государственное бюджетное профессиональное образовательное учреждение
«Пермский химико-технологический техникум»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

для специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»
по МДК 01.03 Сети и системы передачи информации

2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Место дисциплины в основной образовательной программе: МДК 01.03 «Сети и системы передачи информации» является разделом профессионального модуля ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» основной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Формируемые МДК 01.03 «Сети и системы передачи информации» компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 1	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

В результате освоения профессионального модуля студент должен:

Иметь практический опыт	установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; администрирования автоматизированных систем в защищенном исполнении; эксплуатации компонентов систем защиты информации автоматизированных систем; диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении
уметь	осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; обеспечивать работоспособность, обнаруживать и устранять неисправности
знать	состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств; теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.

Методические указания предназначены для проведения практических занятий по МДК.01.03, закрепления теоретических знаний и получения навыков работы в области телекоммуникационных сетей.

Методические указания разработаны в соответствии с рабочей программой профессионального модуля ПМ.01. «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

По учебному плану, и в соответствии с рабочей программой профессионального модуля ПМ.01, на изучение МДК.01.03. обучающимися предусмотрено 94 часов, из них практических – 24.

Методические указания включают 14 практических работ по темам раздела: «Сети и си-

стемы передачи информации» и «Сети передачи данных». Каждая практическая работа содержит сведения о теме, цели ее проведения и формируемых компетенциях, включает пояснения к работе, содержание отчета, контрольные задания или вопросы, список литературы.

К выполнению практических работ обучаемые приступают после подробного изучения соответствующего теоретического материала и прохождения инструктажа по технике безопасности.

Характер практических работ репродуктивный и частично-репродуктивный.

ПРАВИЛА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

1. Студент должен прийти на занятие подготовленным к выполнению работы. Студент, не подготовленный к работе, не может быть допущен к ее выполнению.
2. Каждый студент после выполнения работы должен представить отчет о проделанной работе с анализом полученных результатов и выводом по работе.
3. Таблицы и схемы следует выполнять с помощью чертежных инструментов (линейки, циркуля и т. д.) карандашом.
4. Исправления выполняют на обратной стороне листа отчета. При мелких исправлениях неправильное слово (буква, число и т. п.) аккуратно зачеркивают и над ним пишут правильное пропущенное слово (буква, число)
5. Вспомогательные расчеты можно выполнить на отдельных листах, а при необходимости на листах отчета.
6. Если студент не выполнил работу или часть работы, то он может выполнить работу или оставшуюся часть во внеурочное время, согласованное с преподавателем.
7. Оценку по работе студент получает, с учетом срока выполнения работы, если:
   - расчеты выполнены правильно и в полном объеме;
   - сделан анализ проделанной работы и вывод по результатам работы;
   - студент может пояснить выполнение любого этапа работы;
   - отчет выполнен в соответствии с требованиями к выполнению работы;
   - студент ответил на дополнительные теоретические вопросы преподавателя.
8. программой работы после сдачи отчетов при удовлетворительных оценках.

ОПИСАНИЕ РАБОЧЕГО МЕСТА ОБУЧАЮЩЕГОСЯ

1. Практические работы по дисциплине выполняются частично в учебной аудитории, частично в компьютерном классе.
2. Для выполнения практических работ необходимы:
   - персональные компьютеры;
   - конспект лекций;
   - методические указания;
   - чертежные инструменты;
   - калькулятор.
3. Выполнение работ и оформление отчета студент выполняет индивидуально.
4. По выполнению всех этапов задания и оформления студент предоставляет отчет по практическим работам.
5. Для получения оценки студент защищает практическую работу по предоставленному отчету и отвечая на вопросы преподавателя по теории.

ПРАКТИЧЕСКИЕ РАБОТЫ

ПРАКТИЧЕСКАЯ РАБОТА №1
Монтаж кабельных сред технологий Ethernet.

Цель работы

1. Познакомиться с пассивным оборудованием и аксессуарами локальных сетей, необходимыми для прокладки кабельных систем.
2. Освоить операции монтажа кабеля «витая пара» в коннекторы RJ-45 и неразъемные соединения.

Оборудование: кабель UTP 5e, коннекторы RJ-45, обжимные клещи, компьютерный класс.

Задание

Создание компьютерных сетей, как правило, включает в себя прокладку кабельных систем. Думаю, что Вам будет полезно познакомится с пассивным оборудованием (коннекторами BNC и RJ-45, розетками, патч- и кросс-панелями, коаксиальным кабелем и кабелем «витая пара» и т.д) и аксессуарами (шкафы, стойки, короба, плинтуса и т.д.) локальных сетей необходимыми для этого, увидеть вживую, подержать в руках.

Полезно также получить навыки выполнения элементарных операций по "заделке" кабеля «витая пара» в различные разъемы. Эти навыки необходимы в профессии монтажника кабельных систем. Практику монтажа кабеля в различные кабелепроводы и его укладки за подвесной потолок желающие смогут получить на четвертом курсе.

Порядок выполнения

1. Внимательно прослушайте посвященную пассивному оборудованию и аксессуарам кабельных систем рассказ-демонстрацию преподавателя. Зарисуйте внешний вид представленных оборудования и аксессуаров. Также, в свой отчет, внесите их основные характеристики.
2. Просмотрите демонстрацию преподавателя монтажа кабеля «витая пара» в коннектор RJ-45.
3. Объединившись с кем-нибудь из одногрупников, изготовьте патч-корд для прямого соединения. Оба конца патч-корда необходимо обжать в соответствии со стандартом EIA/TIA 568B. Необходимую раскладку проводов по этому стандарту можно найти в лекционном материале. Запишите в отчет необходимую для этого последовательность действий.
4. Проверьте работоспособность изготовленного вами патч-корда, подключив им компьютер к локальной сети.
5. Просмотрите демонстрацию преподавателя монтажа кабеля «витая пара» в розетку, содержащую неразъемное соединение S110 или S66 типа. Запишите в отчет необходимую для этого последовательность действий.
6. Объединившись с кем-нибудь из одногрупников, соедините кабелем две розетки. Проверьте работоспособность получившейся кабельной системы.
7. Сделайте соответствующие выводы.

Содержание отчета

Отчет должен содержать:

- Название работы
- Цель работы
- Таблицу разводки по схеме A и B
- Описание техники монтажа и использованных инструментов.

Контрольные вопросы

1. Что такое «витая пара»?
2. Как нужно обжать кабель «витая пара», если компьютеры будут взаимодействовать через коммутатор?
3. Как нужно обжать кабель «витая пара», если компьютеры будут взаимодействовать напрямую?
4. Какие пары «витой пары используются при технологии Fast Ethernet?

Рекомендуемая литература

Основная

1. Костров Б.В. Сети и системы передачи информации: учебник для студентов учреждений среднего профессионального образования / Б.В. Костров, В.Н. Ручкин. –М.: Издательский центр «Академия», 2017г.

Дополнительная

1. Литвинская О.С. Основы теории передачи информации: учебное пособие / Литвинская О.С., Чернышев Н.И. — Москва: КноРус, 2021 — 168 с. — ISBN 978-5-406-08653-7. — URL: https://book.ru/book/940469 (дата обращения: 23.04.2021). —Текст: электронный.

ПРАКТИЧЕСКАЯ РАБОТА №2
Работа с коммуникационным оборудованием

Цель работы

Приобрести навыки по установке управляемого коммутатора D-LINK DES

Оборудование: компьютерный класс, управляемый коммутатор.

Задание

Управляемые коммутаторы являются сложными устройствами, позволяющими выполнять расширенный набор функций 2-го и 3-го уровня модели OSI. Управление коммутаторами может осуществляться посредством Web-интерфейса, командной строки (CLI), протокола SNMP, Telnet и т.д.

Настраиваемые коммутаторы занимают промежуточную позицию между ними. Они предоставляют пользователям возможность настраивать определенные параметры сети с помощью интуитивно понятных утилит управления, Web-интерфейса, упрощенного интерфейса командной строки, протокола SNMP.

Средства управления коммутаторами

Большинство современных коммутаторов поддерживают различные функции управления и мониторинга. К ним относятся дружественный пользователю Web-интерфейс управления, интерфейс командной строки (Command Line Interface, CLI), Telnet, SNMP-управление. В коммутаторах D-Link серии Smart также реализована поддержка начальной настройки и обновления программного обеспечения через утилиту D-Link SmartConsole Utility.

Web-интерфейс управления позволяет осуществлять настройку и мониторинг параметров коммутатора, используя любой компьютер, оснащенный стандартным Web-браузером. Браузер представляет собой универсальное средство доступа и может непосредственно подключаться к коммутатору по протоколу HTTP.

Главная страница Web-интерфейса обеспечивает доступ к различным настройкам коммутатора и отображает всю необходимую информацию об устройстве. Администратор может быстро посмотреть статус устройства, статистику по производительности и т.д., а также произвести необходимые настройки.

Доступ к интерфейсу командной строки коммутатора осуществляется путем подключения к его консольному порту терминала или персонального компьютера с установленной программой эмуляции терминала. Это метод доступа наиболее удобен при первоначальном подключении к коммутатору, когда значение IP-адреса неизвестно или не установлено, в случае необходимости восстановления пароля и при выполнении расширенных настроек коммутатора. Также доступ к интерфейсу командной строки может быть получен по сети с помощью протокола Telnet.

Пользователь может использовать для настройки коммутатора любой удобный ему интерфейс управления, т.к. набор доступных через разные интерфейсы управления функций одинаков для каждой конкретной модели.

Еще один способ управления коммутатором — использование протокола SNMP (Simple Network Management Protocol). Протокол SNMP является протоколом 7-го уровня модели OSI и разработан специально для управления и мониторинга сетевыми устройствами и приложениями связи. Это выполняется путем обмена управляющей информацией между агентами, располагающимися на сетевых устройствах, и менеджерами, расположенными на станциях управления. Коммутаторами D-Link поддерживается протокол SNMP версий 1, 2c и 3.

Также стоит отметить возможность обновления программного обеспечения коммутаторов (за исключением неуправляемых). Это обеспечивает более долгий срок эксплуатации устройств, т.к. позволяет добавлять новые функции либо устранять имеющиеся ошибки по мере выхода новых версий ПО, что существенно облегчает и удешевляет использование устройств.

Компания D-Link распространяет новые версии ПО бесплатно. Сюда же можно включить возможность сохранения настроек коммутатора на случай сбоев с последующим восстановлением или тиражированием, что избавляет администратора от выполнения рутинной работы.

Порядок выполнения

Зайти на устройство через "консольный" порт (RS-232). Подключаем кабель (DB-9 cable):

Рекомендованные производителем параметры подключения следующие:

terminal - VT 100+;
speed - 9600;
parity - none;
data bits - 8;
stop bit - 1;
sofware flow control - none;
hardware flow control - none.

Запускаем "minicom":

```
$ minicom --device /dev/ttyS0 --baudrate 9600 --8bit --noinit
```

Сразу идём в меню настроек утилиты "minicom" для корректировки параметров сеанса связи с коммутатором: "Ctrl+O". Переходим в подменю "Serial port setup". Нажав клавишу "F", выбираем значение "No" для опции "Hardware Flow Control". Подтверждаем выбор и выходим из меню конфигурирования. Готово, мы в коммутаторе:

```
      DES-3028 Fast Ethernet Switch Command Line Interface
                  Firmware: Build 2.00.B27
    Copyright(C) 2008 D-Link Corporation. All rights reserved.
UserName:
```

Просто нажимаем пару раз "Enter", проходя этапы ввода логина и пароля, и вот, мы можем просмотреть текущую конфигурацию устройства:

```
# show switch
```

```
Device Type        : DES-3028 Fast Ethernet Switch
MAC Address        : MAC
IP Address         : 10.90.90.90 (Manual)
VLAN Name          : default
Subnet Mask        : 255.0.0.0
Default Gateway    : 0.0.0.0
Boot PROM Version  : Build 1.00.B06
Firmware Version   : Build 2.00.B27
Hardware Version   : A2
Serial Number      : Serial
System Name        :
System Location    :
System Contact     :
Spanning Tree      : Disabled
GVRP               : Disabled
```

```
IGMP Snooping      : Disabled
VLAN trunk         : Disabled
802.1x             : Disabled
TELNET             : Enabled(TCP 23)
WEB                : Enabled(TCP 80)
RMON               : Disabled
SSH                : Disabled
SSL                : Disabled
Clipaging          : Enabled
Syslog Global State: Disabled
Dual Image         : Supported
Password Encryption Status : Disabled
```

Приступим к конфигурированию как таковому.

На всякий случай явно отключаем автоматическую настройку с помощью DHCP:

```
# disable autoconfig
```

Назначим свой IP-адрес:

```
# config ipif System ipaddress 192.168.1.2/24 state enable
```

Удостоверимся в том, что изменения приняты:

```
# show ipif
```

```
Interface Name  : System
IP Address      : 192.168.1.2 (MANUAL)
Subnet Mask     : 255.255.255.0
VLAN Name       : default
Admin. State    : Enabled
Link Status     : Link UP
Member Ports    : 1-28
```

Обратите внимание на то, что "shell" устройства регистро-чувствительный, в частности, команда "System" так и вводится, с большой буквы, в то время как другие - с маленькой.

Задаём маршрут по умолчанию, необходимый для обеспечения доступности управляющего функционала коммутатора:

```
# create iproute default 192.168.1.1 1
```

Удостоверимся, что маршрут верно задан:

```
# show iproute
```

```
IP Address/Netmask  Gateway         Interface    Hops     Protocol
------------------  --------------  -----------  -------  --------
0.0.0.0/0           192.168.1.1     System       1        Default
192.168.1.0/24      0.0.0.0         System       1        Local
```

Проверим, достижим ли с коммутатора какой-нибудь удалённый ресурс:

```
# ping 192.168.12.12 times 4
```

```
Reply from 192.168.12.12, time<10ms
Reply from 192.168.12.12, time<10ms
Reply from 192.168.12.12, time<10ms
Ping Statistics for 192.168.12.12
Packets: Sent =4, Received =4, Lost =0
```

И так, теперь, когда железка доступна для подключения не только локального, но и удалённого, вынесем работу из гудящей и холодной серверной в кресло администратора, приняв меры, в то-же время, к обеспечению безопасности соединения. А точнее: дополним сетевую конфигурацию, заведём на коммутаторе административный аккаунт, инициируем SSH-сервер и предпишем работать через него.

Отключаем расширенную систему авторизации на устройстве, оставляя локальную базу:

```
# config authen_login default method local
# config authen_enable default method local_enable
# config authen parameter response_timeout 30
# config authen parameter attempt 5
# disable authen_policy
# config admin local_enable
```

Создаём парочку административных аккаунтов:

```
# create account admin superadmin
# create account admin trivialadmin
```

```
Enter a case-sensitive new password:********
Enter the new password again for confirmation:********
Success.
```

Когда придёт в голову сменить пароль, делаем это так:

```
# config account trivialadmin
```

Удостоверимся, что аккаунты созданы в том виде, как нам было угодно:

```
# show account
```

```
Username         Access Level
-----------------  ------------
superadmin        Admin
trivialadmin      Admin
```

Велим коммутатору шифровать сохранённые в энергонезависимой памяти пароли:

```
# enable password encryption
```

Включаем поддержку доступа к устройству по протоколу SSH:

```
# enable ssh

TELNET will be disabled when enable SSH.
Success.
```

Поддержку менее безопасного протокола доступа Telnet даже отключать не приходится, прошивка устройства не может работать одновременно и с SSH и с Telnet.

Явно указываем, каким образом мы будем проходить проверку подлинности:

```
# config ssh authmode password enable
```

Задаём параметры подключения клиента SSH к серверу:

```
# config ssh server maxsession 3 contimeout 600 authfail 10 rekey never
```

Вводим заранее созданных пользователей в список допущенных для работы с SSH:

```
# config ssh user superadmin authmode password
# config ssh user trivialadmin authmode password
```

Отдельно явно разрешаем использование протокола шифрования трафика SSH:

```
# config ssh algorithm RSA enable
```

Для самоуспокоения можно пробежаться по настройкам, с помощью команды "show" с соответствующими аргументами удостоверится, что желаемые настройки применены верно. После чего - сохраняем всё, и настройки и журнал событий, в энергонезависимую память:

```
# save all
```

Перезагружаем коммутатор:

```
# reboot
```

Теперь идём на своё рабочее место и подключаемся к устройству используя для это протокол SSH.

Первым делом стоит подкорректировать настройки портов. Например таким образом:

```
# config ports 1-24 speed auto flow_control enable state enable
# config ports 25 speed 100_full state enable
# config ports 26,28 speed 1000_full master flow_control enable state enable
```

Здесь мы позволили клиентским портам принимать конфигурацию клиента, предлагая аппаратный контроль потока передаваемых данных, выделили один порт для связи с маршрутизатором на скорости 100 Мегабит с полным "дуплексом" и выделили два "гигабитных" порта для связи с другими коммутаторами.

Очень желательно явно выставлять параметры интерфейсов, предназначенных для связи между коммутаторами и маршрутизаторами. На моей практике неоднократно наблюдались огромные, до 30%-40% потери пакетов из-за того, что оборудование не могло договорится о режимах работы в автоматической конфигурации.

Следует иметь в виду, что у D-Link при конфигурировании "гигабитных" портов нужно явно указывать, какая сторона ведущая, а какая ведомая. В частности, если этот коммутатор "ведущий" (master), что на втором "гигабитные" порты должны быть инициированы как "ведомые" (slave), например:

```
# config ports 25,27 speed 1000_full slave flow_control enable state enable
```

Далее следует чуть подкорректировать общие настройки, имеющие отношение к обеспечению условий коммутации.

Что-бы огорчить любителей повесить на порт нашего коммутатора свой коммутатор и нацеплять за ним кучу незарегистрированного оборудования, явно укажем не принимать запросы на порту более чем с одного MAC:

```
# config port_security ports 1-24 admin_state enable max_learning_addr 1 lock_address_mode DeleteOnTimeout
```

Естественно, для "транков" ограничение на количество обслуживаемых MAC снимаем:

```
# config port_security ports 25-28 admin_state disable
```

Насколько я понял из документации, опция "DeleteOnTimeout" регламентирует периодичность пересмотра таблицы коммутации (Forwarding Database) MAC на портах. Надо полагать (вернее, так сказано в документации, но я мог неверно перевести), что MAC-адрес клиента неактивного порта будет удалён из таблицы и другому MAC-адресу будет позволено работать на нём именно после этого самого пересмотра таблицы. Сменить период пересмотра таблицы можно с помощью соответствующей команды (по умолчанию период составляет 300 секунд):

```
# config fdb aging_time 120
```

На случай, если понадобится по быстрому, не дожидаясь истечения "таймаута" разблокировать какой-либо порт, очистив историю использования его клиентам, есть команда, которой мы очистим историю использования для портов со второго по седьмой:

```
# clear port_security_entry port 2-7
```

Теперь активируем функционал "Storm Control" для борьбы с клиентами, сорящими "бродкастовыми" и "мультикастовыми" пакетами (зажимаем клиента по максимуму - у нас только традиционные сервисы, не подразумевающие рассылок; в обычной плоской сети реальный "флуд" диагностируется по показателю в 100 Kbs):

```
# config traffic control 1-24 broadcast enable multicast enable unicast disable action drop threshold 64 countdown 5 time_interval 5
```

Можно попробовать применить новый функционал D-Link обнаружения и блокирования потенциальных DoS-атак, пока вреда от него я не замечал:

```
# config dos_prevention dos_type all action drop state enable
# config dos_prevention dos_type tcp_syn_srcport_less_1024 state disable
# disable dos_prevention trap_log
```

Типов атак несколько, вместо "all" можно включать и выключать их обнаружение индивидуально:

Land Attack, Blat Attack, Smurf Attack, TCP Null Scan, TCP Xmascan, TCP SYNFIN, TCP SYN SrcPort less 1024

Видно, что выше я отключил обнаружение атак типа "TCP SYN SrcPort less 1024"; не углублялся в суть вопроса, но при активировании этой опции коммутатор воспринимает попытки взаимодействия Linux/BDS/Apple-машины с сетевым принтером как атаку, блокируя передачу данных.

Для отлова "петель" на стороне клиента используем специализированный функционал коммутатора, регулярно посылающий тестовый пакет обнаружения "loopback" (это работает независимо от протокола STP):

```
# enable loopdetect
# config loopdetect ports 1-24 state enabled
# config loopdetect ports 25-28 state disabled
# config loopdetect recover_timer 180 interval 10
```

Где:

recover_timer - время (в секундах), в течение которого порты будут отключены для стимулирования пользователя порта разобраться, "почему не работает";
interval - период (в секундах) между отправкой пакетов обнаружения петли.

В качестве дополнительной меры обеспечения доступности сервисов, представляемых коммутатором, включим поддержку "Safeguard engine", режима, в котором отбрасываются или отправляются в конец очереди (с пониженным приоритетом) все ARP и "широковещательные" пакеты тогда, когда загрузка процессора возрастёт выше установленного порога:

```
# config safeguard_engine state enable utilization rising 90 falling 30 trap_log disable mode fuzzy
```

Где:

rising 90 - процент загрузки процессора, выше которого включается режим "Safeguard engine";
falling 30 - процент загрузки, ниже которого выключается "Safeguard engine";
mode fuzzy - выбираем режим мягкого противодействия нагрузке, когда широковещательные и ARP пакеты не откидываются полностью, а лишь понижаются в приоритете при обработке.

Далее - обще-системные мелочи.

Велим коммутатору отправлять на удалённый сервер данные своего журнала событий:

```
# enable syslog
# create syslog host 4 ipaddress 192.168.12.12 severity all facility local1 state enable
```

Научим наш коммутатор выспрашивать точное время у соответствующих серверов.

Задаём "часовой пояс":

```
# config time_zone operator + hour 6 min 0
```

Отключим перевод на "летнее время":

```
# config dst disable
```

Укажем наши сервера точного времени:

```
# config sntp primary 192.168.12.12 secondary 192.168.0.12 poll-interval 21600
```

Включим подсистему:

```
# enable sntp
```

Далее отключим то, что не подпадает под понятие базовой настройки.

Отключаем подсистему уведомлений о событиях на SMTP-сервер:

```
# disable smtp
```

Отключаем SNMP:

```
# delete snmp community public
# delete snmp community private
# disable snmp traps
# disable snmp authenticate traps
# disable rmon
```

Отключаем систему уведомления SNMP сервера о изменении MAC клиента на портах:

```
# disable mac_notification
```

Отключаем протокол оповещения и сбора информации о соседнем оборудовании (свободная замена таким протоколам, как: Cisco Discovery Protocol, Extreme Discovery Protocol, Foundry Discovery Protocol или Nortel Discovery Protocol). Вещь полезная, но в небольшой сети не особо нужная, особенно, если нет понимания целесообразности применения:

```
# disable lldp
```

Отключаем перенаправление DHCP запросов на целевой сервер:

```
# disable dhcp_relay
# disable dhcp_local_relay
```

Отключаем зеркалирование портов (применяется для мониторинга и сбора статистики):

```
# disable mirror
```

Отключаем поддержку протокола STP:

```
# disable stp
```

Отключаем функционал единого адреса для стека коммутаторов:

```
# disable sim
```

Отключаем авторизацию клиентов на портах:

```
# disable 802.1x
```

Отключаем инкапсуляцию тегов VLAN в теги VLAN второго уровня (сеть у нас маленькая):

```
# disable qinq
```

Явно отключаем управление "мультикастом", раз уж он не используется:

```
# disable igmp_snooping
# disable mld_snooping
```

Сохраняем конфигурацию:

```
# save all
```

Можно побродить по "web"-интерфейсу коммутатора. Уж не знаю, что там можно было наворотить, но "сайт" успешно завешивает Google Chrome (Linux); браузер начинает беспрерывно перезапрашивать один из "фреймов" панели управления, потребляя при этом половину ресурсов компьютера и не отображая при этом ничего, кроме аляповатого рисунка коммутатора на мозаичном фоне в стиле Web-0.9. Хорошо хоть Firefox (Linux) справился. Первым делом рекомендую забанить анимированную, очень детализированную, с искорками, вертящимися вокруг стилизованного земного шара, картинку-логотип в фрейме меню управления; лично у меня на "нетбуке" после этого обороты вентилятора сразу упали со средних до нулевого уровня.

