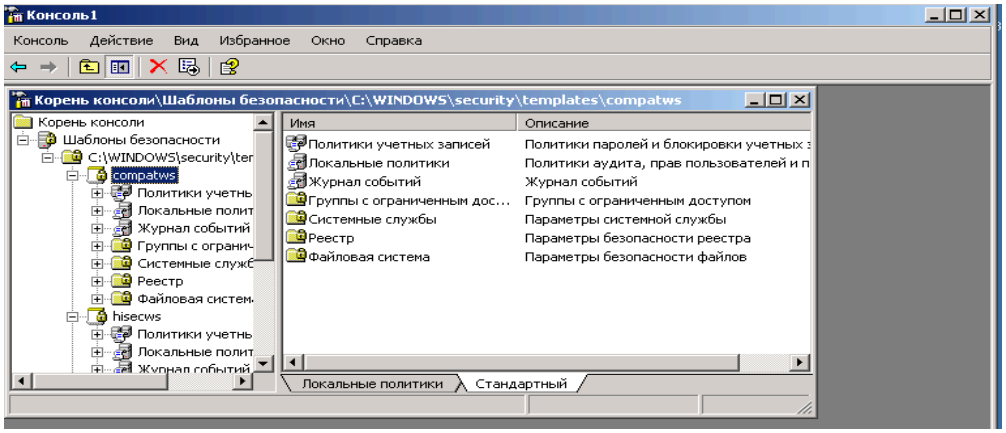


Рис. 2

B. Редактирование и сохранение шаблона безопасности.

1. Щелкните на одном из стандартных шаблонов безопасности (например, compatws), которые Вы видите в окне оснастки Шаблоны безопасности.

2. Если Вы хотите модифицировать какую-либо настройку безопасности, дважды щелкните на ней и отредактируйте значения параметров (рис. 3), например, политика учетных записей-политика паролей- минимальная длина паролей.

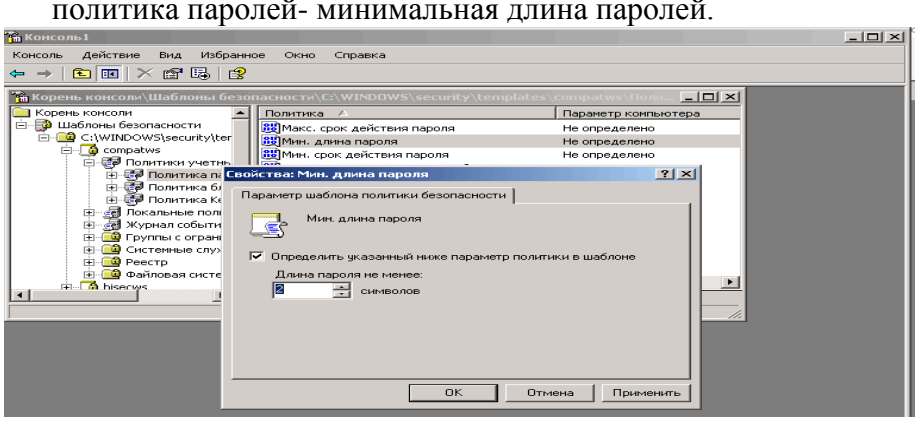


Рис. 3

3. Для сохранения откорректированного стандартного шаблона безопасности под другим именем выполните следующие действия.
4. Укажите откорректированный стандартный шаблон (например, compatws), и нажмите правую кнопку мыши.
5. В появившемся контекстном меню выберите команду Сохранить как.
6. Введите с клавиатуры новое имя файла, например custom. По умолчанию шаблоны безопасности располагаются в каталоге

   %SystemRoot%\Secunfy\Templates.
7. Пользовательский шаблон будет добавлен в определенную заранее конфигурацию безопасности и сохраните под введенным Вами именем.

   Настроив шаблон безопасности для одной ПЭВМ, Вы можете перенести его на другие ПЭВМ Вашей рабочей группы. Шаблоны безопасности являются гибким и удобным инструментом для настройки системы безопасности операционной системы Windows XP.

Задания для самостоятельной работы:

Создайте на базе существующего **Шаблона безопасности новый шаблон** и дайте ему имя ПЗ-8. После этого зафиксируйте список шаблонов, скопируйте изображение экрана в буфер и далее в файл для отчета.

Контрольные вопросы:

1. Для чего используются шаблоны безопасности?
2. В каком месте на диске хранятся (по умолчанию) шаблоны безопасности?
3. Какие разделы включает стандартный Шаблон безопасности?