Рекомендую отключить "web"-интерфейс:

```
# disable web
# disable ssl
```

CLI предоставляет достаточно инструментария для контроля и мониторинга устройства, например:

```
# show error ports 1-24
```

```
Port Number : 2
              RX Frames                    TX Frames
              ---------                    ---------
CRC Error       0          Excessive Deferral    0
Undersize       0          CRC Error             0
Oversize        0          Late Collision        0
Fragment        1          Excessive Collision   0
```

```
Jabber          0          Single Collision      0
Drop Pkts       0          Collision             0
```

```
# show ports
```

```
Port  State/         Settings           Connection       Address
      MDI      Speed/Dupl/FlowCtrl  Speed/Dupl/FlowCtrl Learning
----- -------- ------------------ ------------------  --------
1     Enabled  Auto/Enabled       100M/Full/None      Enabled
      Auto
2     Enabled  Auto/Enabled       100M/Full/802.3x    Enabled
      Auto
3     Enabled  Auto/Enabled       10M/Full/802.3x     Enabled
      Auto
4     Enabled  Auto/Enabled       LinkDown            Enabled
      Auto
5     Enabled  Auto/Enabled       LinkDown            Enabled
      Auto
6     Enabled  Auto/Enabled       100M/Full/None      Enabled
      Auto
7     Enabled  Auto/Enabled       LinkDown            Enabled
....
```

```
# show traffic control
```

```
Port Thres Broadcast Multicast Unicast  Action  Count Time
     hold  Storm     Storm     Storm            down  Interval
---- ----- --------- --------- -------- ------- ----- --------
1    64    Enabled   Enabled   Disabled drop    5     5
2    64    Enabled   Enabled   Disabled drop    5     5
3    64    Enabled   Enabled   Disabled drop    5     5
4    64    Enabled   Enabled   Disabled drop    5     5
5    64    Enabled   Enabled   Disabled drop    5     5
....
```

```
# show utilization ports
```

```
Port   TX/sec   RX/sec Util  Port   TX/sec   RX/sec Util
---- -------- -------- ----  ---- -------- -------- ----
1    0        0        0     22   0        0        0
2    0        0        0     23   0        0        0
3    0        0        0     24   0        0        0
4    0        0        0     25   16       19       1
5    0        0        0     26   14       10       1
6    0        0        0     27   0        0        0
7    0        0        0     28   0        1        1
....
```

```
# show arpenrty
```

```
Interface  IP Address   MAC Address       Type
---------  ------------ ----------------- ---------------
```

```
System    ....      FF-FF-FF-FF-FF-FF Local/Broadcast
System    ....      ....              Dynamic
System    ....      ....              Local
System    ....      FF-FF-FF-FF-FF-FF Local/Broadcast
....
```

```
# show packet ports 1-24
```

```
Port Number : 16
Frame Size   Frame Counts Frames/sec Frame Type   Total      Total/sec
------------ ------------ ---------- ----------   ---------  ---------
64           676290       0          RX Bytes     47389203   0
65-127       34487        0          RX Frames    713350     0
128-255      76           0
256-511      684          0          TX Bytes     1936090115 0
512-1023     1550         0          TX Frames    1330260    0
1024-1518    263          0

Unicast RX   713310       0
Multicast RX 0            0
Broadcast RX 40           0
```

Содержание отчета

Отчет должен содержать:

- Название работы
- Цель работы
- Способы подключения к коммутатору
- Основные команды управления
- Ответы на вопросы

Контрольные вопросы

1. Каково назначение и функции управляемого коммутатора?
2. Какой способ управления коммутатором предпочтительнее и почему?

Рекомендуемая литература

Основная

1. Костров Б.В. Сети и системы передачи информации: учебник для студентов учреждений среднего профессионального образования / Б.В. Костров, В.Н. Ручкин. –М.: Издательский центр «Академия», 2017г.

Дополнительная

2. Литвинская О.С. Основы теории передачи информации: учебное пособие / Литвинская О.С., Чернышев Н.И. — Москва: КноРус, 2021 — 168 с. — ISBN 978-5-406-08653-7. — URL: https://book.ru/book/940469 (дата обращения: 23.04.2021). —Текст: электронный.

ПРАКТИЧЕСКАЯ РАБОТА №3
Работа с сетевыми адаптерами

Цель работы

Приобрести навыки по установке сетевого адаптера в персональный компьютер и настройки его драйвера в операционных системах Windows XP и Linux.

Оборудование: компьютерный класс, сетевые адаптеры.

Задание

Процесс подключения ПК к компьютерной сети можно условно разбить на два этапа:

- монтаж сетевого адаптера (сетевой карты) в ПК;
- настройка драйвера адаптера.

Установка современных сетевых адаптеров не представляет особой сложности. Откройте корпус ПК, вставьте сетевую карту в соответствующий слот расширения (сейчас, это слот шины PCI) и закрепите адаптер в корпусе болтом. Вот и все! Мало того, большинство современных адаптеров поставляются интегрированными в материнскую плату, что еще больше упрощает вашу работу. **Не забудьте подключить сетевую карту к кабельной системе Вашей сети, вставив разъем патч-корда в соответствующий разъем на карте.**

Основные проблемы у Вас возникнут при настройке сетевого адаптера в различных операционных системах. Традиционно, достаточно при настройке необходимо ввести все параметры, указанные системным (сетевым) администратором Вашей локальной сети. Однако, системный администратор - это Вы и есть! И именно Вы обязаны эти параметры определять. Как быть? Учитесь!

В данной работе изучаются только базовые настройки сетевого адаптера. Они позволят персональному компьютеру работать в любой локальной компьютерной сети и сети Интернет. Тонкие настройки драйвера, оптимизирующие и ускоряющие работу сетевой карты в конкретной локальной сети и с конкретными сетевыми протоколами и приложениями, доступные только в дорогих сетевых адаптерах, здесь не рассматриваются. Не рассматриваются здесь и параметры доступные при работе с фирменными технологиями, реализованными производителями активного оборудования, а также параметры, относящиеся к настройке сетевой безопасности и дополнительных сетевых сервисов.

Порядок выполнения

1. Вмонтируйте плату сетевого адаптера в персональный компьютер.
2. Установите драйвер сетевой карты (для операционной системы Windows 7). Установим его вручную, для этого:

- распакуйте из архива с именем **DFE528,** находящегося на прилагающемся компакт диске,
- драйвер сетевого адаптера D-Link 538TX в каталог **C:\TEMP\NET.** Именно этот сетевой адаптер установлен на ПК, на котором выполняется лабораторную работу.
- в **C:\TEMP\NET** найдите и запустите INSTALL.EXE.
- выберите пункт INSTALL в появившемся окне и **немного подождите.** Драйвер будет автоматически установлен.

3. Установите драйвер сетевой карты (для операционной системы Linux). В используемой при проведении практических работ версии Linux – Ubuntu 12.04 LTS драйвер устанавливается автоматически при установке операционной системы. Для ручной настройки (этот путь - один из нескольких):

- узнайте, как называется драйвер, подходящий для имеющегося сетевого адаптера (в нашем случае подходит драйвер с именем **8139too;**
- выполните команду: **modprobe 8139too** , указывая ОС какой драйвер ей использовать;
- выполните команду: **ifup ethO** - тем самым, активируя сетевой адаптер (кстати, **ifdown ethO** остановит работу сетевого адаптера).

Эти действия придется выполнять при каждом запуске Linux, хотя возможно автоматизировать этот процесс, изменив несколько конфигурационных файлов.

Рекомендую все же использовать мастер установки сетевого адаптера - **draknet.** Если эта команда не работает - **draknet** не установлен, то установите его! Данная программа позволит одновременно и настроить сетевой адаптер.

4. Настройте драйвер сетевой карты (для операционной системы Linux).[3] Его можно настроить, ответив на вопросы при установке Linux. Для ручной настройки:

- для этого надо изменить содержание некоторых конфигурационных файлов. В данной работе не рассмотрено.

Для настройки используйте **draknet.** Мастер настройки задаст ряд вопросов, на которые необходимо ответить. Этот же мастер работает и при установке Ubuntu 12.04 LTS.

Помните, в разных версиях Linux настройка сети несколько отличается.

Содержание отчета

Отчет должен содержать:

- Название работы
- Цель работы
- Схему сетевой карты
- Описание технологии установки сетевой карты.

Контрольные вопросы

1. Каково назначение и функции сетевой карты?
2. Что такое драйвер?
3. Каковы особенности установки сетевой карты в разных ОС?

Рекомендуемая литература

Основная

1. Костров Б.В. Сети и системы передачи информации: учебник для студентов учреждений среднего профессионального образования / Б.В. Костров, В.Н. Ручкин. –М.: Издательский центр «Академия», 2017г.

Дополнительная

2. Литвинская О.С. Основы теории передачи информации: учебное пособие / Литвинская О.С., Чернышев Н.И. — Москва: КноРус, 2021 — 168 с. — ISBN 978-5-406-08653-7. — URL: https://book.ru/book/940469 (дата обращения: 23.04.2021). —Текст: электронный.

ПРАКТИЧЕСКАЯ РАБОТА №4
Настройка ADSL-модема

Цель работы

Научиться производить мониторинг и диагностировать ошибки, возникающие при настройке протокола TCP/IP.

Оборудование: компьютерный класс, ADSL-модем.

Задание

ADSL (Asymmetric Digital Subscriber Line — Асимметричная цифровая абонентская линия) входит в число технологий высокоскоростной передачи данных, известных как технологии DSL (Digital Subscriber Line — Цифровая абонентская линия) и имеющих общее обозначение xDSL. К другим технологиям DSL относятся HDSL (High data rate Digital Subscriber Line — Высокоскоростная цифровая абонентская линия), VDSL (Very high data rate Digital Subscriber Line — Сверхвысокоскоростная цифровая абонентская линия) и другие.

Общее название технологий DSL возникло в 1989 году, когда впервые появилась идея использовать аналого-цифровое преобразование на абонентском конце линии, что позволило бы усовершенствовать технологию передачи данных по витой паре медных телефонных проводов. Технология ADSL была разработана для обеспечения высокоскоростного (можно даже сказать мегабитного) доступа к интерактивным видеослужбам (видео по запросу, видеоигры и т.п.) и не менее быстрой передачи данных (доступ в Интернет, удаленный доступ к ЛВС и другим сетям).

Так что же такое ADSL? Прежде всего, ADSL является технологией, позволяющей превратить витую пару телефонных проводов в тракт высокоскоростной передачи данных. Линия ADSL соединяет два модема ADSL, которые подключены к каждому концу витой пары телефонного кабеля (смотрите рисунок 1). При этом организуются три информационных канала — «нисходящий» поток передачи данных, «восходящий» поток передачи данных и канал обычной телефонной связи (POTS) (смотрите рисунок 2). Канал телефонной связи выделяется с помощью фильтров, что гарантирует работу вашего телефона даже при аварии соединения ADSL.

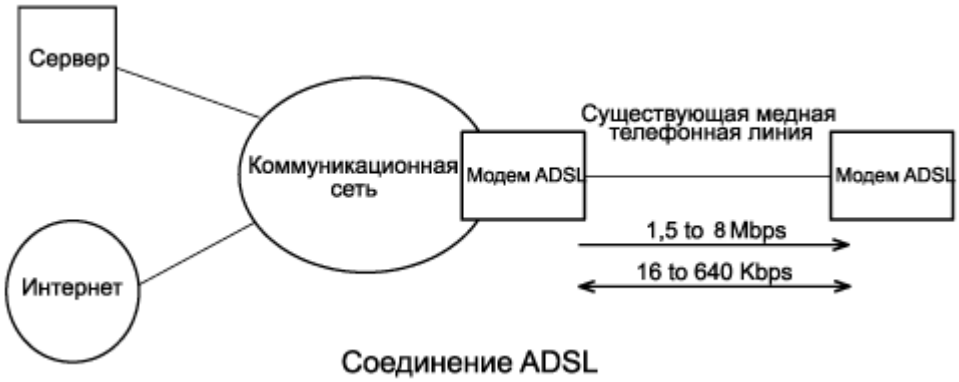


Рисунок1

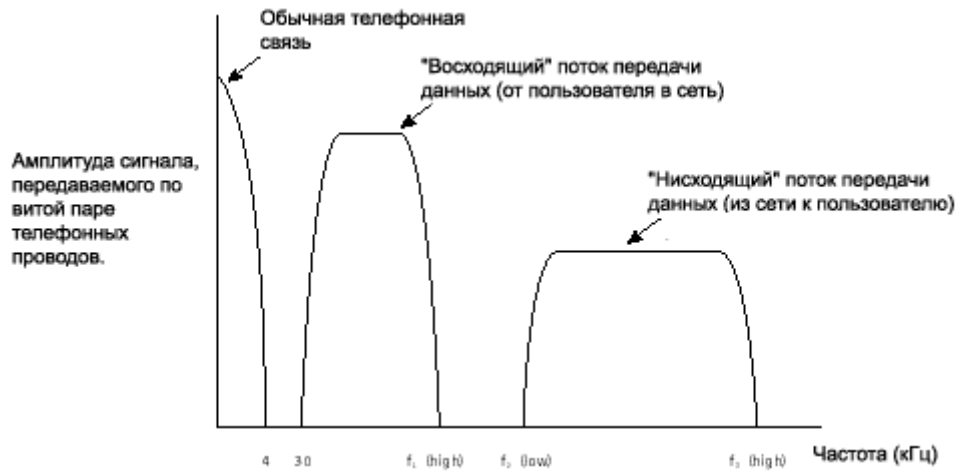


Рисунок 2

ADSL является асимметричной технологией — скорость «нисходящего» потока данных (т.е. тех данных, которые передаются в сторону конечного пользователя) выше, чем скорость «восходящего» потока данных (в свою очередь передаваемого от пользователя в сторону сети). Сразу же следует сказать, что не следует искать здесь причину для беспокойства. Скорость передачи данных от пользователя (более «медленное» направление передачи данных) все равно значительно выше, чем при использовании аналогового модема. Фактически же она также значительно выше, чем ISDN (Integrated Services Digital Network — Интегральная цифровая сеть связи).

Для сжатия большого объема информации, передаваемой по витой паре телефонных проводов, в технологии ADSL используется цифровая обработка сигнала и специально созданные алгоритмы, усовершенствованные аналоговые фильтры и аналого-цифровые преобразователи. Телефонные линии большой протяженности могут ослабить передаваемый высокочастотный сигнал (например, на частоте 1 МГц, что является обычной скоростью передачи для ADSL) на величину до 90 дБ. Это заставляет аналоговые системы модема ADSL работать с достаточно большой нагрузкой, позволяющей иметь большой динамический диапазон и низкий уровень шумов. На первый взгляд система ADSL достаточно проста — создаются каналы высокоскоростной передачи данных по обычному телефонному кабелю. Но, если детально разобраться в работе ADSL, можно понять, что данная система относится к достижениям современной технологии.

Технология ADSL использует метод разделения полосы пропускания медной телефонной линии на несколько частотных полос (также называемых несущими). Это позволяет одновременно передавать несколько сигналов по одной линии. Точно такой же принцип лежит в основе кабельного телевидения, когда каждый пользователь имеет специальный преобразователь, декодирующий сигнал и позволяющий видеть на экране телевизора футбольный матч или увлекательный фильм. При использовании ADSL разные несущие одновременно переносят различные части передаваемых данных. Этот процесс известен как частотное уплотнение линии связи (Frequency Division Multiplexing — FDM) (смотрите рисунок 3). При FDM один диапазон выделяется для передачи «восходящего» потока данных, а другой диапазон для «нисходящего» потока данных. Диапазон «нисходящего» потока в свою очередь делится на один или несколько высокоскоростных каналов и один или несколько низкоскоростных каналов передачи данных. Диапазон «восходящего» потока также делится на один или несколько низкоскоростных каналов передачи данных. Кроме этого может применяться технология эхокомпенсации (Echo Cancellation), при использовании которой диапазоны «восходящего» и «нисходящего» потоков перекрываются (смотрите рисунок 3) и разделяются средствами местной эхокомпенсации.

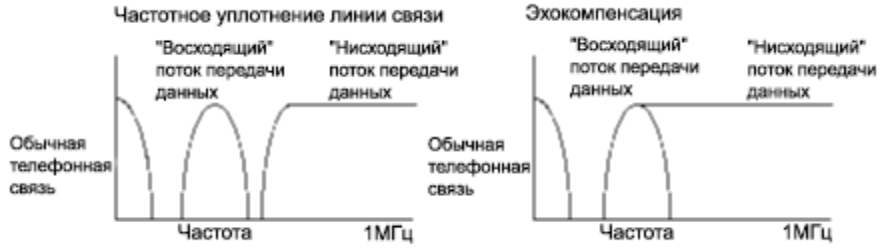


Рисунок 3

Именно таким образом ADSL может обеспечить, например, одновременную высокоскоростную передачу данных, передачу видеосигнала и передачу факса. И все это без прерывания обычной телефонной связи, для которой используется та же телефонная линия. Технология предусматривает резервирование определенной полосы частот для обычной телефонной связи (или POTS — Plain Old Telephone Service). Удивительно, как быстро телефонная связь превратилась не только в «простую» (Plain), но и в «старую» (Old); получилось что-то вроде «старой доброй телефонной связи». Однако, следует отдать должное разработчикам новых технологий, которые все же оставили телефонным абонентам узенькую полоску частот для живого общения. При этом телефонный разговор можно вести одновременно с высокоскоростной передачей данных, а не выбирать одно из двух. Более того, даже если у вас отключат электричество, обычная «старая добрая» телефонная связь будет работать по-прежнему и с вызовом электрика у вас никаких проблем не возникнет. Обеспечение такой возможности было одним из разделов оригинального плана разработки ADSL. Даже одна эта возможность дает системе ADSL значительное преимущество перед ISDN.

Одним из основных преимуществ ADSL над другими технологиями высокоскоростной передачи данных является использование самых обычных витых пар медных проводов телефонных кабелей. Совершенно очевидно, что таких пар проводов насчитывается гораздо больше (и это еще слабо сказано), чем, например, кабелей, проложенных специально для кабельных модемов. ADSL образует, если можно так сказать, «наложенную сеть». При этом дорогостоящей и отнимающей много времени модернизации коммутационного оборудования (как это необходимо для ISDN) не требуется.

ADSL является технологией высокоскоростной передачи данных, но насколько высокоскоростной? Учитывая, что буква «A» в названии ADSL означает «asymmetric» (асимметричная), можно сделать вывод, что передача данных в одну сторону осуществляется быстрее, чем в другую. Поэтому следует рассматривать две скорости передачи данных: «нисходящий» поток (передача данных от сети к вашему компьютеру) и «восходящий» поток (передача данных от вашего компьютера в сеть).

Факторами, влияющими на скорость передачи данных, являются состояние абонентской линии (т.е. диаметр проводов, наличие кабельных отводов и т.п.) и ее протяженность. Затухание сигнала в линии увеличивается при увеличении длины линии и возрастании частоты сигнала, и уменьшается с увеличением диаметра провода. Фактически функциональным пределом для ADSL является абонентская линия длиной 3,5 — 5,5 км при толщине проводов 0,5 мм. В настоящее время ADSL обеспечивает скорость «нисходящего» потока данных в пределах от 1,5 Мбит/с до 8 Мбит/с и скорость «восходящего» потока данных от 640 Кбит/с до 1,5 Мбит/с. Общая тенденция развития данной технологии обещает в будущем увеличение скорости передачи данных, особенно в «нисходящем» направлении.

Для того, чтобы оценить скорость передачи данных, обеспечиваемую технологией ADSL, необходимо сравнить ее с той скоростью, которая может быть доступна пользователям, использующим другие технологии. Аналоговые модемы позволяют передавать данные со скоростью от 14,4 до 56 Кбит/с. ISDN обеспечивает скорость передачи данных 64 Кбит/с на канал (обычно пользователь имеет доступ к двум каналам, что в сумме составляет 128 Кбит/с). Различные технологии DSL дают пользователю возможность передавать данные со скоростью 144 Кбит/с (IDSL), 1,544 и 2,048 Мбит/с (HDSL), «нисходящий» поток 1,5 — 8 Мбит/с и «восходящий» поток 640 — 1500 Кбит/с (ADSL), «нисходящий» поток 13 — 52 Мбит/с и «восходящий» поток 1,5 — 2,3 Мбит/с (VDSL). Кабельные модемы имеют скорость передачи данных от 500 Кбит/с

до 10 Мбит/с (при этом следует учитывать, что полоса пропускания кабельных модемов делится между всеми пользователями, одновременно имеющими доступ к данной линии, поэтому число одновременно работающих пользователей оказывает значительное влияние на реальную скорость передачи данных каждого из них). Цифровые линии E1 и E3 имеют скорость передачи данных, соответственно, 2,048 Мбит/с и 34 Мбит/с.

При использовании технологии ADSL полоса пропускания той линии, с помощью которой конечный пользователь связан с магистральной сетью, принадлежит этому пользователю всегда и целиком. Нужна ли вам линия ADSL? Решать вам, но для того, чтобы вы приняли правильное решение, рассмотрим некоторые преимущества ADSL.

Прежде всего, скорость передачи данных. Цифры были указаны двумя абзацами выше. Причем эти цифры не являются пределом. В новом стандарте ADSL 2 реализованы скорости 10 Мбит/с «нисходящего» и 1 Мбит/с «восходящего» потока при дальности до 3 км, а в технологии ADSL 2+, стандарт которой должен быть утверждён в 2003 году, фигурируют скорости «нисходящего» потока в 20, 30 и 40 Мбит/с (соответственно по 2,3 и 4 парам). Для того, чтобы подключиться к сети Интернет или к ЛВС, не нужно набирать телефонный номер. ADSL создает широкополосный канал передачи данных, используя уже существующую телефонную линию. После установки модемов ADSL вы получаете постоянно установленное соединение. Высокоскоростной канал передачи данных всегда готов к работе — в любой момент, когда вам это потребуется.

Полоса пропускания линии принадлежит пользователю целиком. В отличие от кабельных модемов, которые допускают разделение полосы пропускания между всеми пользователями (что в значительной мере оказывает влияние на скорость передачи данных), технология ADSL предусматривает использование линии только одним пользователем. Технология ADSL позволяет полностью использовать ресурсы линии. При обычной телефонной связи используется около одной сотой пропускной способности телефонной линии. Технология ADSL устраняет этот «недостаток» и использует оставшиеся 99% для высокоскоростной передачи данных. При этом для различных функций используются различные полосы частот. Для телефонной (голосовой) связи используется область самых низких частот всей полосы пропускания линии (приблизительно до 4 кГц), а вся остальная полоса используется для высокоскоростной передачи данных.

Многофункциональность данной системы является не самым последним аргументом в ее пользу. Так как для работы различных функций выделены различные частотные каналы полосы пропускания абонентской линии, ADSL позволяет одновременно передавать данные и говорить по телефону. Вы можете звонить по телефону и отвечать на звонки, передавать и принимать факсы, одновременно с этим находясь в сети Интернет или получая данные из корпоративной сети ЛВС. Все это по одной и той же телефонной линии. ADSL открывает совершенно новые возможности в тех областях, в которых в режиме реального времени необходимо передавать качественный видеосигнал. К ним относится, например, организация видеоконференций, обучение на расстоянии и видео по запросу. Технология ADSL позволяет провайдерам предоставлять своим пользователям услуги, скорость передачи данных которых более чем в 100 раз превышает скорость самого быстрого на данный момент аналогового модема (56 Кбит/с) и более чем в 70 раз превышает скорость передачи данных в ISDN (128 Кбит/с).

Технология ADSL позволяет телекоммуникационным компаниям предоставлять частный защищенный канал для обеспечения обмена информацией между пользователем и провайдером. Не следует забывать и о затратах. Технология ADSL эффективна с экономической точки зрения хотя бы потому, что не требует прокладки специальных кабелей, а использует уже существующие двухпроводные медные телефонные линии. То есть, если у вас дома или в офисе есть подключенный телефонный аппарат, вам не нужно прокладывать дополнительные провода для использования ADSL. (Хотя есть и ложка дегтя. Компания, обеспечивающая вам возможность обычной телефонной связи, должна при этом предоставлять и услугу ADSL.)

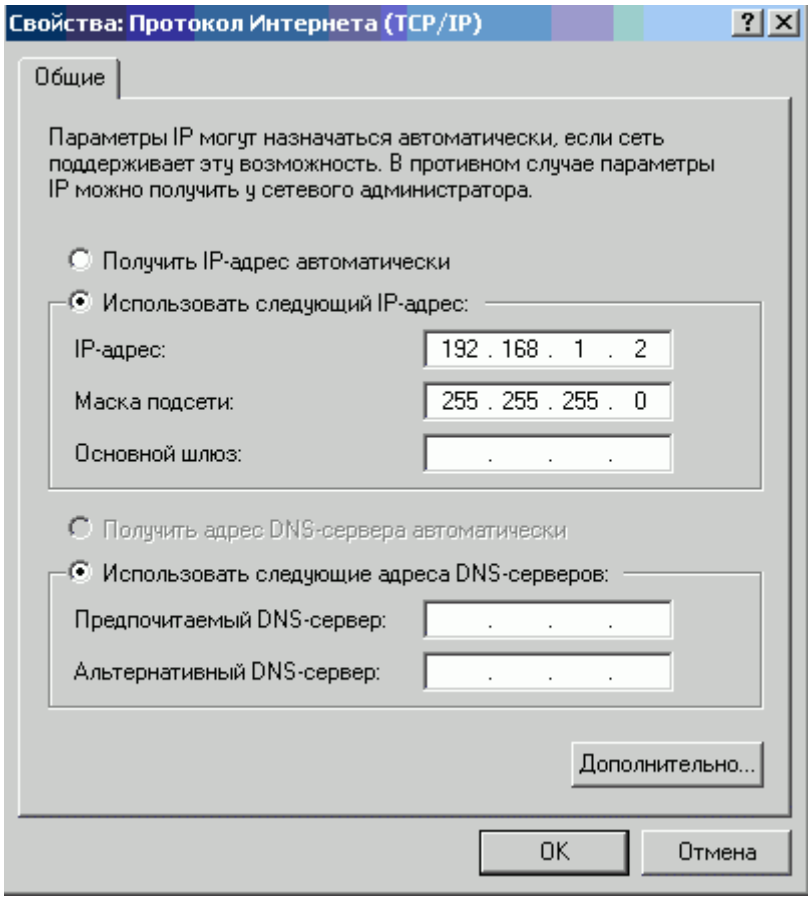
Для того, чтобы линия ADSL работала, необходимо не так уж много оборудования. На обоих концах линии устанавливаются модемы ADSL: один на стороне пользователя (дома или в офисе), а другой на стороне сети (у провайдера Интернет или на телефонной станции). Причем пользователю совсем не обязательно покупать свой модем, но достаточно взять его у провайдера в аренду.

Кроме того, пользователю для того, чтобы модем ADSL работал, необходимо иметь компьютер и интерфейсную плату, например, Ethernet 10baseT.

По мере того, как телефонные компании постепенно вступают на еще неосвоенное поле передачи данных форматов видео и мультимедиа конечному пользователю, технология ADSL продолжает играть большую роль. Разумеется, через какое-то время широкополосная кабельная сеть охватит всех потенциальных пользователей. Но успех этих новых систем будет зависеть от того, какое количество пользователей будет вовлечено в процесс использования новых технологий уже сейчас. Принося кинофильмы и телевидение, видеокаталоги и Интернет в дома и офисы, ADSL делает данный рынок жизнеспособным и прибыльным как для телефонных компаний, так и для других компаний, предоставляющих услуги в различных областях.

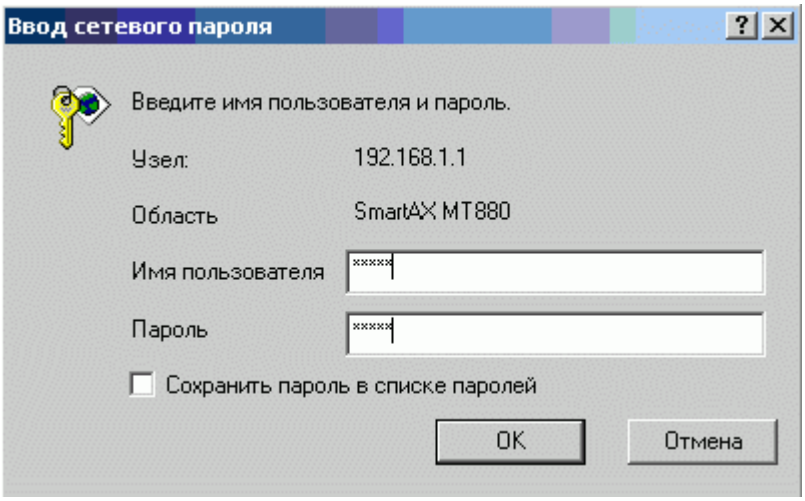
Порядок выполнения

1. Откройте свойства протокола Интернета TCP/IP в подключении по локальной сети и введите следующие параметры:

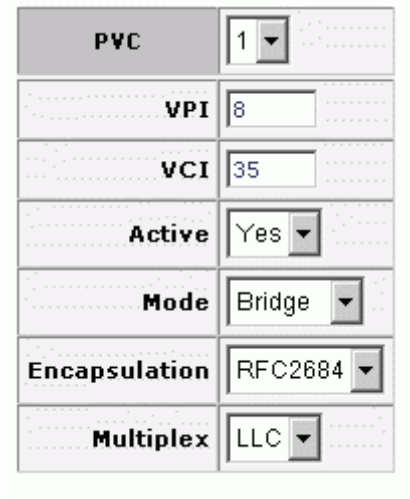


2. Запустите Web-браузер и введите адрес «192.168.1.1».

3. Введите **Имя пользователя**: «admin», **Пароль**: «admin» и нажмите **«ОК».**

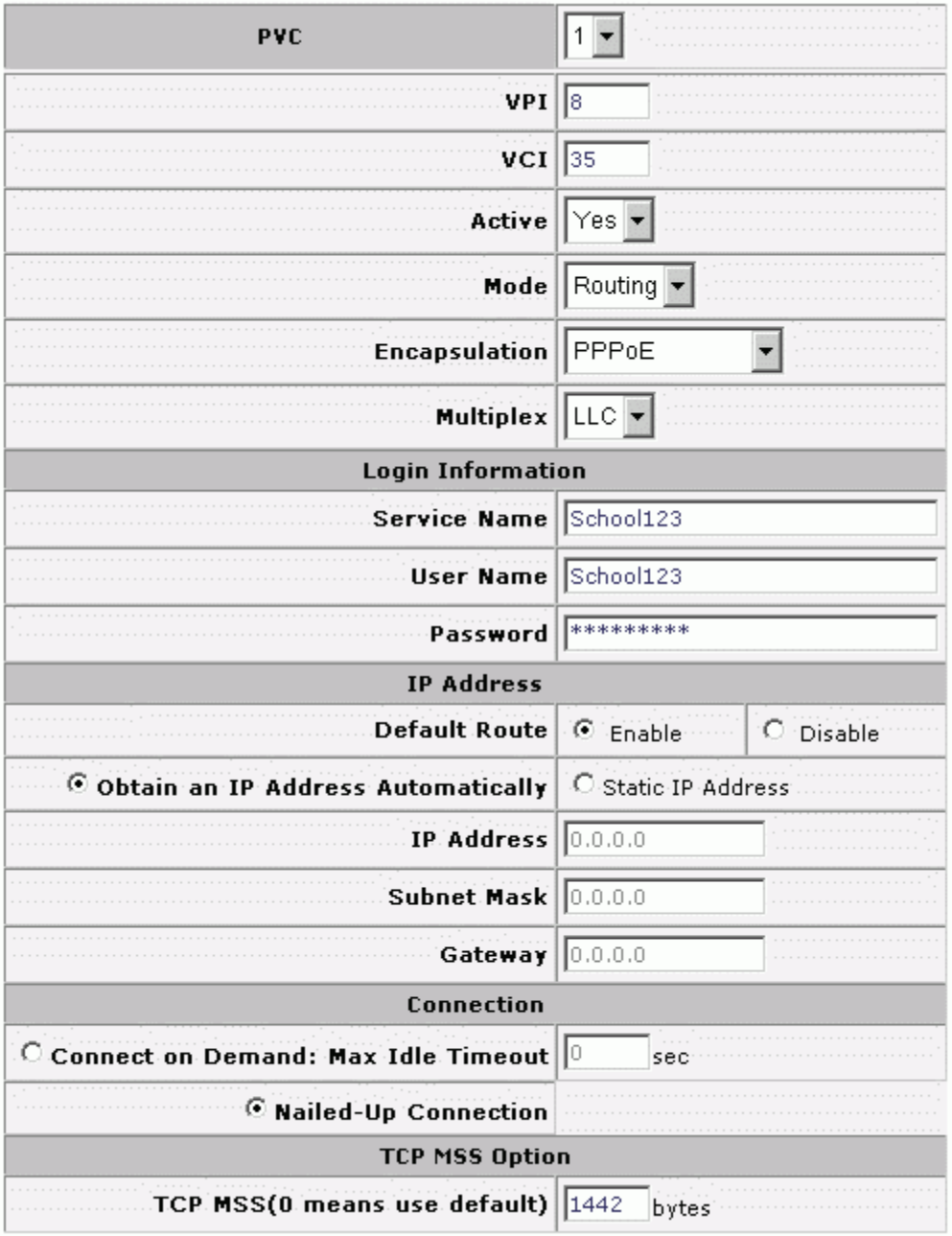


4. В меню слева выберите **«ATM Setting»**, **PVC >> 1**:



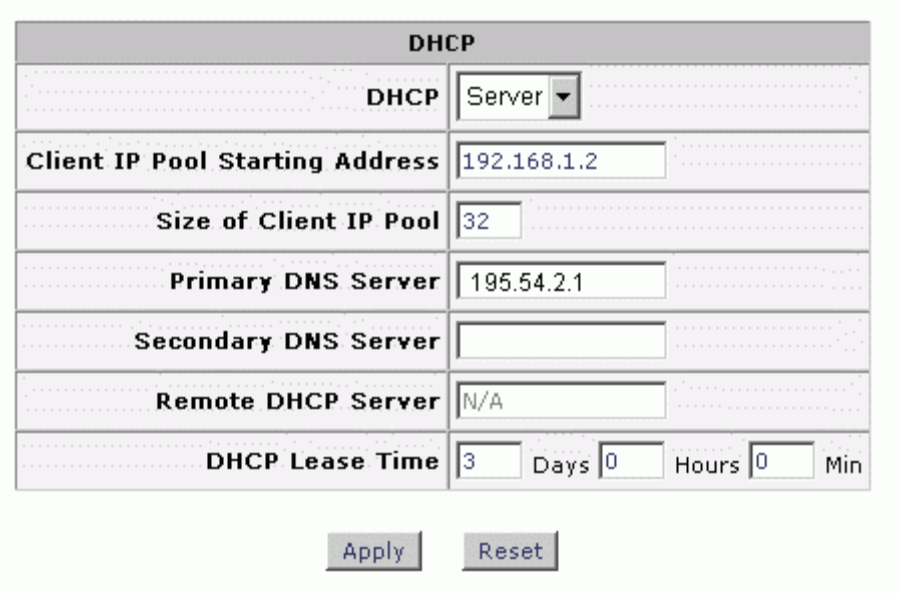
5. Выберите Mode >> Routing.
   В полях **«Service Name», «User Name», «Password»** пропишите имя абонента латинскими буквами.

В **«Default Route»** поставьте галочку **«Enable»**.

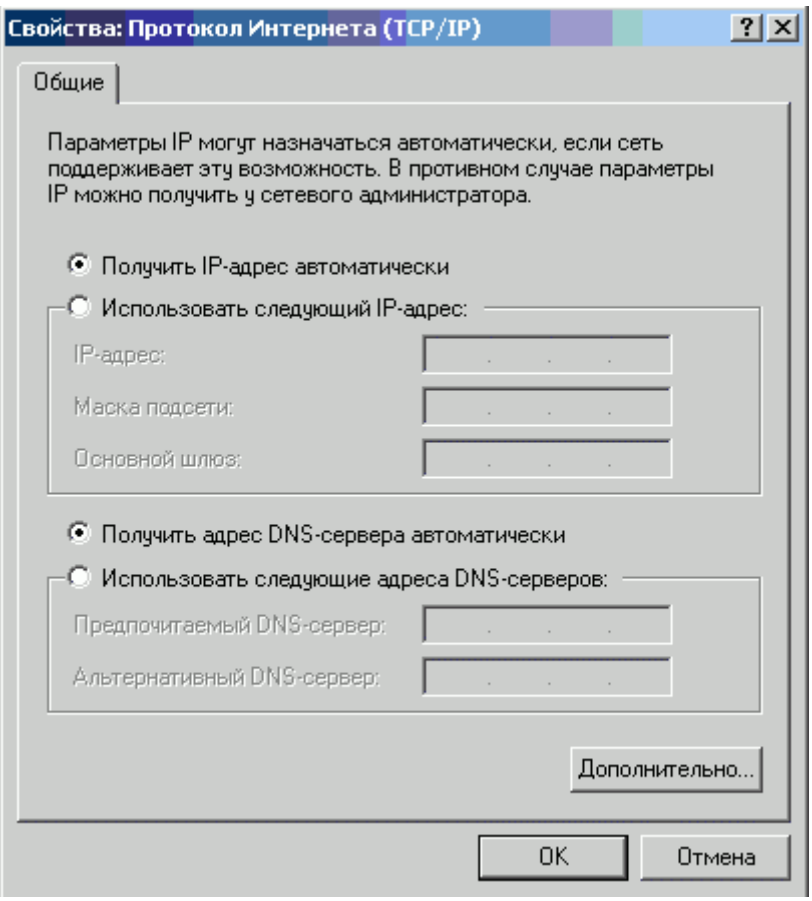


Для сохранения настроек нажмите **«Apply»**.

6. Выберите Other Setting >> DHCP Mode и настройте все так, как показано на рисунке ниже.
   DNS-сервер: 195.54.2.1.
   Нажмите **«Apply»**.



7. В диалоговом окне «Свойства: Протокол Интернета TCP/IP» пропишите следующее:



Содержание отчета

Отчет должен содержать:

- Название работы
- Цель работы
- Презентацию с выполненным заданием

Контрольные вопросы

1. Что такое технология ADSL?
2. Какое значение скорости может достигаться при использовании данной технологии?
3. Каковы ограничения применения этой технологии?

Рекомендуемая литература

Основная

1. Костров Б.В. Сети и системы передачи информации: учебник для студентов учреждений среднего профессионального образования / Б.В. Костров, В.Н. Ручкин. –М.: Издательский центр «Академия», 2017г.

Дополнительная

3. Литвинская О.С. Основы теории передачи информации: учебное пособие / Литвинская О.С., Чернышев Н.И. — Москва: КноРус, 2021 — 168 с. — ISBN 978-5-406-08653-7. — URL: https://book.ru/book/940469 (дата обращения: 23.04.2021). —Текст: электронный.

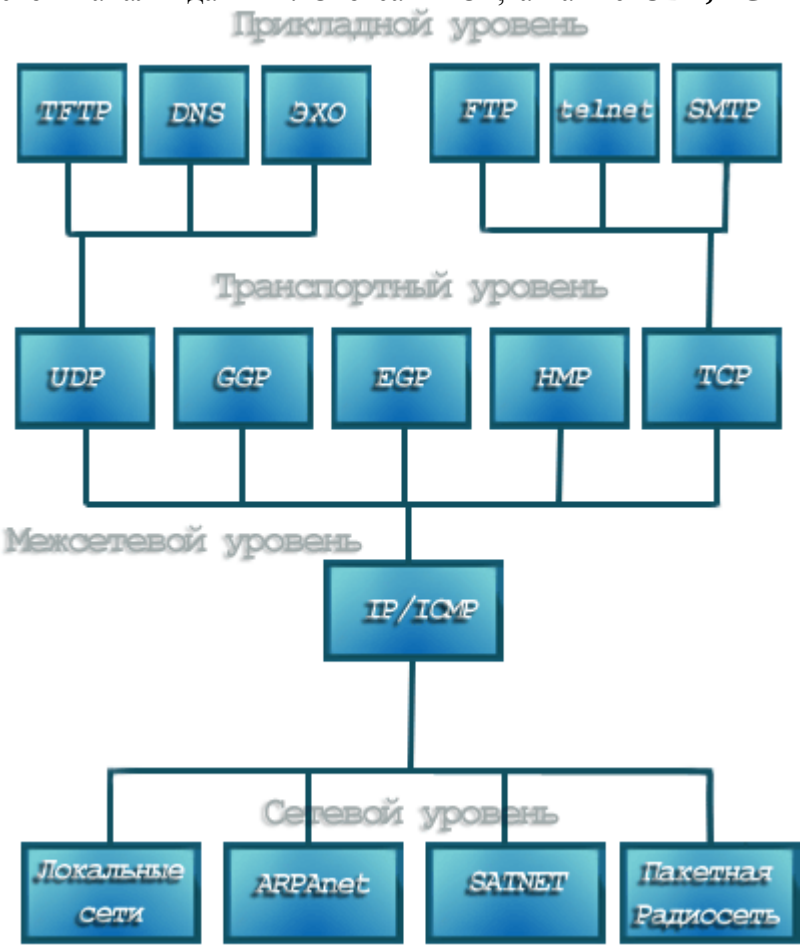
ПРАКТИЧЕСКАЯ РАБОТА № 5.1
Работа с протоколом TCP/IP

Цель работы
Получить навыки в настройке протокола **TCP/IP** в операционных системах

Оборудование: компьютерный класс.

Задание

TCP/IP - аббревиатура термина **Transmission Control Protocol/Internet Protocol** (Протокол управления передачей/Интернет Протокол) - это согласованный заранее стандарт, служащий для обмена данных между двумя узлами(компьютерами в сети), причём неважно, на какой платформе эти компьютеры и какая между ними сеть. TCP/IP служит как мост, соединяющий все узлы сети воедино, за это он и завоевал свою популярность. TCP/IP зародился в результате исследований, профинансированных ARPA (Advanced Research Project Agency) - специальным отделением правительства США в 1970-х годах. Он был задуман, как общий стандарт, который объединит все сети в единую виртуальную "сеть сетей"(internetwork). Таким образом был создан Интернет, в результате преобразования существующего конгломерата вычислительных сетей, носивших название ARPAnet, с помощью TCP/IP.
Название "TCP/IP" связано с двумя протоколами: **TCP** и **IP**. Но TCP/IP - это не только эти два протокола. Это целое семейство протоколов, объединенное под одним началом - IP-протоколом. В это семейство входят протоколы, которые взаимодействуют с протоколом IP и с его помощью строят свои каналы данных. Это сам TCP, а также **UDP, ICMP, telnet, SMTP, FTP** и многие другие.



Почему же эти протоколы повсеместно связывают друг с другом настолько тесно? Стоит сказать сначала несколько слов про протокол IP. На него возложена важная задача - маршрутизация. Он обеспечивает доставку данных по каналам(маршрутам) к адресату, т.е. отвечает за доставку данных из пункта A в пункт B. Но сам IP является дейтограмным протоколом, а значит, он не гарантирует, что посланные по нему данные придут к получателю полностью и без искажений(а такое часто происходит из-за помех на канале связи). Надёжность передачи данных по IP протоколу обеспечивают протоколы более высокого уровня. Расскажем об основных из них.

TCP - Transmission Control Protocol. Он занимается передачей больших объёмов данных по сети с помощью IP-протокола, разделяя их по частям и вновь собирая воедино в конце маршрута. При отправке с помощью TCP/IP данные кодируются и делятся на TCP-пакеты(сегменты) так, чтобы потом была возможность восстановить их при распаковке в случае их повреждения. Существуют целые науки о таком кодировании. Простым же примером обеспечения безопасности TCP-пакета является проверка на чётность(для чего к каждому байту добавляется ещё по одному биту) и хранение контрольной суммы в заголовке TCP-пакета. При помещении данных в TCP-конверт вычисляется контрольная сумма, которая записывается в TCP-заголовок. Если при приеме заново вычисленная сумма не совпадает с той, что указана на конверте, значит при передаче данные были утеряны или искажены, поэтому протокол требует пересылку этого пакета заново. Таким образом, для работы по этому протоколу TCP модули должны быть установлены и у адресата, и у отправителя такого пакета.

В большинстве случаев TCP-пакет пересылается в одной IP-дейтограмме. Но бывает, что TCP разбивает сегмент на несколько дейтограмм. Иными словами, TCP не сохраняет во время передачи границы записей, но по прибытию данные будут собраны воедино в правильной последовательности.

TCP требует от получателя подтверждения прихода данных. Он использует ожидания (таймауты) и повторные передачи для обеспечения надежной доставки. Отправителю разрешается передавать некоторое количество данных, не дожидаясь подтверждения приема ранее отправленных данных. Таким образом, между отправленными и подтвержденными данными существует "окно" уже отправленных, но ещё не подтвержденных данных. Количество байт, которое можно передавать без подтверждения, называется размером окна(этот размер устанавливается в стартовых файлах ПО). TCP является двунаправленным протоколом и данные могут передаваться по нему в двух направлениях одновременно, за счёт этого подтверждения принятия данных идут вместе с данными, идущими в этот момент в противоположном направлении. Такие возможности TCP даются не просто так. Его реализация требует немалой производительности от машины и большой пропускной способности сети.

Таким образом, протокол TCP обеспечивает гарантированную доставку с установлением логического соединения в виде байтовых потоков. Он освобождает прикладные процессы от необходимости использовать ожидания и повторные передачи для обеспечения надежности. Наиболее типичными прикладными процессами, использующими TCP, являются ftp и telnet. Кроме того, TCP использует система X-Windows. Однако бывают случаи, когда нам не столь нужна точность информации, сколь скорость передачи(например, при передаче мультимедийных данных). В таких случаях применяют другой протокол передачи данных.

User Datagram Protocol - протокол пользовательских дейтаграмм. Он приходит на смену TCP, когда нас не заботит точность передаваемых данных. Этот протокол реализует дейтограммный метод передачи данных. Дейтаграмма - это пакет, передаваемый через сеть независимо от других пакетов без установления логического соединения и подтверждения приема. Она сама содержит в себе все нужные данные для доставки.

В отличие от TCP, UDP не требует установки соединения и при передаче не делит свои дейтограммы на части. Схема без установления соединения привлекательна также тем, что позволяет при передаче данных от исходного источника к большому числу приемников минимизировать общий трафик. Использование точек разветвления (разветвителей) поможет сократить исходящий от передатчика трафик для передачи данных N машинам в N раз! Таким образом мультикастинговая передача с помощью UDP более практична, чем с TCP.

На практике UDP находит применение при транслировании мультимедийных данных, а также, например, в SNMP (Simple Network Management Protocol - простой протокол управления сетями) и многих других программах.

Альтернатива TCP - UDP - позволяет программисту гибко и рационально использовать предоставленные ресурсы, исходя из своих возможностей и потребностей. Именно для этого и служит TCP/IP. Входящие в его состав протоколы предоставляют широкие возможности настройки сети с помощью IP-протокола.

Сети бывают одноранговые и многоранговые, где число уровней редко превышает два. В одноранговой сети все ее узлы имеют равные права. Среди популярных представителей этого семейства Northern Computers, Kantech, Parsec и большинство др. систем, в том числе и российского производства. Также существует понятие одноранговой архитектуры.

Одноранговая архитектура – архитектура информационной сети, в которой:

- все абонентские системы равноправны
- каждая абонентская системы может предоставлять и потреблять ресурсы.

Недостатки одноранговой сети: необходимость иметь в каждом контролере полную базу данных; при современной стоимости полупроводниковой памяти это практически не имеет значения. Невозможность реализации некоторых глобальных функций требующих взаимосвязанной работы нескольких контроллеров.

Достоинства: максимальная «живучесть» сети, поскольку каждый контроллер имеет все необходимое для автономной работы при выключенном компьютере или повреждении элемента сети. Для систем безопасности это является существенным фактором.

В настоящее время одноранговые сети переживают небывалый подъем. Это связано с использованием p-2-p (peer to peer). Каждый пользователь Интернета может стать участником такой сети, скачав дистрибутив выбранной сети.

В одноранговой сети все рабочие станции могут выступать по отношению у другим рабочим станциям сети как серверы. То есть каждая машина в одноранговой сети является сервером для других. Используя одноранговую сеть, мы имеем дело с лесом серверов, нежели с лесом клиентов.

Состав используемой сетевой аппаратуры определяется ее выбором на стадии проектирования конфигурации сети.

Порядок выполнения

1. Внимательно прочтите пояснения к работе.
2. Произведите настройку протокола TCP/IP в ОС Windows

Для настройки сетевого интерфейса заходим «Пуск»→Настройки→Сетевые подключения→Подключение по локальной сети→Свойства→Протокол Интернета TCP/IP. В нашем случае основной шлюз, Ip-адрес и маска подсети задаются автоматически провайдером. (рис. 1)

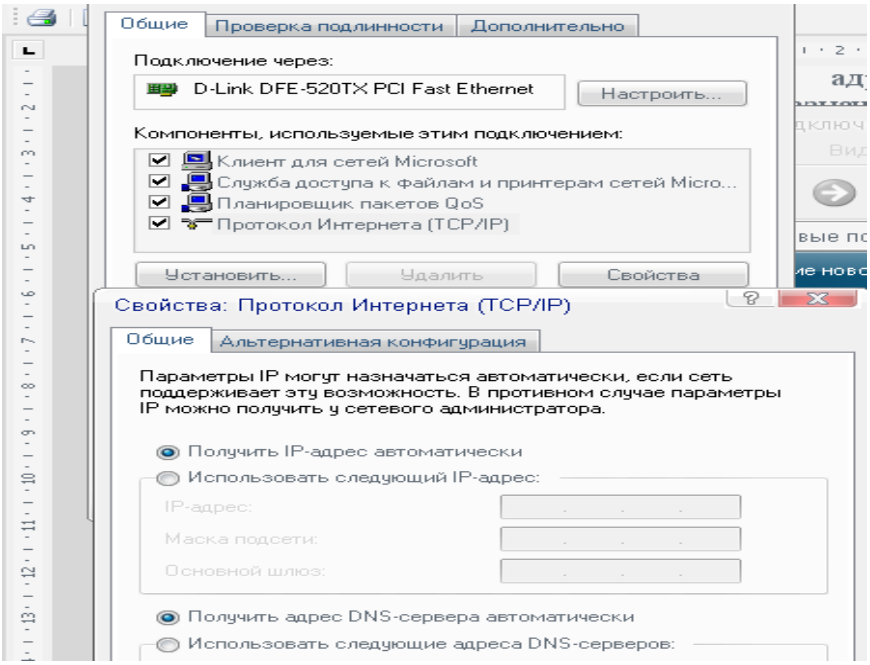


рис. 1

Может быть вариант, когда подключение вообще не установлено. Тогда после установки сетевых драйверов и подключения сетевого кабеля нужно проделать следующее:

- зайти в сетевые подключения
- выбрать раздел «Создать новое подключения»
- нажать кнопку «далее», выбрать из списка именно тот тип подключения, с помощью которого будет осуществляться передача пакетов с данными (рис. 2)

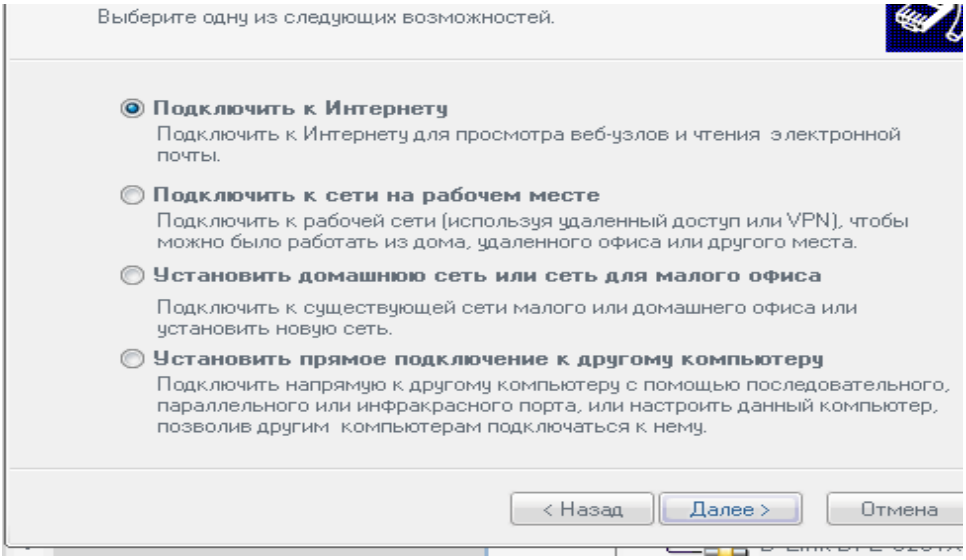


рис. 2

- в зависимости от сделанного выбора ввести либо наименование провайдера, который предоставляет канал, либо ввести необходимые параметры протокола Интернета, как было описано выше.

3. Произведите настройку одноранговой сети Windows XP.
   - Используя папку «Мой компьютер» дайте имя своему компьютеру и рабочей группе.
   - Используя папку «Мое сетевое окружение» убедитесь, что все компьютеры рабочей группы доступны.

Содержание отчета

Отчет должен содержать:

- Название работы
- Цель работы
- Описание процесса установки протокола и настройки однораноговой сети (в виде презентации)

Контрольные вопросы

1. Что такое IP-адрес?
2. Какие форматы представления IP-адресов существуют?
3. В чем достоинство и недостаток представления в каждой форме?
4. Что такое маска подсети?

Рекомендуемая литература

Основная

1. Костров Б.В. Сети и системы передачи информации: учебник для студентов учреждений среднего профессионального образования / Б.В. Костров, В.Н. Ручкин. –М.: Издательский центр «Академия», 2017г.

Дополнительная

4. Литвинская О.С. Основы теории передачи информации: учебное пособие / Литвинская О.С., Чернышев Н.И. — Москва: КноРус, 2021 — 168 с. — ISBN 978-5-406-08653-7. — URL: https://book.ru/book/940469 (дата обращения: 23.04.2021). —Текст: электронный.

ПРАКТИЧЕСКАЯ РАБОТА №5.2
Работа с протоколом TCP/IP

Цель работы

Научиться производить мониторинг и диагностировать ошибки, возникающие при настройке протокола TCP/IP.

Оборудование: компьютерный класс

Задание

Даже в самом простом случае сети с двумя узлами, существует много аппаратуры и параметров программного обеспечения, взаимосвязь между которыми может значительно влиять на эффективность работы сети. Обычно, подход к такой сложной проблеме должен начинаться с декомпозиции общей проблемы на более мелкие части и так далее, до нахождения первоисточников проблемы и затем уж выполняется систематический и логический план удаления возможных причин, пока не будет достигнуто её решение.

Так с чего же начать? Квалифицированный сетевой аналитик всегда начинает с полного понимания текущей сетевой среды. Вообще, этот подход подразумевает документирование сетевой топологии, прикладных программ и используемых протоколов.

Если сетевая конфигурация неизвестна, используйте команду ping -R hostname и/или команды traceroute. Опция - R команды ping допускает использование возможности записи маршрута IP. Отрицательный результат выполнения ping означает, что не работает или узел или сеть. Для того, чтобы узнать, что именно не работает, требуется воспользоваться другими средствами. Команда ping также не дает информации о состоянии узла-адресата. Команда traceroute, аналогично выводит маршрут, который пакеты IP берут на сетевом узле, но накапливает информацию немного по-другому.

Команда traceroute использует два способа прослеживая передачу информации до адресата: маленькое значение ttl (время жизни) и отказавший номер порта.

Traceroute запускает пакеты UDP с маленькими значениями ttl, чтобы обнаружить промежуточные маршрутизаторы. Команда traceroute была создана для сетевого тестирования, измерения и управления. Вы должны использовать её прежде всего для обнаружения неисправности вручную. Из-за нагрузки, которую она налагает на сеть, вы не должны использовать команду traceroute в течение нормальных операций или из автоматизированных сценариев.

При нормально работающей сети задокументируйте параметры, выдаваемые вам вышеуказанными командами. Это позволит вам сравнить с ними изменение параметров сети, возникшие при добавлении новой аппаратуры или программ.

Чтобы создания полного обзора эффективности и конфигурационной информации сети, используйте пакет **PerfPMR**. Чтобы получать наиболее полные данные о сети вы должны выполнить команду **perfpmr 3600** в тот час, когда нагрузка на сеть является максимальной. Выходные файлы этой команды появятся в каталоге /var/perf/tmp.

Если возможно, установите, что является "нормалью" для вашей сети, контролируя трафик в течение нескольких месяцев.

Поймите проблему

Ограничивают производительность TCP/IP в AIX обычно следующие факторы:

· недостаточное относительное быстродействие аппаратных средств;
· количество циклов CPU, необходимых для выполнения данной части кода ;
· размер пакетов передаваемых данных ;
· производительность, с которой данные кэшируются в клиентской памяти, промежуточном звене и системах сервера;
· качество кода пользователей, который обращается к подсистеме локальной вычислительной сети.

Таким образом, вы должны понять, как каждый из этих факторов способствует недостаточной сетевой эффективности.

Все узлы, присоединенные к локальной вычислительной сети совместно используют общий канал передачи. Поэтому сети с большим количеством серверов и сотнями рабочих станций, передача мультимедийных данных и т.п. могут совершенно загрузить канал передачи данных.

Настройка эффективности работы CPU является предметом особого рассмотрения и в этой книге не приводится.

Размер пакета данных также играет большую роль в ограничении эффективности сети. Обычное рассуждение приводит нас к выводу, что большие пакеты лучше, так как уменьшается количество передаваемой служебной информации (адрес и т.п.) и снижается нагрузка узлов. Это верно до той степени величины пакетов, которая не вызывает фрагментацию, так как фрагментация пакетов может представлять уже другую проблему.

При недостаточной памяти клиента для кэширования получаемых данных, некоторые данные могут быть пропущены. При постоянном заторе происходит эффект "пинг-понга", когда передающий узел всё время пытается передать пакеты принимающему узлу, а тот отбрасывает их обратно.

Выбор "правильного" инструмента

Для контроля и настройки современных гетерогенных сетей администраторы должны иметь соответствующие инструментальные средства.

Сетевые диагностические инструментальные средства можно разделить на две категории: на те, которые сообщают вам, что происходит и на те, которые, позволяют некоторым образом прореагировать на то, что происходит.

Для физического уровня: тестер (TDR)

Для сетей Ethernet, вероятно, наиболее полезный инструмент - тестер (TDR). TDR присоединяется к сети вместо одного из терминаторов. Затем тестер испускает сигнал известной мощности и формата и измеряет ответ. Каждый тип сетевой неисправности дает специфический тип ответа на TDR. Вы должны ознакомиться с документацией на тестер, чтобы интерпретировать эти ответы. Вы должны правильно установить параметры TDR для разных типов кабелей.

Для канального уровня: команда ifconfig

Вы можете использовать команду ifconfig, чтобы проверить состояние физического сетевого интерфейса (является ли он работоспособным и готовым получать пакеты, правильно ли вы его сконфигурировали, текущий адрес Internet).

Для сетевого уровня: команда tokstat

Команда tokstat отображает статистику, определенного драйвера устройства Token-Ring.

Для сетевого уровня: команда ping

Команда Packet InterNet Groper (ping) посылает дейтаграмму ECHO_REQUEST протокола ICMP (не требует наличия серверных процессов на зондируемом узле) на конкретный узел, чтобы определить является ли этот узел доступным. Часть ответа, которую вы получаете от ping - это время передачи дейтаграммы туда и обратно.

Изменяя количество данных и выдавая ping на промежуточные узлы, вы можете получать информацию о том, какие узлы включены и работают. В выполнении команды ping участвуют система маршрутизации, схемы разрешения адресов и сетевые шлюзы, поэтому для достижения успешного результата этой команды сеть должна быть в более или менее работоспособном состоянии. Если ответа от узла нет, вы можете быть совершенно уверены, что более сложные средства тем более не работают.

Для сетевого уровня: команда traceroute

Вы можете использовать команду traceroute, чтобы выявлять последовательность шлюзов, через которые проходят пакеты для достижения определенного узла.

Для сетевого уровня: команда iptrace

Вы должны использовать команду iptrace всякий раз, когда вы должны рассмотреть пакеты, которые машина посылает и получает. Но следует учитывать следующее: эта команда захватывает все передаваемые и получаемые пакеты на сетевом уровне в соответствии набору фильтров в команде iptrace. Так как эта команда является пользовательским процессом она должна конкурировать с другими процессами за CPU. Следовательно, на сильно загруженной машине, iptrace может не захватывать все пакеты. И так как iptrace отслеживает пакеты на сетевом уровне, то нет ника-

ких доказательств того, что пакет попал в кабель, так как прежде пакет должен пройти через драйвер и адаптер, чтобы добраться до кабеля.

В случаях, когда все же неясно, что приводит к заторам в сети, вы должны использовать специализированный сетевой анализатор.

Для транспортного уровня: команда tcpdump

Команда tcpdump следит за трафиком в сети и регистрирует заголовки пакета, которые соответствуют булеву выражению, задаваемому пользователем. Если никаких параметров не задано, команда будет отслеживать все пакеты в сети.

Для канального, сетевого и транспортного уровней: команда netstat

Команда netstat возвращает набор статистики относительно состояния сети. Команда netstat - хороший инструмент, чтобы помочь определить размещение проблемы.

Как только проблема изолирована, вы можете использовать более сложные инструментальные средства, чтобы продолжить её решение. Например, вы могли бы использовать команды netstat -i и netstat -v, чтобы определить, имеется ли проблема с конкретным аппаратным интерфейсом и затем выполнить диагностику, чтобы ещё более изолировать проблему.

Или, если команда netstat -s показывает, что существуют ошибки протокола, вы могли бы затем использовать команду iptrace для детализированного анализа.

Для канального, сетевого и транспортного уровней: команда netpmon

Этот инструмент контролирует и выдаёт статистику сетевого ввода-вывода и связанного с обслуживанием сети использования CPU.

Команда netpmon покажет трафик узла на канальном, сетевом и транспортном уровнях (протоколы TCP и UDP). Эта команда может также обнаружить трафик в другие сети и отображать сетевую статистику трафика сортируя информацию по узлам.

Для канального, сетевого и транспортного уровней: сетевые анализаторы

При специфических проблемах для изучения содержания пакетов данных в сети вы можете использовать анализатор протокола. Анализатор протокола фиксирует полную структуру сетевых данных, без связи с используемыми протоколами или с сетевой операционной системой. Он обрабатывает структуру как необработанные данные.

Доступны несколько коммерческих пакетов. Они будут фиксировать структуру данных и декодировать их согласно типа протокола, показывая информацию управления в соответствующих уровнях модели OSI.

Анализатор протокола - очень ценный инструмент, но требует неплохого знания сетевых протоколов.

Вы также должны знать, что термин "сетевой анализатор" может означать различные вещи у разных продавцов. Некоторые продавцы могут полагать, что сетевой монитор будет называться сетевым анализатором. Мониторы фиксируют информацию о трафике, типа количество переданных фреймов в секунду или число фреймов, которые содержат ошибки. Эти устройства не являются истинными анализаторами, так как они неспособны декодировать информацию протокола более высокого уровня, которую содержит переданный фрейм.

Для уровней от канального до прикладного: Performance Reporter

Ранее было невозможно получить сводное представление обо всех системах и сетевой эффективности в сложной и распределенной среде. IBM SystemView for AIX Performance Reporter (Performance Reporter) устраняет эту проблему обеспечивая эффективные, информативные отчеты основанные на данных, сгенерированных из встроенной базы данных. Этот инструмент позволяет часто обнаруживать возможные проблемы до их возникновения.

Данные, собранные Performance Reporter помогут вам узнать то, какие пользователи используют какие ресурсы и проанализировать узкие места и другие проблемы производительности.

Вы можете собрать информацию о производительности с узлов под управлением AIX, Sun Solaris, и HP-UX. Вы можете легко использовать данные из базы данных Performance Reporter в других прикладных программах. Модель данных хорошо зарегистрирована и просто изменяется.

Порядок выполнения

1. Внимательно изучите теоретический материал.
2. Диагностируйте ошибку и продемонстрируйте преподавателю результат.

3. Напишите отчет по работе.

Содержание отчета

Отчет должен содержать:

- Название работы
- Цель работы
- Решение индивидуального задания.

Контрольные вопросы

1. Какие основные проблемы возникают при использовании протокола TCP/IP?
2. Какие основные команды необходимо использовать при диагностике?
3. Как определить время передачи пакета?

Рекомендуемая литература

Основная

1. Костров Б.В. Сети и системы передачи информации: учебник для студентов учреждений среднего профессионального образования / Б.В. Костров, В.Н. Ручкин. –М.: Издательский центр «Академия», 2017г.

Дополнительная

5. Литвинская О.С. Основы теории передачи информации: учебное пособие / Литвинская О.С., Чернышев Н.И. — Москва: КноРус, 2021 — 168 с. — ISBN 978-5-406-08653-7. — URL: https://book.ru/book/940469 (дата обращения: 23.04.2021). —Текст: электронный.

ПРАКТИЧЕСКАЯ РАБОТА № 6
Преобразование форматов адресов

Цель работы

Изучить форматы и IP-адресов и приобрести навыки в их преобразовании

Задание

IP-адрес (ай-пи адрес, сокращение от англ. Internet Protocol Address) — уникальный идентификатор (адрес) устройства (обычно компьютера), подключённого к интернету.

Каждое устройство (компьютер, ноутбук, выделенный сервер, мобильный телефон и т.д.) в сети Интернет имеет свой IP-адрес. Так как вы в настоящий момент подключены к интернету — это означает, что и у вашего компьютера также имеется свой уникальный адрес в сети. Однако вы можете быть подключены к интернету через маршрутизатор в вашей локальной сети. В этом случае ваш компьтер из интернета виден с тем адресом, который имеет ваш маршрутизатор.

IP-адреса состоят из четырех чисел (от 0 до 255), разделенных точками и выглядят как 127.0.0.1 или 245.139.237.146.

Поскольку эти номера обычно назначаются провайдерами интернет услуг в регионе на базе блоков, IP-адрес может быть использован для определения региона или страны, из которой компьютер подключается к Интернет.

Поскольку для человека запоминать IP-адреса дело довольно утомительное, существуют специальные базы соответствий IP адресов символьным именам, которые проще запоминать. Такие имена называются узлами (hostname). Узлы могут быть преобразованы в IP адреса и наоборот.

IP адреса могут быть статические (в том случае, если отдельному пользователю провайдером выделен один постоянный адрес), а также динамическими (если провайдер выдает пользователю IP адрес в момент подключения из пула свободных адресов по DHCP).

Кроме того один компьютер на основе виртуальных узлов может действовать как несколько устройств с несколькими IP адресами и узлами. Например, — услуги хостинга в Интернет.

Знание своего IP адреса позволяет организовать доступ к службам и программам на своем компьютере (игры, чаты, FTP, удаленный доступ к рабочему столу и др.)

Вы когда-либо замечали, что IP адреса часто указаны парами (IP адрес и маска подсети)? Маска подсети говорит вам что еще более важнее, она говорит стеку tcp/ip вашего компьютера две вещи о IP адресе: (1) какая часть адреса является идентификатором сети; и (2) какая часть определяет отдельное подключение в этой сети.

Для случайного пользователя, самая важная вещь, которую можно отсюда вынести, заключается в том, что маска подсети должна быть одинаковой на всех подключениях в пределах этой подсети. Таким образом, когда настраиваете вашу локальную сеть, всюду используйте одинаковую маску подсети. Вы не обязаны использовать маску рекомендованную нами новым пользователям 255.255.255.0 но она является простой и общей при настройке небольших локальных сетей, и с ней трудно ошибиться.

Чтобы увидеть, как работает маска подсети, мы изменим обычный вид IP адреса к ее «реальной» форме, 32-битному двоичному числу, которому он соответствует:

IP адрес 90.0.0.0 =01011010000000000000000000000000

Маска подсети 255.255.255.0 =11111111111111111111111100000000

Часть IP адреса, которая соответствует разделу с единичками маски подсети это идентификатор сети. Часть с нулями это индивидуальный номер. Маска подсети должна иметь в левой ча-

сти только единички, и только нули справа. В примере выше, первые слева 24 позиции IP адреса определяют адрес сети, что объясняет другую форму записи, которую вы можете видеть иногда: 90.0.0.0/24. Это последняя форма записи дает ту же информацию, что и пара IP адрес/маска подсети.

Восемь позиций справа определяют индивидуальный адрес 90.0.0 сети. Самое маленькое значение (00000000) и самое большое значение (11111111) зарезервированы для специального использования. Самый маленький адрес 90.0.0.0 называется «адресом сети». Она используется в таблицах маршрутизации и других местах; оно также часто используется как имя, определяющее всю подсеть. Самый большой номер 90.0.0.255 называется «широковещательным адресом».

Для ваших адресов остаются номера с 00000001 до 11111110, т.е. с 1 до 254 (или впечатлите ваших друзей вычислив это следующим образом: восемь двоичных цифр с двумя исключениями 28-2 или 256-2 = 254 доступных адресов). Первый, доступный для использования в подсети 90.0.0.0 адрес 90.0.0.1. Мы рекомендуем использовать этот адрес для компьютера WinProxy. Здесь нет ничего особенного, связанного с «1» просто, его легко запомнить и также легко записать.

В простой локальной сети, часть адреса сети в IP адресе и маска подсети должны быть одинаковыми у всех компьютеров. В нашем примере здесь, все адреса локальных компьютеров будут начинаться с «90.0.0» и каждый компьютер будет иметь маску 255.255.255.0. Только индивидуальная часть IP адреса будет различной, и эта часть должна быть уникальной для каждого подключения.

Маски подсети не должны быть на границах байтов. В качестве примера запишем адрес 90.0.0.0/29:

IP адрес 90.0.0.0 =01011010000000000000000000000000

Маска подсети 255.255.255.248 =11111111111111111111111111111000

Как вы видите, вы имеете справа три бита для индивидуальных адресов. 23-2 дает вам шесть возможных адресов в каждой сети. Таким образом, 90.0.0.0 это адрес сети, 90.0.0.7 широковещательный адрес, и вы можете использовать адреса с 90.0.0.1 до 90.0.0.6 для индивидуальных адресов. Вы не теряете все остальное место. 90.0.0.8 это тоже адрес сети, и 90.0.0.15 это широковещательный адрес. Сеть 90.0.0.8/29 это совершенно другая сеть по сравнению с 90.0.0.0/29; это верно для всего доступного пространства. 90.0.0.16/29, 90.0.0.24/29 и т.д. В качестве реального примера, вы можете увидеть такой вид адресации, когда провайдер предоставляет клиентам несколько IP адресов, вместо одного.

Порядок выполнения

1. Внимательно прочтите пояснения к работе.
2. Под руководством преподавателя решите следующие задачи:
   - Для следующих IP-адресов укажите сетевые маски: 182.18.29.20, 212.23.189.5, 10.23.0.6
   - Приведите примеры IP-адресов, если заданы маски 255.255.0.0, 255.255.255.192
3. Выполните в соответствии с вариантом задание:

Вариант	Для следующих IP-адресов укажите сетевые маски	По заданной маске записать адрес сети
1	56.45.178.2	255.255.192.0
2	100.0.34.3	255.255.255.224
3	35.98.192.4	255.255.255.248

4	10.255.39.8	255.255.255.0
5	42.36.92.17	255.255.255.96
6	155.76.25.8	255.255.128.0
7	216.5.250.7	255.255.255.128
8	51.45.178.2	255.255.255.240
9	103.0.34.3	255.255.255.252
10	15.98.192.4	255.255.224.0

Содержание отчета

Отчет должен содержать:

- Название работы
- Цель работы
- Решение индивидуального задания

Контрольные вопросы

1. Что такое IP-адрес?
2. Какие форматы представления IP-адресов существуют?
3. В чем достоинство и недостаток представления в каждой форме?
4. Что такое маска подсети?

Рекомендуемая литература

Основная

1. Костров Б.В. Сети и системы передачи информации: учебник для студентов учреждений среднего профессионального образования / Б.В. Костров, В.Н. Ручкин. –М.: Издательский центр «Академия», 2017г.

Дополнительная

6. Литвинская О.С. Основы теории передачи информации: учебное пособие / Литвинская О.С., Чернышев Н.И. — Москва: КноРус, 2021 — 168 с. — ISBN 978-5-406-08653-7. — URL: https://book.ru/book/940469 (дата обращения: 23.04.2021). —Текст: электронный.

ПРАКТИЧЕСКАЯ РАБОТА № 7
Разбиение сети на подсети

Цель работы

Изучить форматы и IP-адресов и приобрести навыки в их преобразовании

Задание

IP-адрес (ай-пи адрес, сокращение от англ. Internet Protocol Address) — уникальный идентификатор (адрес) устройства (обычно компьютера), подключённого к интернету.

Каждое устройство (компьютер, ноутбук, выделенный сервер, мобильный телефон и т.д.) в сети Интернет имеет свой IP-адрес. Так как вы в настоящий момент подключены к интернету — это означает, что и у вашего компьютера также имеется свой уникальный адрес в сети. Однако вы можете быть подключены к интернету через маршрутизатор в вашей локальной сети. В этом случае ваш компьтер из интернета виден с тем адресом, который имеет ваш маршрутизатор.

IP-адреса состоят из четырех чисел (от 0 до 255), разделенных точками и выглядят как 127.0.0.1 или 245.139.237.146.

Поскольку эти номера обычно назначаются провайдерами интернет услуг в регионе на базе блоков, IP-адрес может быть использован для определения региона или страны, из которой компьютер подключается к Интернет.

Поскольку для человека запоминать IP-адреса дело довольно утомительное, существуют специальные базы соответствий IP адресов символьным именам, которые проще запоминать. Такие имена называются узлами (hostname). Узлы могут быть преобразованы в IP адреса и наоборот.

IP адреса могут быть статические (в том случае, если отдельному пользователю провайдером выделен один постоянный адрес), а также динамическими (если провайдер выдает пользователю IP адрес в момент подключения из пула свободных адресов по DHCP).

Кроме того один компьютер на основе виртуальных узлов может действовать как несколько устройств с несколькими IP адресами и узлами. Например, — услуги хостинга в Интернет.

Знание своего IP адреса позволяет организовать доступ к службам и программам на своем компьютере (игры, чаты, FTP, удаленный доступ к рабочему столу и др.)

Вы когда-либо замечали, что IP адреса часто указаны парами (IP адрес и маска подсети)? Маска подсети говорит вам что еще более важнее, она говорит стеку tcp/ip вашего компьютера две вещи о IP адресе: (1) какая часть адреса является идентификатором сети; и (2) какая часть определяет отдельное подключение в этой сети.

Для случайного пользователя, самая важная вещь, которую можно отсюда вынести, заключается в том, что маска подсети должна быть одинаковой на всех подключениях в пределах этой подсети. Таким образом, когда настраиваете вашу локальную сеть, всюду используйте одинаковую маску подсети. Вы не обязаны использовать маску рекомендованную нами новым пользователям 255.255.255.0 но она является простой и общей при настройке небольших локальных сетей, и с ней трудно ошибиться.

Чтобы увидеть, как работает маска подсети, мы изменим обычный вид IP адреса к ее «реальной» форме, 32-битному двоичному числу, которому он соответствует:

IP адрес 90.0.0.0 =01011010000000000000000000000000

Маска подсети 255.255.255.0 =11111111111111111111111100000000

Часть IP адреса, которая соответствует разделу с единичками маски подсети это идентификатор сети. Часть с нулями это индивидуальный номер. Маска подсети должна иметь в левой ча-

сти только единички, и только нули справа. В примере выше, первые слева 24 позиции IP адреса определяют адрес сети, что объясняет другую форму записи, которую вы можете видеть иногда: 90.0.0.0/24. Это последняя форма записи дает ту же информацию, что и пара IP адрес/маска подсети.

Восемь позиций справа определяют индивидуальный адрес 90.0.0 сети. Самое маленькое значение (00000000) и самое большое значение (11111111) зарезервированы для специального использования. Самый маленький адрес 90.0.0.0 называется «адресом сети». Она используется в таблицах маршрутизации и других местах; оно также часто используется как имя, определяющее всю подсеть. Самый большой номер 90.0.0.255 называется «широковещательным адресом».

Для ваших адресов остаются номера с 00000001 до 11111110, т.е. с 1 до 254 (или впечатлите ваших друзей вычислив это следующим образом: восемь двоичных цифр с двумя исключениями 28-2 или 256-2 = 254 доступных адресов). Первый, доступный для использования в подсети 90.0.0.0 адрес 90.0.0.1. Мы рекомендуем использовать этот адрес для компьютера WinProxy. Здесь нет ничего особенного, связанного с «1» просто, его легко запомнить и также легко записать.

В простой локальной сети, часть адреса сети в IP адресе и маска подсети должны быть одинаковыми у всех компьютеров. В нашем примере здесь, все адреса локальных компьютеров будут начинаться с «90.0.0» и каждый компьютер будет иметь маску 255.255.255.0. Только индивидуальная часть IP адреса будет различной, и эта часть должна быть уникальной для каждого подключения.

Маски подсети не должны быть на границах байтов. В качестве примера запишем адрес 90.0.0.0/29:

IP адрес 90.0.0.0 =01011010000000000000000000000000

Маска подсети 255.255.255.248 =11111111111111111111111111111000

Как вы видите, вы имеете справа три бита для индивидуальных адресов. 23-2 дает вам шесть возможных адресов в каждой сети. Таким образом, 90.0.0.0 это адрес сети, 90.0.0.7 широковещательный адрес, и вы можете использовать адреса с 90.0.0.1 до 90.0.0.6 для индивидуальных адресов. Вы не теряете все остальное место. 90.0.0.8 это тоже адрес сети, и 90.0.0.15 это широковещательный адрес. Сеть 90.0.0.8/29 это совершенно другая сеть по сравнению с 90.0.0.0/29; это верно для всего доступного пространства. 90.0.0.16/29, 90.0.0.24/29 и т.д. В качестве реального примера, вы можете увидеть такой вид адресации, когда провайдер предоставляет клиентам несколько IP адресов, вместо одного.

Пример:

Дан IP-адрес: 10.202.15.50/14

1. Найти адрес сети, которой он принадлежит
2. Найти broadcast полученной сети.
3. Посчитать количество эффективных IP-узлов в полученной сети.
4. Разбить полученную сеть на 8 подсетей.
   4.1. Найти маску дочерних сетей.
   4.2. Найти адреса дочерних сетей.

4.3. Найти broadcast-ы дочерних сетей.

4.4. Посчитать количество эффективных IP-узлов в дочерней сети.

Решение:

1. Дан IP-адрес: 10.202.15.50/14

Переведем в двоичное значение:

10.202.15.50=00001010.11001010.00001111. 00110010

Как видно из условия, адресу сети принадлежит первые 14 чисел:

00001010.11001000.0.0

Переведем полученное значение в десятичное: 10.200.0.0.

2. Найдем broadcast полученной сети.

00001010.11001000.00000000.00000000

11111111.11111100.00000000.00000000

00001010.11001011.11111111.11111111

10.203.255.255

3. Посчитаем количество эффективных IP-узлов в полученной сети.

К узлам относится последние 18 значений:

11.11111111.11111111

А это: 262142 узла

Не эффективных два узла: первый и последний. 262140 узла эффективных.

4. Разбиваем полученную сеть на 8 подсетей. $8=2^3$

Прибавляем степень к маске сети: 14+3=17, получим

11111111.11111111.11100000.

100000=32;

Из этого следует, что адреса дочерних сетей будут иметь следующий вид:

1) 10.200.32.0/17

2) 10.200.64.0/17

3) 10.200.96.0/17

4) 10.200.160.0/17

5) 10.200.192.0/17

6) 10.200.224.0/17

7) 10.201.0.0/17

8) 10.201.32.0/17

Найдем broadcast-ы дочерних сетей.

1) 00001010.11001000.00100000.00000000
11111111.11111111.10000000.00000000
00001010.11001000.01011111.11111111
10.200.95.255

2) 00001010.11001000.01000000.00000000 11111111.11111111.10000000.00000000
10010110.11001000.01111111.11111111
10.200.127.255

3) 00001010.11001000.01100000.00000000
11111111.11111111.10000000.00000000
10010110.11001000.00011111.11111111
10.200.31.255

4) 00001010.11001000.10100000.00000000
11111111.11111111.10000000.00000000
10010110.11001000.11011111.11111111
10.200.223.255

5) 00001010.10010110.11000000.00000000 11111111.11111111.10001000.00000000
10010110.11001000.10110111.11111111
10.200.183.255

6) 00001010.10010110.11100000.00000000 11111111.11111111.10000000.00000000
10010110. 11001000.10011111.11111111
10.200.159.255

7) 00001010.11001001.00000000.00000000
11111111.11111111.10000000.00000000
10010110.11001001.01111111.11111111
10.201.127.255

8) 00001010.11001001.00100000.00000000 11111111.11111111.10000000.00000000
10010110.10010110.01011111.11111111
10.201.95.255

4. Посчитаем количество эффективных IP-узлов в полученной сети.

К узлам относится последние 15 значений:

1111111.11111111

А это: 32768 узла. Не эффективных два узла: первый и последний. 32766 узла эффективных.

Порядок выполнения

1. Внимательно прочтите пояснения к работе.
2. Под руководством преподавателя следующие упражнения подробно проделайте разобранный пример.
3. Выполните в соответствии с вариантом задание:

1 вариант

Дан IP-адрес: 10.123.15.60/14

1. Найти адрес сети, которой он принадлежит
2. Найти broadcast полученной сети.
3. Посчитать количество эффективных IP-узлов в полученной сети.
4. Разбить полученную сеть на 8 подсетей.
   4.1. Найти маску дочерних сетей.
   4.2. Найти адреса дочерних сетей.
   4.3. Найти broadcast-ы дочерних сетей.
   4.4. Посчитать количество эффективных IP-узлов в дочерней сети.

2 вариант

Дан IP-адрес: 10.126.35.30/14

1. Найти адрес сети, которой он принадлежит
2. Найти broadcast полученной сети.
3. Посчитать количество эффективных IP-узлов в полученной сети.
4. Разбить полученную сеть на 8 подсетей.
   4.1. Найти маску дочерних сетей.
   4.2. Найти адреса дочерних сетей.
   4.3. Найти broadcast-ы дочерних сетей.
   4.4. Посчитать количество эффективных IP-узлов в дочерней сети.

3 вариант

Дан IP-адрес: 10.128.16.40/14

1. Найти адрес сети, которой он принадлежит
2. Найти broadcast полученной сети.
3. Посчитать количество эффективных IP-узлов в полученной сети.
4. Разбить полученную сеть на 8 подсетей.
   4.1. Найти маску дочерних сетей.
   4.2. Найти адреса дочерних сетей.
   4.3. Найти broadcast-ы дочерних сетей.

4.4. Посчитать количество эффективных IP-узлов в дочерней сети.

4 вариант

Дан IP-адрес: 10.113.16.80/14

1. Найти адрес сети, которой он принадлежит
2. Найти broadcast полученной сети.
3. Посчитать количество эффективных IP-узлов в полученной сети.
4. Разбить полученную сеть на 8 подсетей.
   4.1. Найти маску дочерних сетей.
   4.2. Найти адреса дочерних сетей.
   4.3. Найти broadcast-ы дочерних сетей.
   4.4. Посчитать количество эффективных IP-узлов в дочерней сети.

Содержание отчета

Отчет должен содержать:

- Название работы
- Цель работы
- Решение индивидуального задания

Контрольные вопросы

1. Что такое IP-адрес?
2. Какие форматы представления IP-адресов существуют?
3. В чем достоинство и недостаток представления в каждой форме?
4. Что такое сетевая маска?

Рекомендуемая литература

Основная

1. Костров Б.В. Сети и системы передачи информации: учебник для студентов учреждений среднего профессионального образования / Б.В. Костров, В.Н. Ручкин. –М.: Издательский центр «Академия», 2017г.

Дополнительная

7. Литвинская О.С. Основы теории передачи информации: учебное пособие / Литвинская О.С., Чернышев Н.И. — Москва: КноРус, 2021 — 168 с. — ISBN 978-5-406-08653-7. — URL: https://book.ru/book/940469 (дата обращения: 23.04.2021). —Текст: электронный.

ПРАКТИЧЕСКАЯ РАБОТА № 8
Настройка одноранговой сети

Цель работы
Приобрести навыки по настройке одноранговой сети Windows.

Оборудование: компьютерный класс.

Задание
Одноранговая сеть представляет собой сеть равноправных компьютеров – рабочих станций, каждая из которых имеет уникальное имя и адрес. Все рабочие станции объединяются в ***рабочую группу***. В одноранговой сети нет единого центра управления – каждая рабочая станция сети может отвечать на запросы других компьютеров, выступая в роли сервера, и направлять свои запросы в сеть, играя роль клиента.

Пример одноранговой сети

Одноранговые сети являются наиболее простым для монтажа и настройки, а также дешевым типом сетей. Для построения одноранговой сети требуется всего лишь несколько компьютеров с установленными клиентскими ОС, и снабженных сетевыми картами. Все параметры безопасности определяются исключительно настройками каждого из компьютеров.

К основным достоинствам одноранговых сетей можно отнести:

- простоту работы в них;
- низкую стоимость, поскольку все компьютеры являются рабочими станциями;
- относительную простоту администрирования.

Недостатки одноранговой архитектуры таковы:

- эффективность работы зависит от количества компьютеров в сети;
- защита информации и безопасность зависит от настроек каждого компьютера.

Серьезной проблемой одноранговой сетевой архитектуры является ситуация, когда компьютеры отключаются от сети. В этих случаях из сети исчезают все общесетевые сервисы, которые они предоставляли (например, общая папка на диске отключенного компьютера, или общий принтер, подключенный к нему). Администрировать такую сеть достаточно просто лишь при небольшом количестве компьютеров. Если же число рабочих станций, допустим, превышает 25-30 – то это будет вызывать определенные сложности.

Порядок выполнения

1. Установить на Oracle VM VirtualBox три гостевых операционных системы: Windows 7, Windows 7, Windows 7.
2. Настроить между ними виртуальную компьютерную сеть.
3. Присвоить каждой гостевой ОС имя, IP-адрес, объединить в рабочую группу ALFA.
4. Настроить доступ к общей папке на одной из гостевых ОС.

Содержание отчета

Отчет должен содержать:

- Название работы
- Цель работы

Контрольные вопросы

1. Что такое рабочая группа?
2. Что такое учетная запись?

Рекомендуемая литература

Основная

1. Костров Б.В. Сети и системы передачи информации: учебник для студентов учреждений среднего профессионального образования / Б.В. Костров, В.Н. Ручкин. –М.: Издательский центр «Академия», 2017г.

Дополнительная

8. Литвинская О.С. Основы теории передачи информации: учебное пособие / Литвинская О.С., Чернышев Н.И. — Москва: КноРус, 2021 — 168 с. — ISBN 978-5-406-08653-7. — URL: https://book.ru/book/940469 (дата обращения: 23.04.2021). —Текст: электронный.

ПРАКТИЧЕСКАЯ РАБОТА № 9
Настройка сети на основе выделенного сервера

Цель работы
Приобрести навыки по настройке сети на основе выделенного сервера

Оборудование: компьютерный класс.

Задание
В **иерархических сетях** выделяется один или несколько специальных компьютеров –***серверов***. Серверы обычно представляют собой высокопроизводительные ПК с серверной операционной системой (например, Windows Server 2003 или Windows Server 2008), отказоустойчивыми дисковыми массивами и системой защиты от сбоев. Как правило, на этих компьютерах локальные пользователи не работают, поэтому принято говорить о ***выделенном сервере***. Серверы управляют сетью и хранят информацию, которую совместно используют остальные компьютеры сети. Компьютеры, с которых осуществляется доступ к информации на сервере, называются ***клиентами***.

Пример иерархической сети

По-настоящему иерархической сеть становится тогда, когда в ней задействуются службы***Active Directory*** и создается ***домен Windows***. Попробую остановиться на этом подробнее:
Дело в том, что на локальном компьютере – изолированном, или входящем в одноранговую сеть, все учетные записи пользователей и настройки доступа хранятся на самом компьютере. Конкретнее, учетные записи и параметры безопасности хранятся в реестре, а права доступа к файлам – в файловой системе NTFS.
А в иерархической сети один из компьютеров назначается сервером – ***контроллером домена***. На этом компьютере может работать только серверная ОС. Именно этот сервер хранит все учетные записи пользователей и групп и параметры безопасности. Все остальные компьютеры***присоединяются к домену***. После присоединения изменяется сам принцип входа пользователей в систему. Теперь при входе пользователей в систему каждый компьютер должен запросить и получить разрешение у контроллера домена. Сеть становится ***доменом Windows***. Ее можно присоединить к домену старшего уровня, и так далее – образуется иерархическая древовидная структура.
Таким образом, в одноранговой сети вполне могут работать разные серверы – например, файловый сервер; прокси-сервер, через который осуществляется общий доступ к интернету; сервер печати и т.д. Иерархической сеть делает лишь развертывание в ней домена Windows и служб активного каталога (Active Directory).
С точки зрения системного администрирования, сеть с выделенным сервером хотя и более сложная в создании и обслуживании, но в то же время наиболее управляемая и контролируемая.

Иерархические сети обладают рядом преимуществ по сравнению с одноранговыми:

- выход из строя рабочих станций никак не сказывается на работоспособности сети в целом;
- проще организовать локальные сети с большим количеством рабочих станций;
- администрирование сети осуществляется централизованно — с сервера;
- обеспечивается высокий уровень безопасности данных.

Тем не менее, клиент-серверной архитектуре присущ ряд недостатков:

- неисправность или сбой единственного сервера может парализовать всю сеть;
- наличие выделенных серверов повышает общую стоимость сети;
- it-персонал должен обладать достаточными знаниями и навыками администрирования домена.

Выбор архитектуры сети зависит от специфики организации, назначения сети и количества рабочих станций. От выбора типа сети зависит также и ее дальнейшее будущее: расширяемость, возможность использования того или иного ПО и оборудования, надежность сети и многое другое.

Порядок выполнения

1. Установить на Oracle VM VirtualBox три гостевых операционных системы: Windows 7, Windows 7, Windows Server 2008R2.
2. Настроить между ними виртуальную компьютерную сеть.
3. Развернуть домен на базе Windows Server 2008R2.
4. Подключить рабочие станции к домену.

Содержание отчета

Отчет должен содержать:

- Название работы
- Цель работы

Контрольные вопросы

1. Что такое домен?
2. Чем отличается локальная и доменная учетная записи?

Рекомендуемая литература

Основная

1. Костров Б.В. Сети и системы передачи информации: учебник для студентов учреждений среднего профессионального образования / Б.В. Костров, В.Н. Ручкин. –М.: Издательский центр «Академия», 2017г.

Дополнительная

9. Литвинская О.С. Основы теории передачи информации: учебное пособие / Литвинская О.С., Чернышев Н.И. — Москва: КноРус, 2021 — 168 с. — ISBN 978-5-406-08653-7. — URL: https://book.ru/book/940469 (дата обращения: 23.04.2021). —Текст: электронный.

ПРАКТИЧЕСКАЯ РАБОТА № 10
Настройка Active Directory, GPO

Цель работы
Приобрести навыки по настройке Active Directory, GPO.

Оборудование: компьютерный класс.

Задание

Технология Active Directory (AD) является службой каталогов, созданной компанией Microsoft. Служба каталогов содержит данные в организованном формате и предоставляет к ним упорядоченный доступ. Служба Active Directory — это не изобретение компании Microsoft, а реализация существующей индустриальной модели (а именно X.500), коммуникационного протокола (LDAP — Lightweight Directory Access Protocol) и технологии поиска данных (службы DNS).

Изучение Active Directory следует начать со знакомства с целью, поставленной перед этой технологией. В общем плане, каталогом считается контейнер хранения данных.

Телефонный справочник является наглядным примером службы каталогов, поскольку содержит набор данных и предоставляет возможность получения необходимых сведений из каталога. Справочник содержит различные записи, каждая из которых имеет собственное значение, например, имена/фамилии абонентов, их домашний адрес и, собственно, номер телефона. В расширенном справочнике записи группируются по географическому расположению, типу или обоим признакам. Таким образом, для каждого географического расположения может быть сформирована иерархия типов записей. Кроме того, телефонный оператор также подходит под определение службы каталогов, поскольку имеет доступ к данным. Следовательно, если дать запрос на получение каких-либо данных каталога, оператор выдаст требуемый ответ на полученный запрос.

Служба каталогов Active Directory предназначена для хранения информации о всех сетевых ресурсах. Клиенты имеют возможность отправлять запросы Active Directory для получения информации о любом объекте сети. В список возможностей Active Directory входят следующие функции.

- Безопасное хранилище данных. Каждый объект в Active Directory имеет собственный список управления доступом (ACL), который содержит список ресурсов, получивших право доступа к объекту, а также предопределенный уровень доступа к этому объекту.
- Многофункциональный механизм запросов, основанный на созданном Active Directory глобальном каталоге (GC). Все клиенты, поддерживающие Active Directory, могут обращаться к этому каталогу.
- Репликация данных каталога на все контроллеры домена упрощает доступ к информации, повышает степень ее доступности и увеличивает надежность всей службы.
- Концепция модульного расширения, которая позволяет добавлять новые типы объектов или дополнять существующие объекты. Например, к объекту “пользователь” можно добавить атрибут “зарплата”.
- Сетевое взаимодействие с использованием нескольких протоколов. Служба Active Directory основана на модели X.500, благодаря чему поддерживаются различные сетевые протоколы, например, LDAP 2, LDAP 3 и HTTP.

- Для реализации службы имен контроллеров доменов и поиска сетевых адресов вместо NetBIOS используется служба DNS.

Информация каталога распределяется по всему домену, тем самым позволяя избежать чрезмерного дублирования данных.

Хотя Active Directory распределяет информацию каталога по различным хранилищам, пользователи имеют возможность запросить Active Directory на получение информации о других доменах. *Глобальный каталог* содержит сведения о всех объектах леса предприятия, помогая осуществлять поиск данных в рамках всего леса.
При запуске утилиты DCPROMO (программы повышения обычного сервера до контроллера домена) на компьютере под управлением Windows для создания нового домена, утилита создает домен на сервере DNS. Затем клиент связывается с сервером DNS для получения информации о своем домене. Сервер DNS предоставляет информацию не только о домене, но и о ближайшем контроллере домена. Клиентская система, в свою очередь, подключается к базе данных домена Active Directory на ближайшем контроллере домена с целью нахождения необходимых объектов (принтеров, файловых серверов, пользователей, групп, организационных подразделений), входящих в домен. Поскольку каждый контроллер домена хранит ссылки на другие домены в дереве, клиент может выполнять поиск во всем дереве домена.

Разновидность Active Directory, которая перечисляет все объекты в лесу доменов, доступна для тех случаев, когда необходимо найти данные за пределами дерева доменов клиента. Подобная версия называется глобальный каталог. Глобальный каталог можно хранить на любом контроллере домена в лесу AD.

Глобальный каталог предоставляет быстрый доступ к каждому объекту, который располагаться в лесу доменов, но при этом содержит только некоторые параметры объектов. Для получения всех атрибутов следует обратиться к службе Active Directory целевого домена (контроллеру интересующего домена). Глобальный каталог можно настроить на предоставление необходимых свойств объектов.

Для упрощения процесса создания объектов Active Directory контроллер домена содержит копию и иерархию классов для всего леса. Служба Active Directory содержит структуры классов в расширяемой схеме, в которую можно добавить новые классы.

Схема (schema) — это часть конфигурационного пространства имен Windows, которое поддерживается всеми контроллерами доменов в лесу. Конфигурационное пространство имен Windows состоит из нескольких структурных элементов, таких как физическое расположение, сайты Windows и подсети.
Сайт (site) содержится внутри леса и может объединять компьютеры из любого домена, причем все компьютеры сайта должны иметь быстрые и надежные сетевые соединения для резервирования данных контроллера домена.
Подсеть (subnet) — это группа IP-адресов, выделенная сайту. Подсети позволяют ускорить репликацию данных Active Directory между контроллерами доменов.

С увеличением парка компьютеров на предприятии все более остро встаёт вопрос о стоимости его управления и содержания. Ручная настройка компьютеров отнимает немало времени у персонала и заставляет, с увеличением количества компьютеров, увеличивать штат обслуживающего их персонала. К тому же при большом количестве машин следить за соблюдением принятых на предприятии стандартов настройки становится всё труднее. Групповые политики (Group Policy) являются комплексным инструментом централизованного управления компьютерами с ОС Windows 2000 и выше в домене Active Directory. К компьютерам под управлением ОС Windows NT4/9x групповые политики не применяются: они управляются системными политиками (System Policy), которые в данной статье рассматриваться не будут.

Объекты групповых политик

Все настройки, которые вы создадите в рамках групповых политик, будут храниться в объектах групповой политики (Group Policy Object, GPO). Объекты групповых политик бывают двух типов: локальный объект групповой политики и объекты групповых политик Active Directory. Локальный объект групповой политики есть на компьютерах под управлением Windows 2000 и выше. Он может быть только один, и это единственный GPO, который может быть на компьютере, не входящем в домен.

Объект групповой политики — это общее название набора файлов, директорий и записей в базе Active Directory (если это не локальный объект), которые хранят ваши настройки и определяют, какие ещё параметры вы можете изменить с помощью групповых политик. Создавая политику, вы фактически создаёте и изменяете объект групповой политики. Локальный объект групповой политики хранится в %SystemRoot%\System32\GroupPolicy. GPO Active Directory хранятся на контроллере домена и могут быть связаны с сайтом, доменом или OU (Organizational Unit, подразделение или организационная единица). Привязка объекта определяет его область действия. По умолчанию в домене создается два объекта групповой политики: Default Domain Policy и Default Domain Controller Policy. В первом определяется политика по умолчанию для паролей и учетных записей в домене. Второй связывается с OU Domain Controllers и повышает настройки безопасности для контроллеров домена.

Создание объекта групповой политики

Для того чтобы создать политику (то есть фактически создать новый объект групповой политики), открываем Active Directory Users & Computers и выбираем, где создать новый объект. Создавать и привязывать объект групповой политики можно только к объекту сайта, домена или OU.

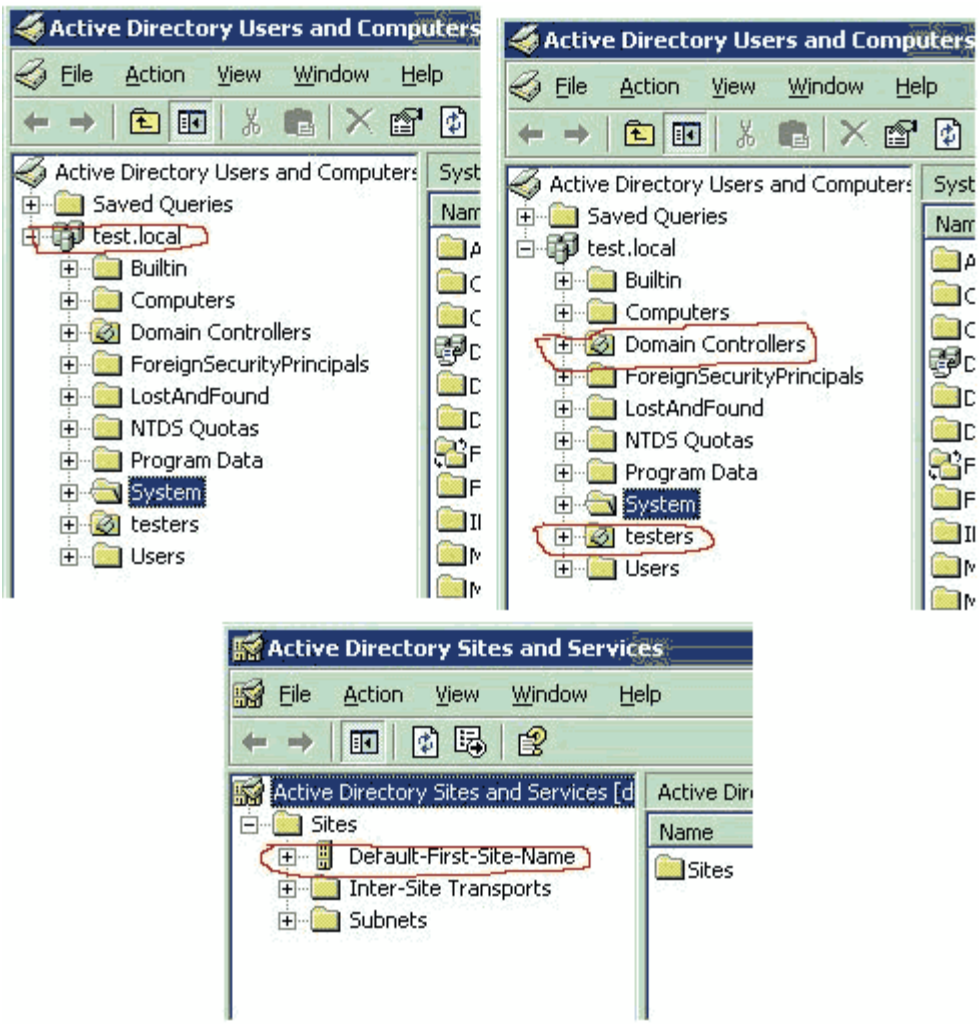


Рис. 1. Создание объекта групповой политики.

Чтобы создать GPO и связать его, например, с OU testers щёлкаем правой кнопкой мыши на этом OU и в контекстном меню выбираем properties. В открывшемся окне свойств открываем вкладку Group Policy и нажимаем New.

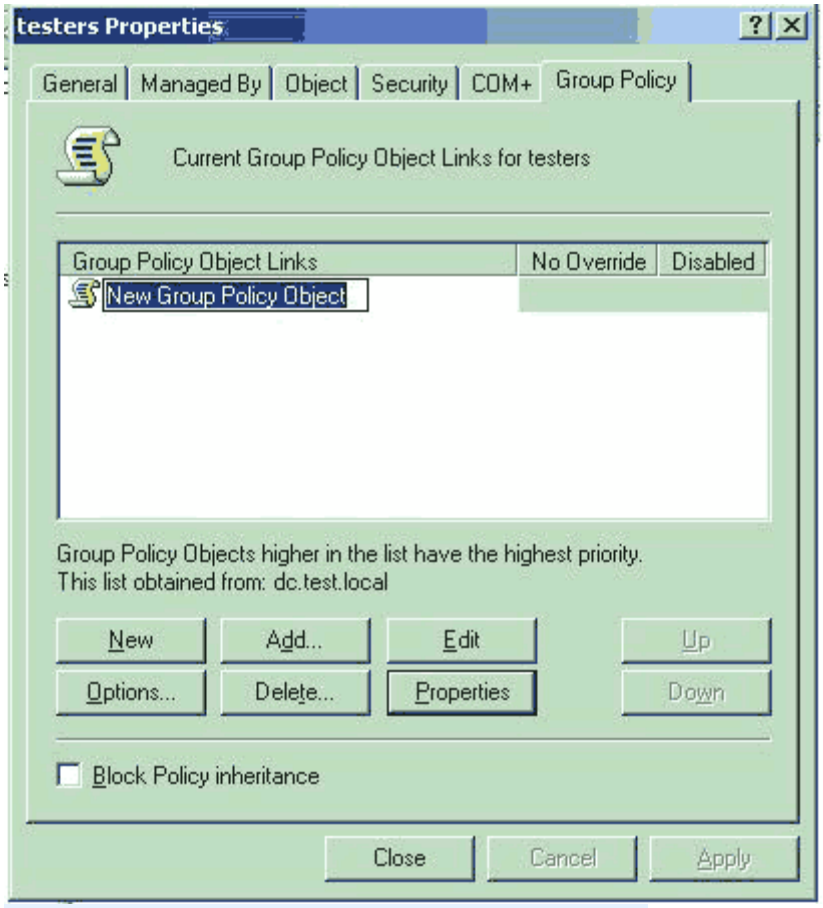


Рис. 2. Создание объекта групповой политики.

Даём название объекту GP, после чего объект создан, и можно приступать к конфигурированию политики. Дважды щёлкаем на созданном объекте или нажимаем кнопку Edit, откроется окно редактора GPO, где вы можете настроить конкретные параметры объекта.

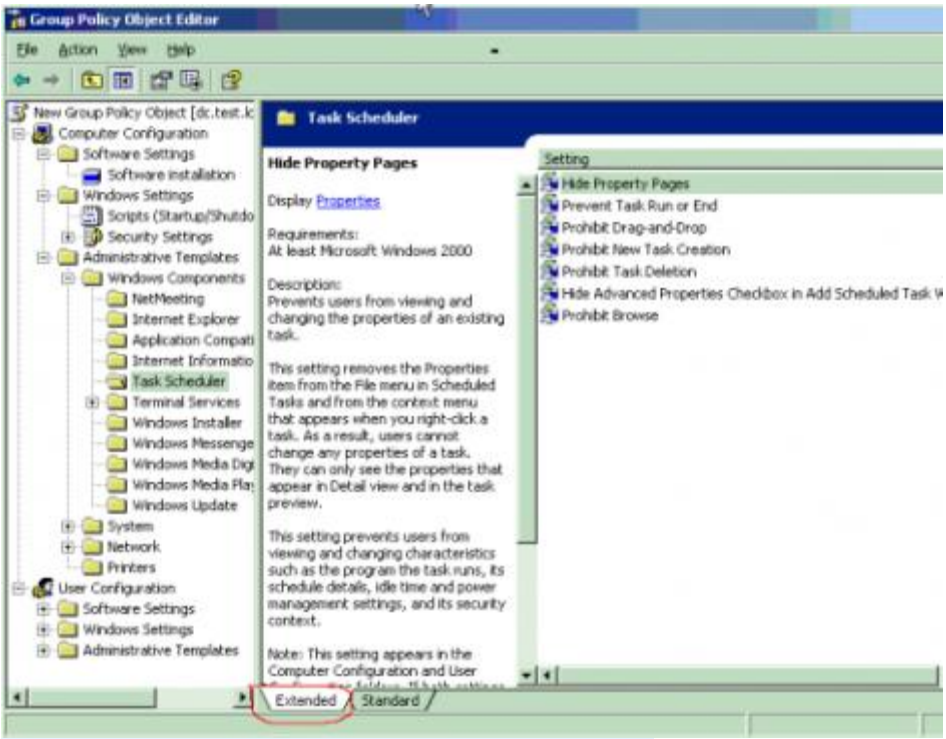


Рис. 3. Описание настроек во вкладке Extended.

Большинство основных настроек интуитивно понятны (к тому же имеют описание, если открыть вкладку Extended), и мы не будем подробно останавливаться на каждой. Как видно из рис. 3, GPO состоит из двух разделов: Computer Configuration и User Configuration. Настройки первого раздела

применяются во время загрузки Windows к компьютерам, находящимся в этом контейнере и ниже (если не отменено наследование), и не зависят от того, какой пользователь вошел в систему. Настройки второго раздела применяются во время входа пользователя в систему.

Порядок применения объектов групповой политики

Когда компьютер запускается, происходят следующие действия:

1. Читается реестр и определяется, к какому сайту принадлежит компьютер. Делается запрос серверу DNS с целью получения IP адресов контроллеров домена, расположенных в этом сайте.
2. Получив адреса, компьютер соединяется с контроллером домена.
3. Клиент запрашивает список объектов GP у контроллера домена и применяет их. Последний присылает список объектов GP в том порядке, в котором они должны применяться.
4. Когда пользователь входит в систему, компьютер снова запрашивает список объектов GP, которые необходимо применить к пользователю, извлекает и применяет их.

Групповые политики применяются при загрузке ОС и при входе пользователя в систему. Затем они применяются каждые 90 минут, с вариацией в 30 минут для исключения перегрузки контроллера домена в случае одновременного запроса большого количества клиентов. Для контроллеров домена интервал обновления составляет 5 минут. Изменить это поведение можно в разделе Computer Configuration\Administrative Templates\System\Group Policy. Объект групповой политики может действовать только на объекты «компьютер» и «пользователь». Политика действует только на объекты, находящиеся в объекте каталога (сайт, домен, подразделение), с которым связан GPO и ниже по «дереву» (если не запрещено наследование). Например: Объект GPO создан в OU testers (как мы сделали выше).

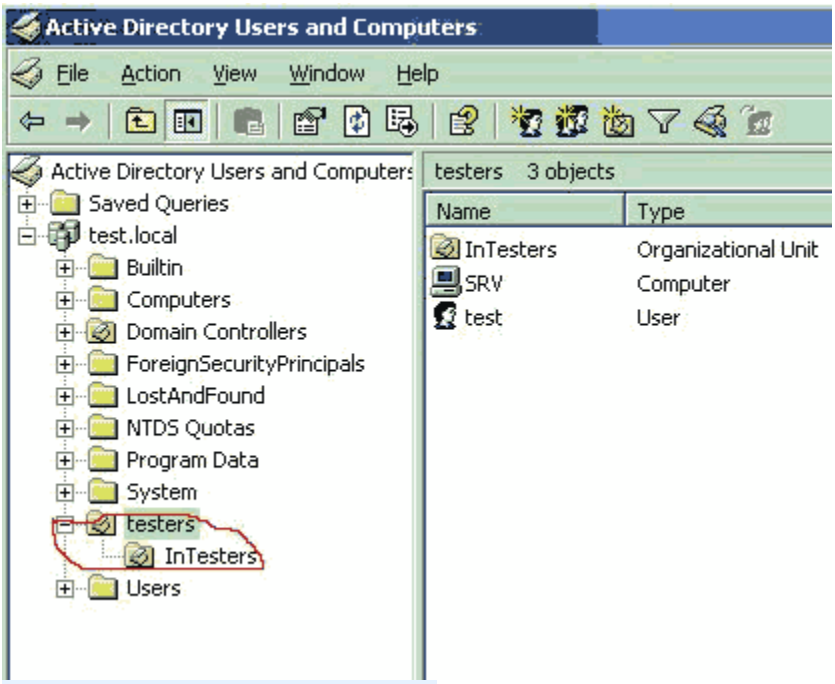


Рис. 4. Наследование настроек.

Все настройки, сделанные в этом GPO, будут действовать только на пользователей и компьютеры, находящиеся в OU testers и OU InTesters. Рассмотрим порядок применения политик на примере. Пользователь test, расположенный в OU testers, входит на компьютер comp, находящийся в OU compOU (см. рис. 5).

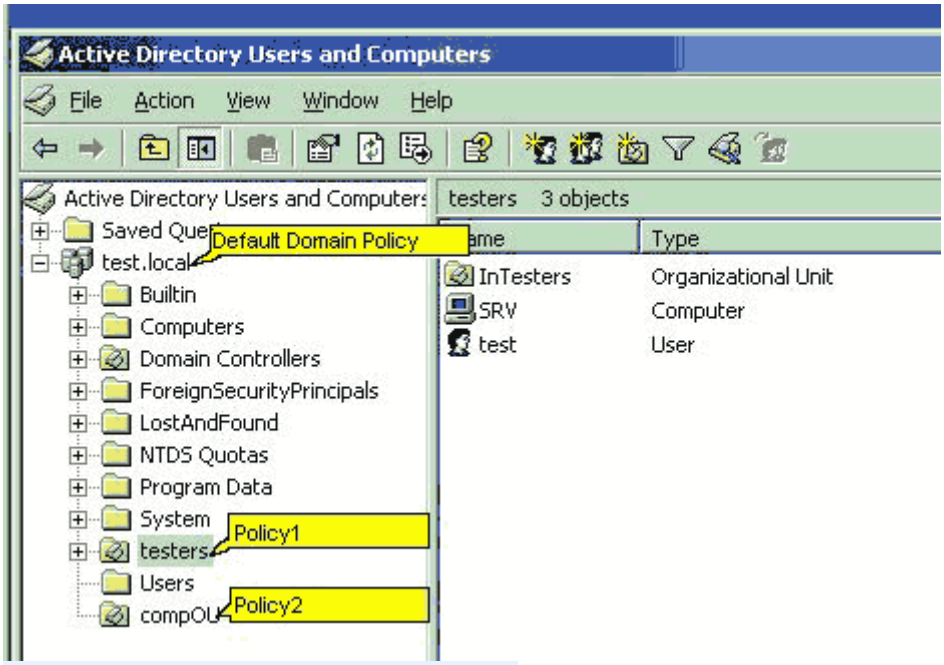


Рис. 5. Порядок применения политик.

В домене существуют четыре GPO:

1. SitePolicy, связанный с контейнером сайта;
2. Default Domain Policy, связанный с контейнером домена;
3. Policy1, связанный с OU testers;
4. Policy2, связанный с OU compOU.

При загрузке Windows на рабочей станции comp, параметры, определённые в разделах Computer Configuration, применяются в таком порядке:

1. Параметры локального GPO;
2. Параметры GPO SitePolicy;
3. Параметры GPO Default Domain Policy;
4. Параметры GPO Policy2.

При входе пользователя test на компьютер comp — параметры, определенные в разделах User Configuration:

1. Параметры локального GPO;
2. Параметры GPO SitePolicy;
3. Параметры GPO Default Domain Policy;
4. Параметры GPO Policy1.

То есть GPO применяются в таком порядке: локальные политики, политики уровня сайта, политики уровня домена, политики уровня OU.

Групповые политики применяются к клиентам с ОС Windows XP асинхронно, а с ОС Windows 2000 — синхронно, то есть пользовательский экран входа появляется только после применения всех политик компьютера, а политики пользователя применяются до того, как появился рабочий стол. Асинхронное применение политик означает, что пользовательский экран входа появляется раньше, чем успевают примениться все политики компьютера, а рабочий стол — раньше, чем применятся все пользовательские политики, что приводит к ускорению загрузки и входа пользователя.
Описанное выше поведение изменяется в двух случаях. Первый — компьютер клиента обнаружил медленное сетевое подключение. По умолчанию в этом случае применяются только параметры настройки защиты и административные шаблоны. Медленным считается подключение с пропускной способностью менее 500 Кб/сек. Изменить это значение можно в Computer Configuration\Administrative Templates\System\Group Policy\Group Policy slow link detection. Также

в разделе Computer Configuration\Administrative Templates\System\Group Policy можно настроить некоторые другие параметры политик так, чтобы и они обрабатывались по медленному соединению. Второй способ изменения порядка применения политик — опция User Group policy loopback processing. Эта опция изменяет порядок применения политик по умолчанию, при котором пользовательские политики применяются после компьютерных и перезаписывают последние. Вы можете установить опцию loopback, чтобы политики компьютера применялись после пользовательских политик и перезаписывали все пользовательские политики, противоречащие политикам компьютера. У параметра loopback есть 2 режима:

1. Merge (соединить) — сначала применяется компьютерная политика, затем пользовательская и снова компьютерная. При этом компьютерная политика заменяет противоречащие ей параметры пользовательской политики своими.
2. Replace (заменить) — пользовательская политика не обрабатывается.

Проиллюстрировать применение параметра User Group policy loopback processing можно, например, на общедоступном компьютере, на котором необходимо иметь одни и те же ограниченные настройки, независимо от того, какой пользователь им пользуется.

Приоритетность, наследование и разрешение конфликтов

Как вы уже заметили, на всех уровнях объекты групповой политики содержат одинаковые параметры настройки, и один и тот же параметр может быть определён на нескольких уровнях поразному. В таком случае действующим значением будет применившееся последним (о порядке применения объектов групповой политики говорилось выше). Это правило распространяется на все параметры, кроме определённых как not configured. Для этих параметров Windows не предпринимает никаких действий. Но есть одно исключение: все параметры настройки учётных записей и паролей могут быть определены только на уровне домена, на остальных уровнях эти настройки будут проигнорированы.

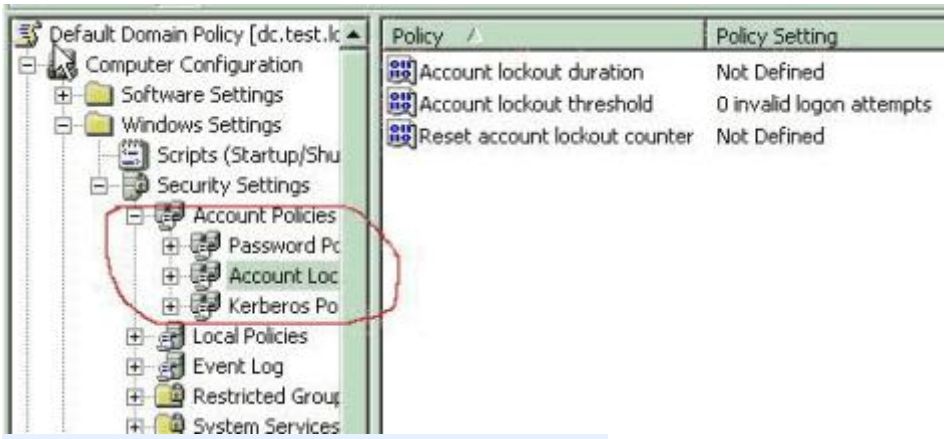


Рис. 6. Active Directory Users and Computers.

Если на одном уровне расположены несколько GPO, то они применяются «снизу вверх». Изменяя положение объекта политик в списке (кнопками Up и Down), можно выбрать необходимый порядок применения.

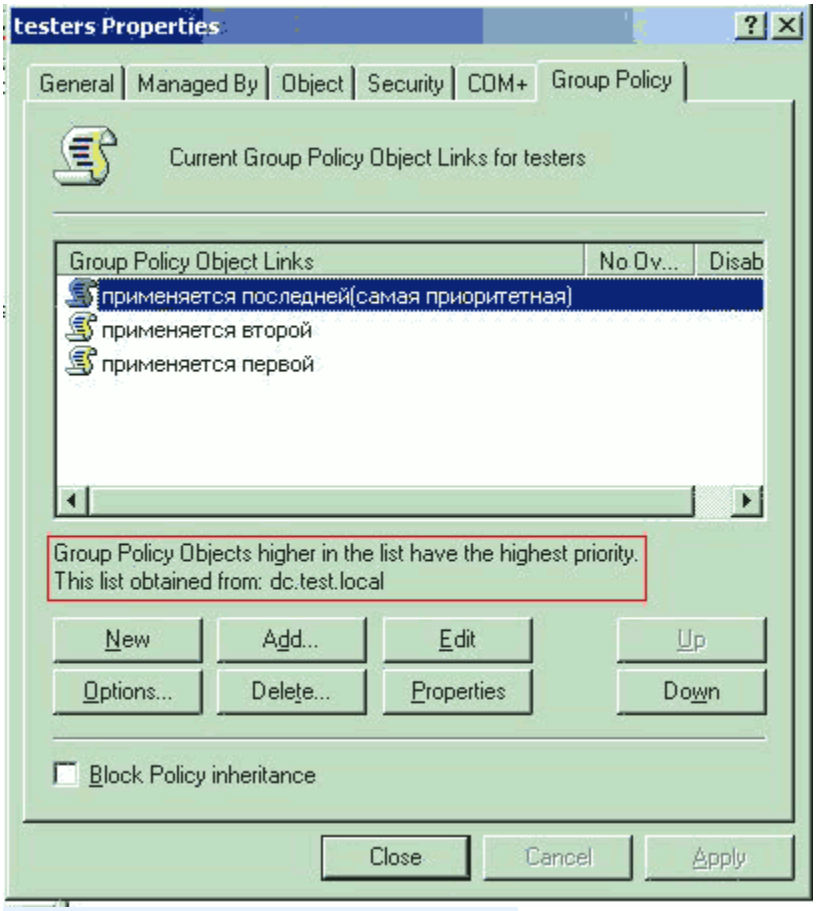


Рис. 7. Порядок применения политик.

Иногда нужно, чтобы определённая OU не получала параметры политик от GPO, связанных с вышестоящими контейнерами. В этом случае нужно запретить наследование политик, поставив флажок Block Policy inheritance (Блокировать наследование политик). Блокируются все наследуемые параметры политик, и нет способа блокировать отдельные параметры. Параметры настройки уровня домена, определяющие политику паролей и политику учетных записей, не могут быть заблокированы.

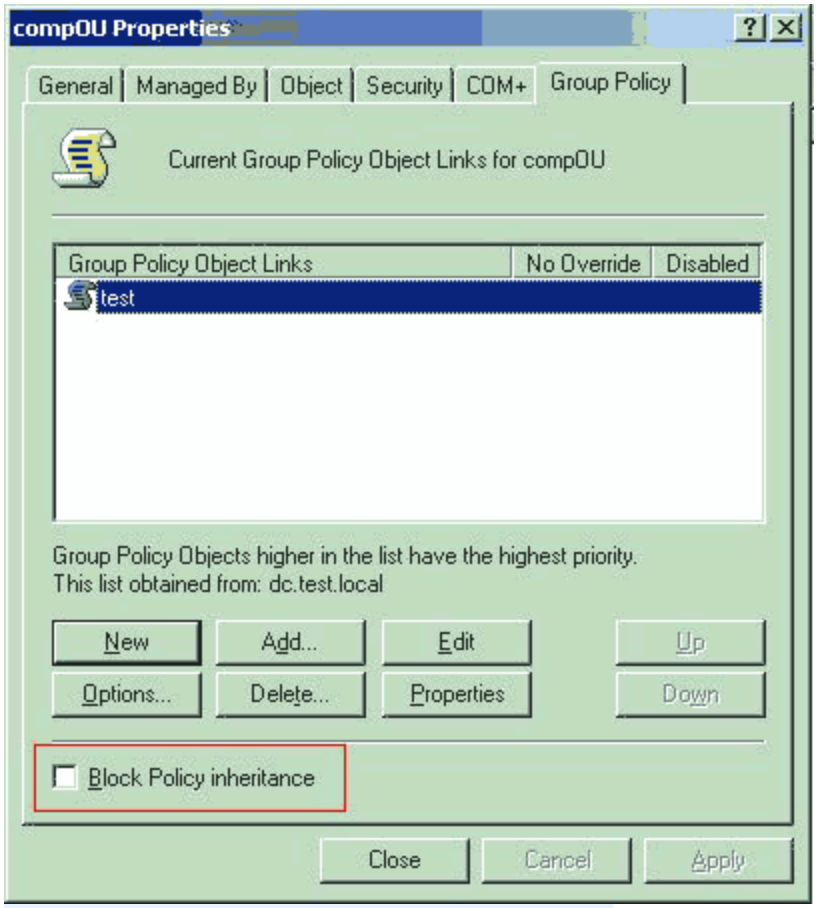


Рис. 9. Блокирование наследования политик.

В случае если требуется, чтобы определённые настройки в данном GPO не перезаписывались, следует выбрать нужный GPO, нажать кнопку Options и выбрать No Override. Эта опция предписывает применять параметры GPO там, где заблокировано наследование политик. No Override устанавливается в том месте, где GPO связывается с объектом каталога, а не в самом GPO. Если GPO связан с несколькими контейнерами в домене, то для остальных связей этот параметр не будет сконфигурирован автоматически. В случае если параметр No Override сконфигурирован для нескольких связей на одном уровне, приоритетными (и действующими) будут параметры GPO, находящегося вверху списка. Если же параметры No Override сконфигурированы для нескольких GPO, находящихся на разных уровнях, действующими будут параметры GPO, находящегося выше в иерархии каталога. То есть, если параметры No override сконфигурированы для связи GPO с объектом домена и для связи с GPO объектом OU, действующими будут параметры, определённые на уровне домена. Галочка Disabled отменяет действие этого GPO на данный контейнер.

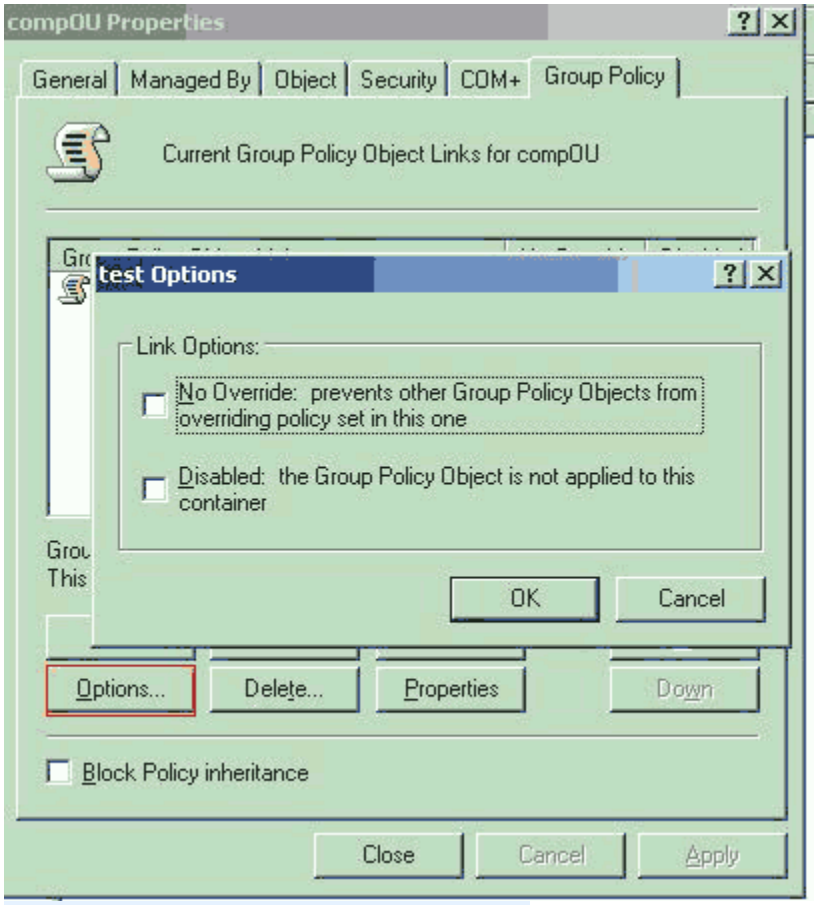


Рис. 10. Опции No Override и Disabled.

Как уже было сказано выше, политики действуют только на пользователей и компьютеры. Часто возникает вопрос: «как сделать так, чтобы определенная политика действовала на всех пользователей, входящих в определенную группу безопасности?». Для этого GPO привязывается к объекту домена (или любому контейнеру, находящемуся выше контейнеров или OU, в которых находятся все объекты пользователей из нужной группы) и настраиваются параметры доступа. Нажимаем Properties, на вкладке Security удаляем группу Authenticated Users и добавляем требуемую группу с правами Read и Apply Group Policy.

Определение настроек, действующих на компьютер пользователя

Для определения конечной конфигурации и выявления проблем вам потребуется знать, какие настройки политик действуют на данного пользователя или компьютер в данный момент. Для этого существует инструмент Resultant Set of Policy (результирующий набор политик, RSoP). RSoP может работать как в режиме регистрации, так и в режиме планирования. Для того чтобы вызвать RSoP, следует нажать правой кнопкой на объекте «пользователь» или «компьютер» и выбрать All Tasks.

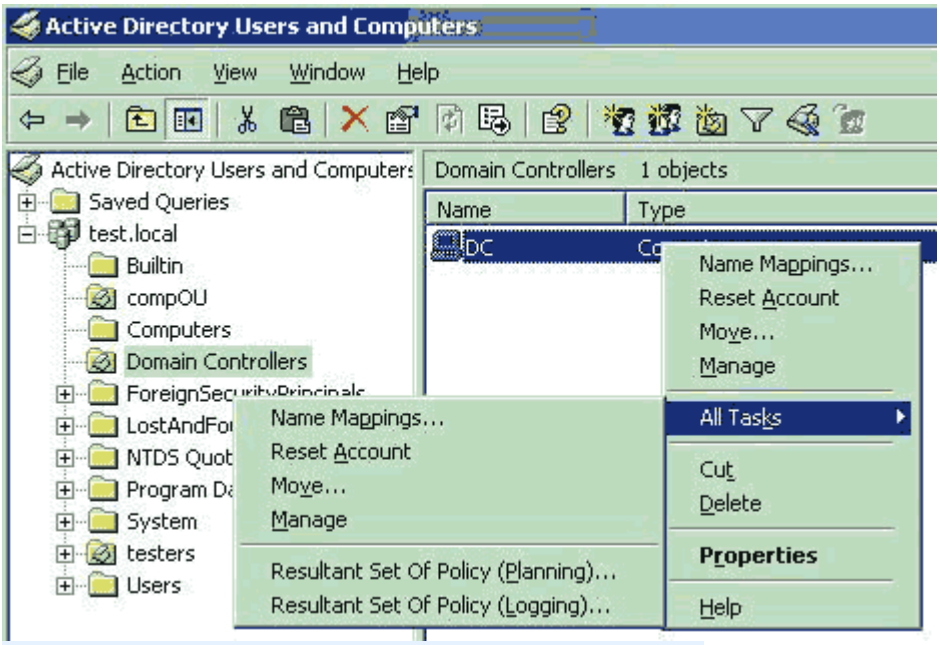


Рис. 11. Вызов инструмента Resultant Set of Policy.

После запуска (в режиме регистрации, logging) вас попросят выбрать, для какого компьютера и пользователя определить результирующий набор, и появится окно результирующих настроек с указанием, из какого GPO какой параметр применился.

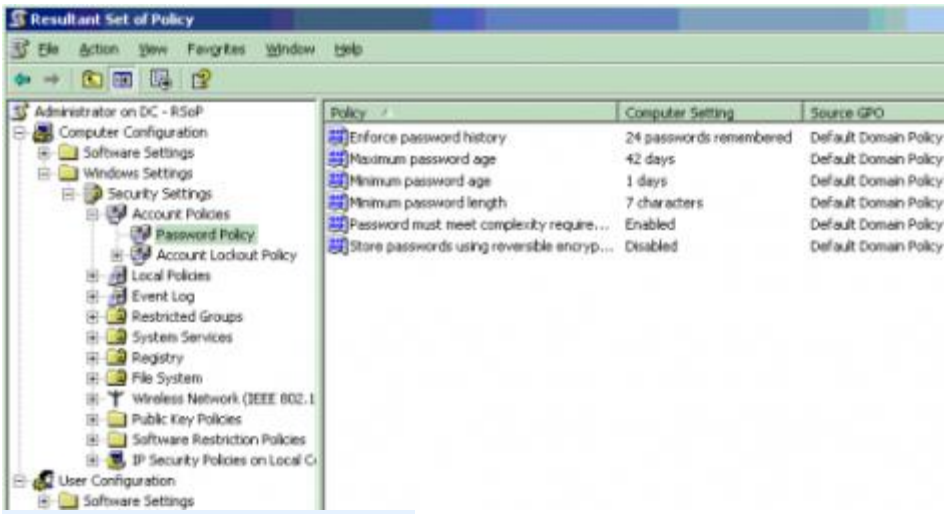


Рис. 12. Resultant Set of Policy.

Другие инструменты управления групповыми политиками

GPResult — это инструмент командной строки, обеспечивающий часть функционала RSoP. GPResult есть по умолчанию на всех компьютерах с Windows XP и Windows Server 2003.

GPUpdate принудительно запускает применение групповых политик — как локальных, так и основанных на Active Directory. В Windows XP/2003 пришла на смену параметру /refreshpolicy в инструменте secedit для Windows 2000.

Описание синтаксиса команд доступно при запуске их с ключём /?.

Порядок выполнения

1. Установить на Oracle VM VirtualBox три гостевых операционных системы: Windows 7, Windows 7, Windows Server 2008R2.
2. Настроить между ними виртуальную компьютерную сеть.
3. Развернуть домен на базе Windows Server 2008R2.
4. Настроить AD, GPO по заданию преподавателя.

Содержание отчета

Отчет должен содержать:

- Название работы
- Цель работы

Контрольные вопросы

1. Что такое Active Directory?
2. Что такое редактор GPO?

Рекомендуемая литература

Основная

1. Костров Б.В. Сети и системы передачи информации: учебник для студентов учреждений среднего профессионального образования / Б.В. Костров, В.Н. Ручкин. –М.: Издательский центр «Академия», 2017г.

Дополнительная

10. Литвинская О.С. Основы теории передачи информации: учебное пособие / Литвинская О.С., Чернышев Н.И. — Москва: КноРус, 2021 — 168 с. — ISBN 978-5-406-08653-7. — URL: https://book.ru/book/940469 (дата обращения: 23.04.2021). —Текст: электронный.

ПРАКТИЧЕСКАЯ РАБОТА № 11
Настройка свойств Web-браузера

Цель работы

Научиться использовать расширенные возможности Web-браузера

Оборудование: компьютерный класс.

Задание

Веб-обозреватель, или браузер (от англ. Web browser) — это программное обеспечение для поиска, просмотра веб-сайтов, то есть для запроса веб-страниц (преимущественно из Сети), для их обработки, вывода и перехода от одной страницы к другой.

Большинство браузеров также наделены способностями к просмотру оглавления FTP-серверов.

Браузеры постоянно развивались со времён зарождения Всемирной паутины, и с её ростом становились всё более важной программой типичного персонального компьютера. Ныне браузер — комплексное приложение для обработки и вывода разных составляющих веб-страницы, и для предоставления интерфейса между веб-сайтом и его посетителем. Практически все популярные браузеры распространяются бесплатно или «в комплекте» с другим приложением: Internet Explorer (как неотъемлемая часть Microsoft Windows), Mozilla Firefox (бесплатно, свободное ПО), Opera (бесплатно, начиная с версии 8.50), Safari (совместно с Mac OS или бесплатно для Windows).

Порядок выполнения

1. Запустите приложение Internet Explorer. Произведите тонкую настройку браузера и проверьте результаты при использовании сети Интернет.
2. Обозреватель Internet Explorer, как и все программы, входящие в Microsoft Office, можно настроить. Для настройки используется диалоговое окно Свойства обозревателя (рис.1), открываемое при выборе одноименной команды в меню Сервис. Среди настраиваемых параметров: вид домашней страницы обозревателя Internet Explorer, цвет текста и фона Web-страниц, используемые шрифты и языки, защита передаваемой и получаемой информации, ограничение доступа к Web-страницам и т. п. Рассмотрим более подробно диалоговое окно Свойства обозревателя и настраиваемые с его помощью параметры работы программы.

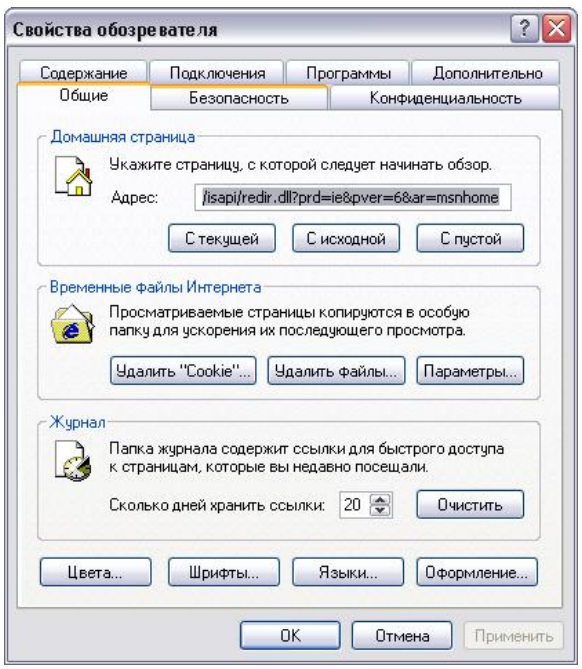


Рис. 1. Диалоговое окно Свойства обозревателя

Для настройки основных параметров обозревателя Internet Explorer предназначена вкладка Общие диалогового окна Свойства обозревателя.

Область Домашняя страница позволяет задать страницу, называемую домашней и загружаемую по умолчанию при каждом запуске обозревателя. Именно к этой странице осуществляется переход при нажатии кнопки Домой на панели инструментов окна обозревателя. В области Домашняя страница расположено поле, содержащее адрес страницы, и три кнопки: С текущей, С исходной, С пустой. При нажатии кнопки С текущей в поле Адрес заносится адрес страницы, открытой в обозревателе в данный момент. Нажатие кнопки С исходной приводит к установке в качестве домашней страницы — страницы Microsoft, имеющей адрес http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=5.5&ar=msnhome. Кнопка С пустой устанавливает в качестве домашней пустую страницу.

Программа Internet Explorer при просмотре Web-страниц помещает их содержимое во временные файлы. Эти файлы можно использовать при повторном просмотре Web-страниц, что значительно ускоряет их загрузку. Настройка временных файлов осуществляется в области Временные файлы Интернета. Нажатие кнопки Удалить файлы этой области приводит к удалению временных файлов с диска. Используйте данную кнопку в том случае, если у вас на диске недостаточно места, и вы уверены, что не будете повторно открывать уже просмотренные Web-страницы. Для настройки параметров управления временными файлами воспользуйтесь кнопкой Настройка и открываемым ею одноименным диалоговым окном.

Область Журнал вкладки Общие позволяет указать число дней, в течение которых Internet Explorer будет сохранять ссылки на просмотренные страницы в папке журнала. Нажатие кнопки Очистить приводит к удалению информации из папки.

В нижней части вкладки Общие расположены кнопки, позволяющие задать используемое цветовое оформление Интернета, шрифты, предпочтительный язык для отображения информации, располагаемой на Web-странице, и другие параметры оформления.

Используемые цвета

При нажатии кнопки Цвета вкладки Общие открывается диалоговое окно Цвета, показанное на рис. 2. Оно разделено на две области.

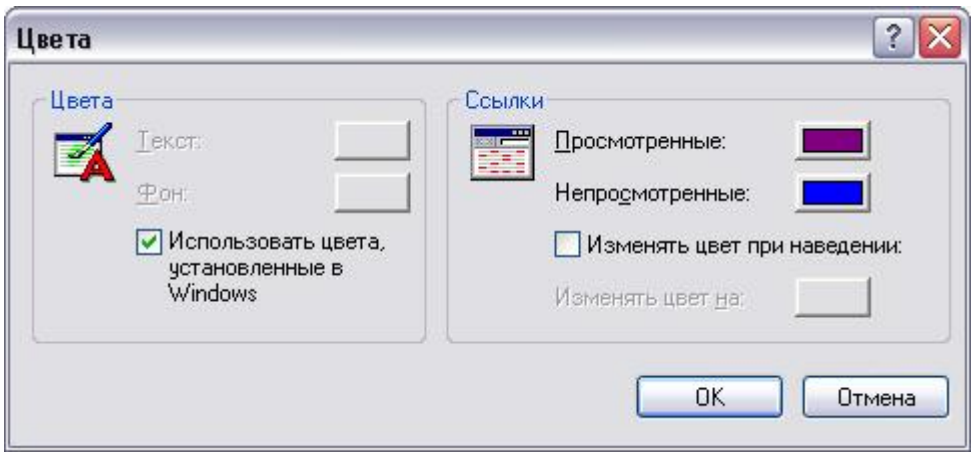


Рис. 2. Диалоговое окно, предназначенное для настройки цветов

Область Цвета позволяет задать цвет текста и фона Web-страниц. Для изменения заданного цвета текста или фона нажмите кнопку, расположенную справа от соответствующей надписи. Откроется диалоговое окно Цвет, содержащее базовую цветовую палитру. Выберите с помощью курсора устраивающий вас цвет и нажмите кнопку ОК.

При установке флажка Использовать цвета, установленные в Windows кнопки, расположенные в области Цвета, не доступны. В этом случае для отображения цвета текста и фона Web-страниц используются стандартные установки Windows.

С помощью кнопок, расположенных в области Ссылки, меняется цвет просмотренных ссылок и ссылок, по которым еще не осуществлялся переход. При установке флажка Изменять цвет при наведении можно задать цвет ссылок при наведении на них указателя мыши.

Настройка шрифтов

Кнопка Шрифты, находящаяся на вкладке Общие, открывает одноименное диалоговое окно, показанное на рис. 7.3.

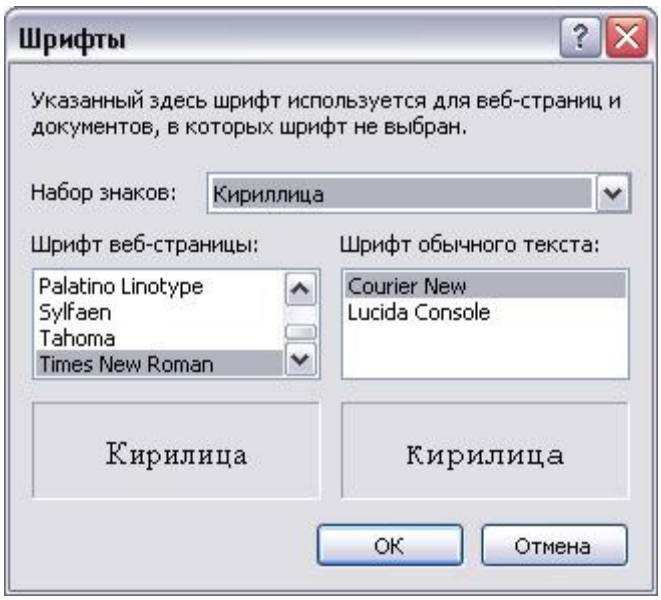


Рис.3. Диалоговое окно, используемое для настройки шрифтов

В его верхней части расположен раскрывающийся список, содержащий наборы символов, установленных на компьютере. Ниже него расположены списки, позволяющие установить шрифт следующей информации, содержащейся на Web-странице:

- Шрифт веб-страницы — используется для вывода текста, оформленного с применением форматирования
- Шрифт обычного текста — используется для вывода текста Web-страницы, оформленного без применения форматирования

Выбор языка

Кнопка Языки, расположенная на вкладке Общие, открывает диалоговое окно Выбор языка (рис. 4), позволяющее задать список языков, используемых Internet Explorer для отображения содержимого Web-страниц. Для добавления в список языка необходимо нажать кнопку Добавить и в открывшемся диалоговом окне Добавление языка выбрать используемый язык.

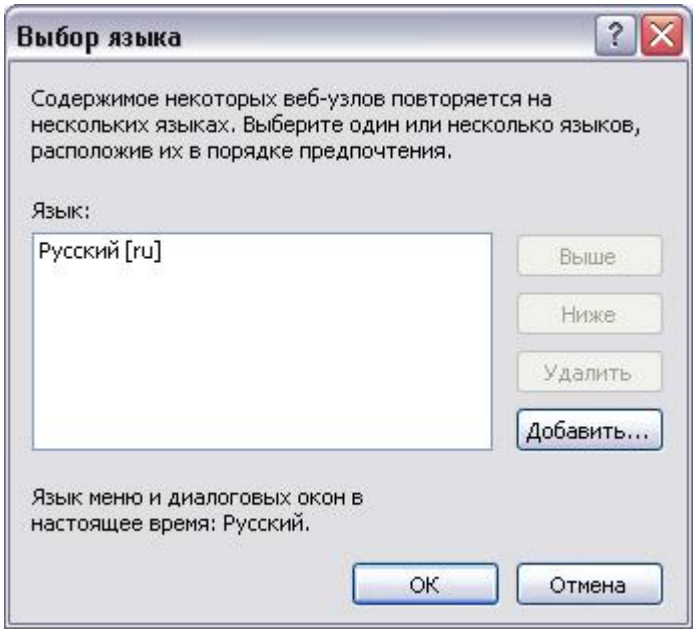


Рис.4. Диалоговое окно Выбор языка

Оформление Web-страниц

Кнопка Оформление, размещенная на вкладке Общие, открывает диалоговое кно Оформление (рис.5), содержащее флажки, перечисленные в табл. 1.

Таблица 1. Флажки оформления Web-страницы

Флажок	Назначение
Не учитывать цвета, указанные на веб-страницах	Флажок устанавливается в случае, если для задания цветовых настроек текста, фона и ссылок используется диалоговое окно Цвета (см. рис.2)
Не учитывать шрифты, указанные на веб-страницах	Установка флажка используется в случае задания настроек шрифтов текста в диалоговом окне Шрифты (см. рис.3)
Не учитывать размеры шрифтов, указанные на веб-страницах	Установка флажка используется в случае задания настроек размеров шрифтов текста в диалоговом окне Шрифты (см. рис. 3)
Оформлять, используя стиль пользователя	Флажок устанавливается в случае, если для оформления всех выводимых страниц используется пользовательская библиотека стилей. Для указания местонахождения библиотеки предназначены расположенное под флажком поле и кнопка Обзор

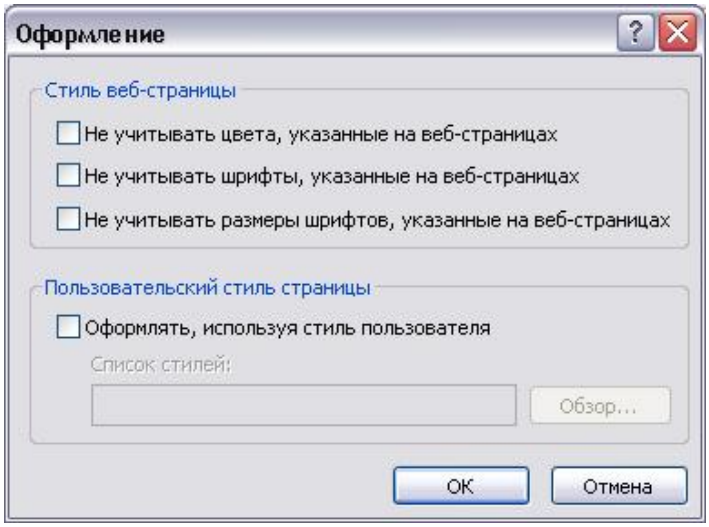


Рис. 5. Диалоговое окно Оформление

Защита информации

При работе в сети Интернет пользователю необходимо заботиться о том, чтобы пересылаемые им данные, особенно информация конфиденциального характера, не была доступна посторонним пользователям. С другой стороны, проблема безопасности данных встает при пересылке файлов и программ между Web-узлами и вашим компьютером. Без применения системы зашиты вы можете получить программу, которая при запуске повредит хранящиеся в вашем компьютере данные.

Степень надежности Web-узлов в Интернете различна. Программа Internet Explorer позволяет распределять получаемые вами по сети данные по зонам безопасности и устанавливать разные уровни защиты в зависимости от того, кто является их отправителем. Перед загрузкой Web-страницы Internet Explorer проверяет соответствие узла заданной зоне безопасности. Для того чтобы узнать, к какой зоне безопасности относится загруженная страница, посмотрите на строку состояния. В ее правой части размещается название зоны.

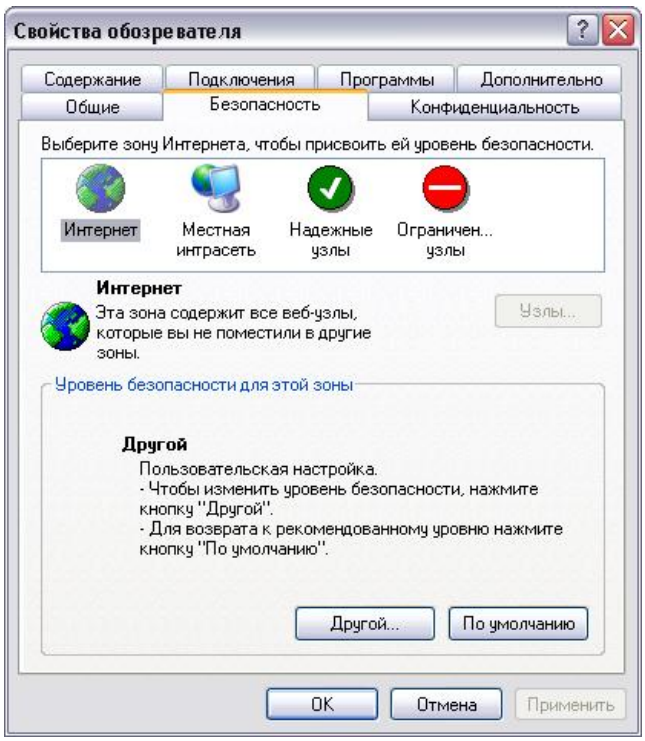


Рис. 6. Вкладка, позволяющая настроить параметры безопасности

Используя вкладку Безопасность (рис. 6) диалогового окна Свойства обозревателя, можно установить для зон Интернета разные параметры безопасности. В верхней части вкладки расположен представленный в виде значков список основных категорий зон, на которые имеется доступ с компьютера пользователя (табл. 2).

Таблица 2. Основные категории зон безопасности

Зона	Назначение
Интернет	В эту зону входит все то, что не имеет отношения к вашему компьютеру, внутренней сети или иной зоне. По умолчанию зона обладает средним уровнем защиты
Местная интрасеть	Данная зона содержит адреса, для которых использование прокси-сервера не обязательно. Эти адреса назначаются системным администратором с помощью административного комплекта Internet Explorer (IEAK). По умолчанию зона имеет уровень защиты ниже среднего
Надежные узлы	Зона содержит узлы, которым вы доверяете и с которых можно загружать информацию и программы, не беспокоясь о возможном повреждении ваших собственных данных или компьютера. По умолчанию эта зона имеет низкий уровень защиты
Ограниченные узлы	Данная зона содержит узлы, которым вы не доверяете. По умолчанию эта зона имеет высокий уровень защиты

На вкладке содержится ползунок, используемый для задания уровня безопасности зоны, выбранной из верхнего списка (табл.3).

Таблица. 3. Уровни безопасности

Уровень безопасности	Выполняемое программой действие
Высокий	При угрозе безопасности с Web-узла выдается уведомление. Информация, которая может нести угрозу безопасности, не загружается. Небезопасные функции отключаются
Средний	Перед загрузкой небезопасного содержимого с Web-узла выдается уведомление. После предупреждения появляется запрос на подтверждение или отмену загрузки активного содержимого
Ниже среднего	Большая часть содержимого запускается без предупреждения. При угрозе безопасности с Web-узла выдается уведомление

Низкий	Обеспечивает минимальный уровень безопасности. При потенциальной угрозе безопасности с Web-узла выдается уведомление, после чего активное содержимое загружается на компьютер

Вкладка Безопасность диалогового окна Свойства обозревателя содержит кнопки, перечисленные в табл. 4.

Таблица 4. Кнопки вкладки Безопасность

Кнопка	Назначение
Узлы	Позволяет добавить или удалить узел из заданной зоны
По умолчанию	Позволяет для выбранной зоны установить уровень защиты, принятый по умолчанию
Другой	Открывает диалоговое окно Правила безопасности для определения дополнительных настроек защиты

Параметры вкладки Содержание

Вкладка Содержание (рис.7) диалогового окна Свойства обозревателя содержит три области, имеющие следующее назначение:

- Ограничение доступа — позволяет ввести ограничения на просмотр информации в Интернете
- Сертификаты — предназначена для просмотра личных сертификатов безопасности, установленных на данном компьютере, сертификатов узлов и издателей
- Личные данные — хранит персональные данные, предоставляемые узлам при запросах

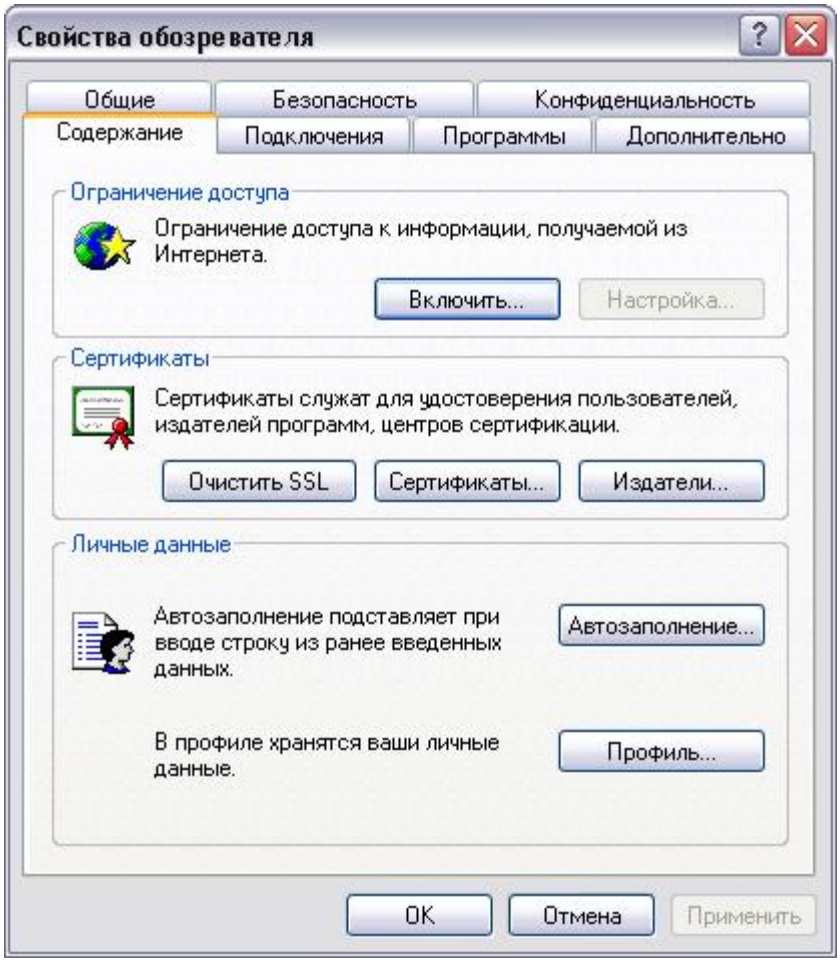


Рис. 7. Вкладка Содержание

Персональные компьютеры появились во многих семьях. При этом постоянно растет число домашних компьютеров, подключенных к Интернету. Используя область Ограничение доступа вкладки Содержание, вы сможете ввести ограничения на просмотр детьми в Интернете информации, использующей ненормативную лексику, текст и рисунки о насилии и сексе.

Область содержит кнопку Включить, при нажатии на которую открывается диалоговое окно Ограничение доступа (рис. 8), содержащее четыре вкладки: Оценки, Разрешенные узлы, Общие и Дополнительно.

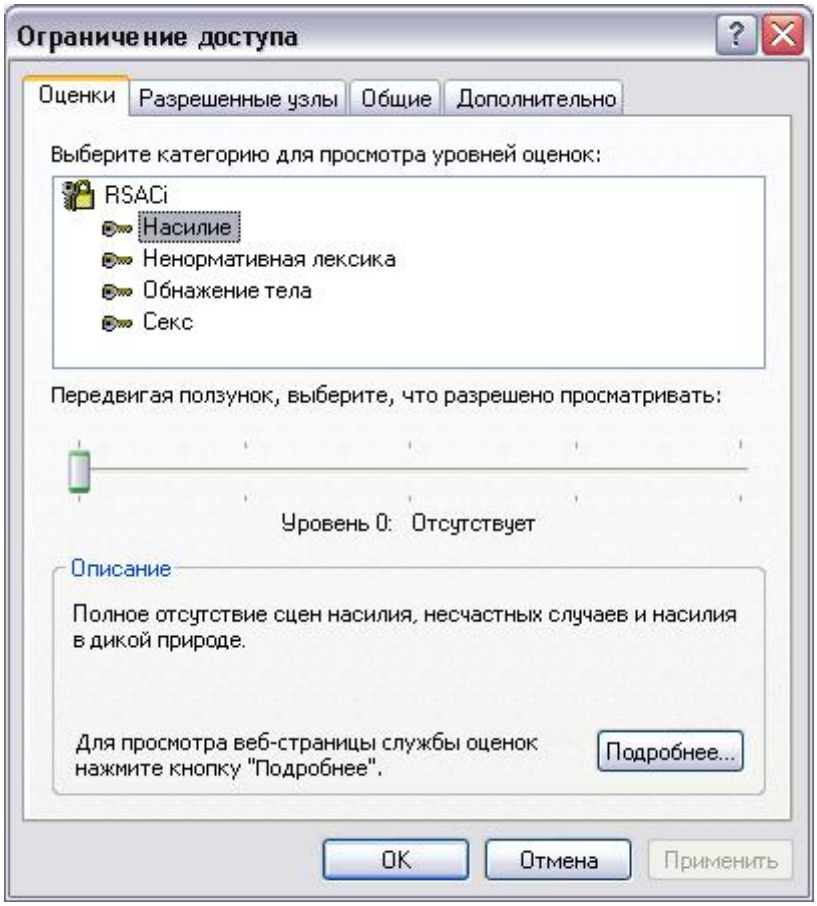


Рис. 8. Диалоговое окно, используемое для ограничения доступа к информации

В верхней части вкладки Оценки расположен список разделов, на которые можно задать ограничения, а ниже него — ползунок, указывающий уровень ограничения. Для изменения уровня запрета на просмотр информации выберите из списка настраиваемую категорию. При этом в области Описание вкладки отображается информация об установленном уровне запрета для данного раздела. Перемещая движок, измените установленный уровень доступности материал данной категории.

Вкладка Разрешенные узлы позволяет сформировать список узлов, которые можно просматривать или, наоборот, не просматривать, несмотря на параметры, установленные на вкладке Оценки.

Флажок Пользователи могут просматривать узлы, не имеющие оценок вкладки Общие определяет разрешение на просмотр не имеющих оценки узлов для пользователей данного компьютера. При установке этого флажка пользователь получает доступ к нежелательному материалу, если рейтинг Web-страницы не определен. Если этот флажок не установлен, пользователь не будет иметь доступа к Web-страницам, не имеющим оценки, даже если они не содержат нежелательного материала.

Установленный флажок Разрешить ввод пароля для просмотра запрещенных узлов вкладки Общие позволяет просматривать запрещенную для просмотра информацию Web-страниц после ввода пароля.

Настройка подключения к Интернету

Вкладка Подключение (рис.9) диалогового окна Свойства обозревателя позволяет настроить параметры удаленного доступа.

В верхней части вкладки находится кнопка Установить, при нажатии на нее запускается мастер подключения к Интернету, который поможет установить соединение. Расположенные ниже переключатель и кнопка Настройка позволяют осуществить самостоятельную настройку параметров соединения.

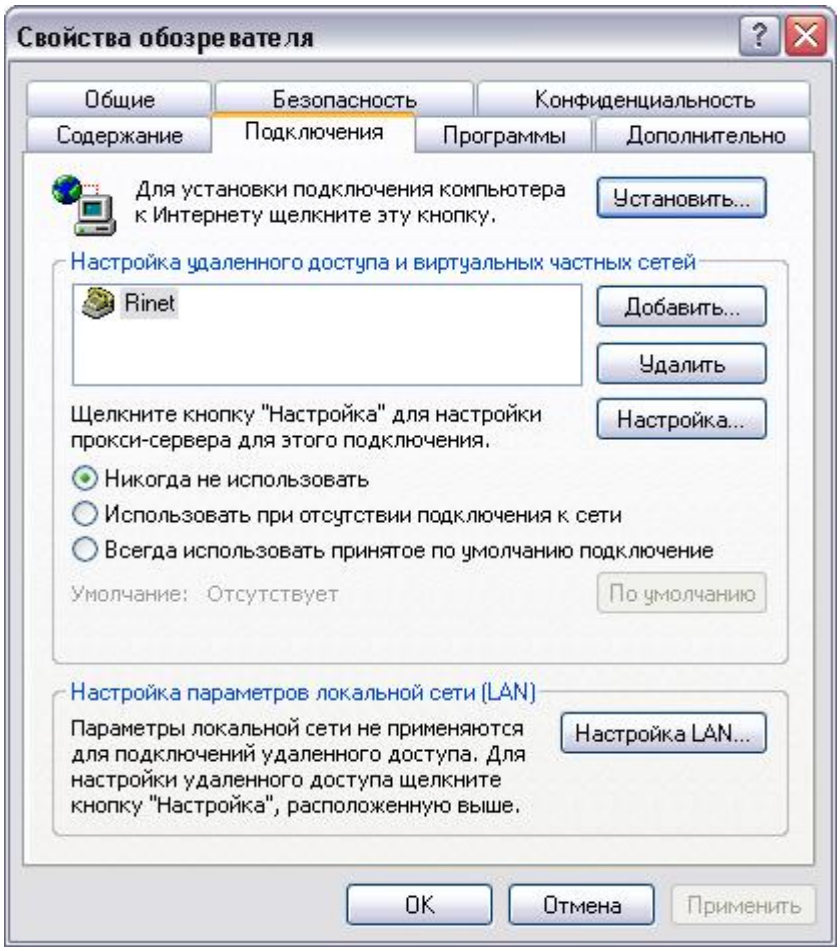


Рис.9. Вкладка, предназначенная для настройки подключения к Интернету

В области Настройка удаленного доступа находится список соединений для удаленного доступа к сети, установленных на компьютере, и три кнопки:

- Добавить — добавляет в список с помощью мастера новое соединение для удаленного доступа к сети
- Удалить — удаляет из списка выделенное соединение с Интернетом
- Настройка — открывает диалоговое окно Настройка, позволяющее просмотреть и изменить настройки подключения выбранного соединения

Установленная под списком опция Не использовать указывает на необходимость при подключении к Интернету выбирать используемое соединение вручную.

Опция Использовать при отсутствии подключения к сети указывает, что для выхода в Интернет при отсутствии подключения программа Internet Explorer будет использовать соединение для удаленного доступа к сети, принятое по умолчанию.

Установив расположенную под списком опцию Всегда использовать принятые по умолчанию, с помощью кнопки По умолчанию можно указать, какое соединение использовать по умолчанию при подключении к Интернету.

Область Настройка локальной сети позволяет осуществить подключение к Интернету через прокси-сервер локальной сети, который служит защитным барьером между внутренней сетью и Интернетом, не позволяя другим пользователям Интернета получить доступ к конфиденциальной информации внутренней сети.

Настройка соединения

Чтобы настроить соединение для удаленного доступа к сети Интернет, выберите его в списке соединений на вкладке Подключение и нажмите кнопку Настройка. Откроется одноименное диалоговое окно (рис. 7.10), предназначенное для просмотра и изменения параметров. В его верхней части расположены два флажка:

- Автоматическое определение настроек — при установке флажка осуществляется автоматическое определение настроек прокси-сервера или параметров автоматической настройки, используемых для подключения к Интернету и настройки обозревателя Internet Explorer.
- Использовать сценарий автоматической настройки — при установке флажка для автоматической настройки используется файл, содержащий параметры настройки, предоставленные системным администратором.

При установке флажка Использовать сценарий автоматической настройки становится доступным для ввода информации поле Адрес, предназначенное для задания адреса URL или имени файла, используемого для настройки Internet Explorer.

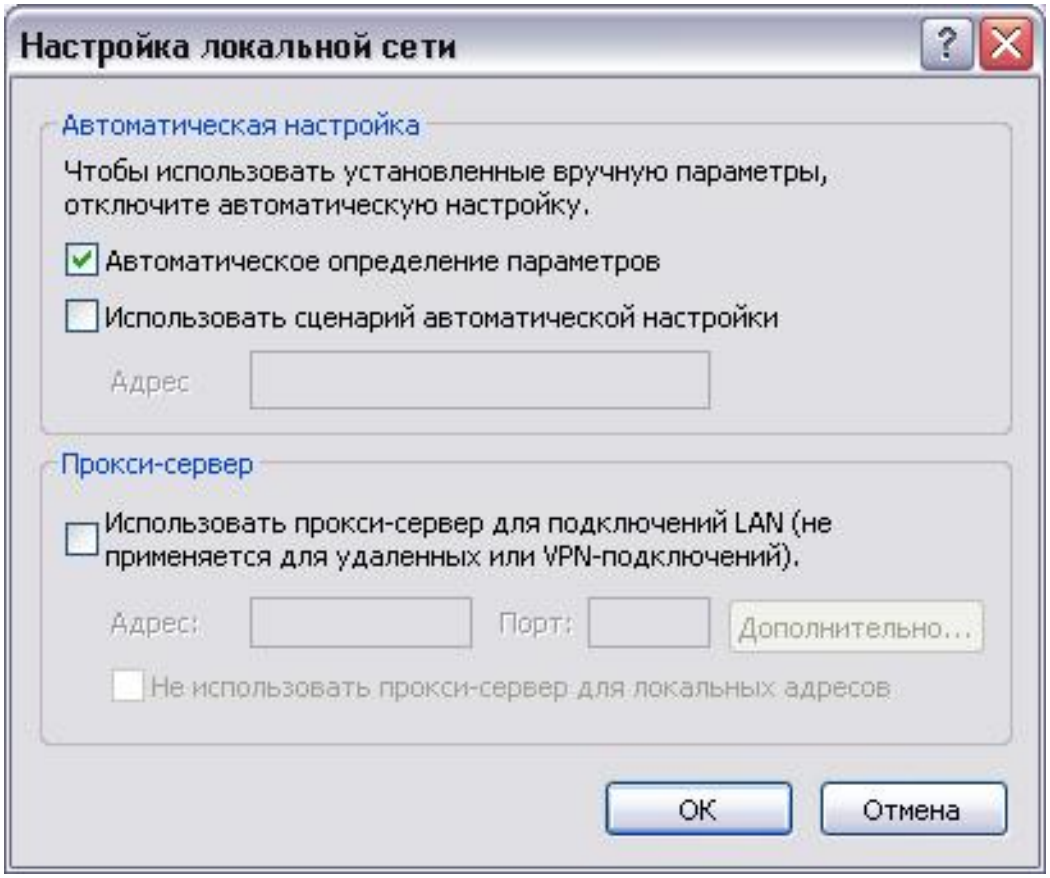


Рис. 10. Диалоговое окно, предназначенное для настройки соединения

Область Прокси-сервер позволяет осуществить подключение к Интернету через прокси-сервер локальной сети. При установке флажка Использовать прокси-сервер становятся доступными для ввода следующие поля:

- Адрес — адрес прокси-сервера, предоставляемый системным администратором сети
- Порт — порт прокси-сервера, используемый для доступа к Интернету

При подключении к Интернету через прокси-сервер локальной сети необходимо осуществить дополнительные настройки прокси-сервера. Для этого нажмите кнопку Дополнительно. Откроется диалоговое окно Параметры прокси-сервера, в котором необходимо ввести адрес и порт прокси-сервера, используемого для доступа к Интернету по протоколам HTTP, Secure, FTP, Gopher и Socks.

Для настройки удаленного доступа предназначена область Настройка удаленного доступа диалогового окна Настройка. Она содержит поля, в которые нужно ввести данные, предоставленные провайдером:

- Имя пользователя — имя пользователя;
- Пароль — пароль;
- Домен — имя домена.

Нажатие кнопки Свойства этой области открывает окно, предназначенное для изменения номера телефона, модема и других дополнительных параметров текущего соединения удаленного доступа к сети.

Формирование списка используемых программ

Используя вкладку Программы (рис.11) диалогового окна Свойства обозревателя, можно задать применяемые вместе с Internet Explorer программы:

- редактора HTML — для редактирования HTML-файлов;
- электронной почты — для работы с электронной почтой;
- групп новостей — для чтения групп новостей Интернета;
- вызовов по Интернету — для набора номера;
- календаря — для просмотра календаря;
- адресной книги — для работы с адресной книгой.

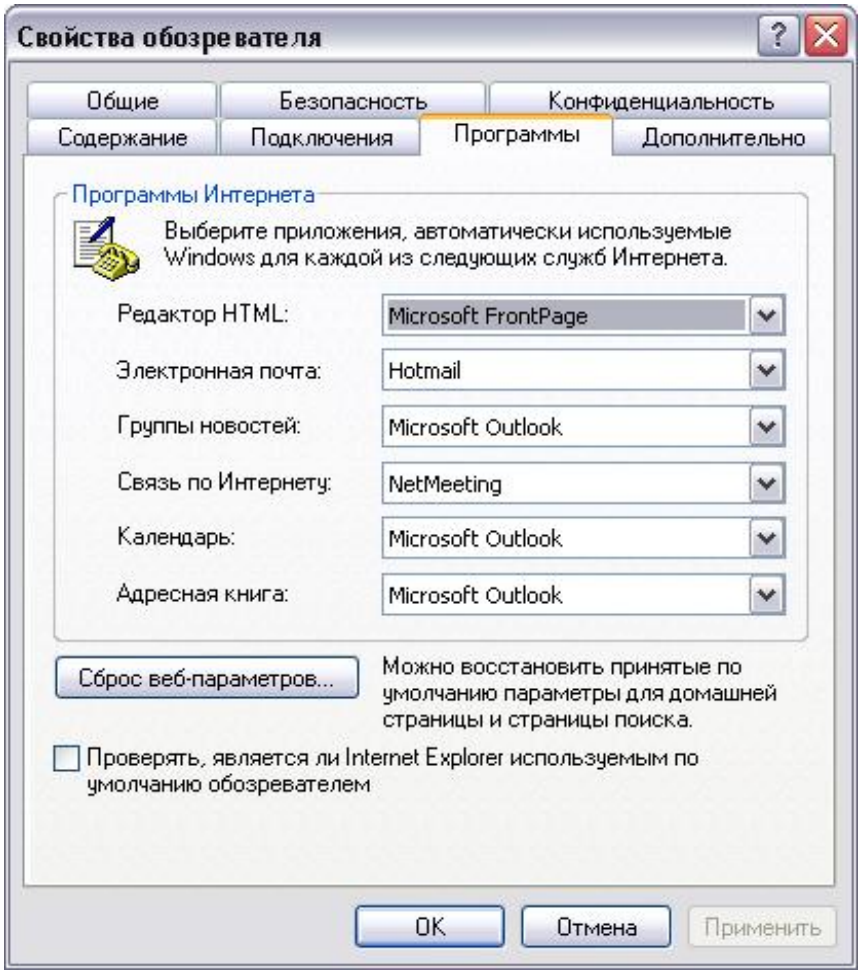


Рис. 11. Вкладка, позволяющая задать список используемых программ

При установке флажка Проверять, является ли Internet Explorer обозревателем, используемым по умолчанию при каждом запуске Internet Explorer выполняет проверку, зарегистрирован ли Internet Explorer в качестве средства просмотра Интернета, используемого по умолчанию. Если зарегистрирована другая программа, будет предложено восстановить применение Internet Explorer в качестве стандартного средства просмотра информации в Интернете.

Дополнительные настройки обозревателя

Для дополнительных настроек обозревателя используется вкладка Дополнительно (рис.12) диалогового окна Свойства обозревателя, содержащая большой список параметров, сгруппированных по разделам. Для их установки достаточно установить флажок или одну из предлагаемых опций.

Чтобы восстановить значения, установленные в системе по умолчанию, нажмите кнопку Восстановить значения по умолчанию.

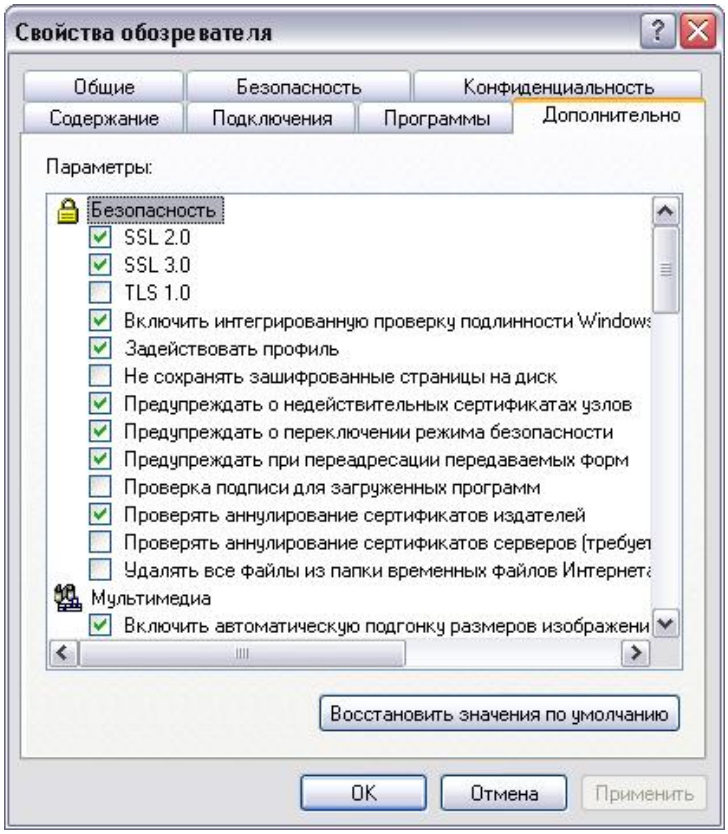


Рис. 12. Настройка дополнительных параметров обозревателя

Содержание отчета

Отчет должен содержать:

- Название работы
- Цель работы
- Презентацию с выполненным заданием

Контрольные вопросы

1. Что такое Веб-браузер?
2. Каковы достоинства применения этой технологии?
3. Каковы ограничения применения этой технологии?

Рекомендуемая литература

Основная

1. Костров Б.В. Сети и системы передачи информации: учебник для студентов учреждений среднего профессионального образования / Б.В. Костров, В.Н. Ручкин. –М.: Издательский центр «Академия», 2017г.

Дополнительная

11. Литвинская О.С. Основы теории передачи информации: учебное пособие / Литвинская О.С., Чернышев Н.И. — Москва: КноРус, 2021 — 168 с. — ISBN 978-5-406-08653-7. — URL: https://book.ru/book/940469 (дата обращения: 23.04.2021). —Текст: электронный.

ПРАКТИЧЕСКАЯ РАБОТА №12
Защита информации в Интернет

Цель работы

Приобрести навыки по установке сетевого адаптера в персональный компьютер и настройки его драйвера в операционных системах Windows XP и Linux.

Оборудование: компьютерный класс, сетевые адаптеры.

Задание

Вредоносная программа — компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе, либо для скрытого нецелевого использования ресурсов системы, либо иного воздействия, препятствующего нормальному функционированию компьютерной системы. К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

Независимо от типа, вредоносные программы способны наносить значительный ущерб, реализуя любые угрозы информации — угрозы нарушения целостности, конфиденциальности, доступности.

1. Сетевые черви. К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

- ✓ проникновения на удаленные компьютеры;
- ✓ запуска своей копии на удаленном компьютере;
- ✓ дальнейшего распространения на другие компьютеры в сети.

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т. д.

Некоторые черви обладают свойствами других разновидностей вредоносного программного обеспечения. Например, некоторые черви содержат троянские функции или способны заражать выполняемые файлы на локальном диске, т. е. имеют свойство троянской программы и/или компьютерного вируса.

2. Классические компьютерные вирусы. К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью:

- ✓ последующего запуска своего кода при каких-либо действиях пользователя;
- ✓ дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей, вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

- ✓ при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
- ✓ вирус скопировал себя на съёмный носитель или заразил файлы на нем;
- ✓ пользователь отослал электронное письмо с зараженным вложением.

3. Троянские программы. В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для массированных DoS-атак на удалённые ресурсы сети).

4. Хакерские утилиты и прочие вредоносные программы. К данной категории относятся:

- ✓ утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);

- ✓ программные библиотеки, разработанные для создания вредоносного ПО;
- ✓ хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- ✓ «злые шутки», затрудняющие работу с компьютером;
- ✓ программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- ✓ прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.

Руткит (Rootkit) - программа или набор программ, использующих технологии сокрытия системных объектов (файлов, процессов, драйверов, сервисов, ключей реестра, открытых портов, соединений и пр.) посредством обхода механизмов системы.

В системе Windows под термином руткит принято считать программу, которая внедряется в систему и перехватывает системные функции, или производит замену системных библиотек. Перехват и модификация низкоуровневых API функций в первую очередь позволяет такой программе достаточно качественно маскировать свое присутствие в системе, защищая ее от обнаружения пользователем и антивирусным ПО. Кроме того, многие руткиты могут маскировать присутствие в системе любых описанных в его конфигурации процессов, папок и файлов на диске, ключей в реестре. Многие руткиты устанавливают в систему свои драйверы и сервисы (они естественно также являются «невидимыми»).

В последнее время угроза руткитов становится все более актуальной, т.к. разработчики вирусов, троянских программ и шпионского программного обеспечения начинают встраивать руткит-технологии в свои вредоносные программы. Одним из классических примеров может служить троянская программа Trojan-Spy.Win32.Qukart, которая маскирует свое присутствие в системе при помощи руткит-технологии. Ее RootKit-механизм прекрасно работает в Windows 95, 98, ME, 2000 и XP.

Современные антивирусные программы обеспечивают комплексную защиту программ и данных на компьютере от всех типов вредоносных программ и методов их проникновения на компьютер (Интернет, локальная сеть, электронная почта, съемные носители информации). Большинство антивирусных программ сочетает в себе функции постоянной защиты (антивирусный монитор) и функции защиты по требованию пользователя (антивирусный сканер).

Межсетевой экран — это программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа к компьютеру. Другое распространенное название сетевого экрана — файервол от английского термина firewall. Иногда сетевой экран называют еще брандмауэром (нем. brandmauer) — это немецкий эквивалент слова firewall. Основная задача сетевого экрана — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации сетевого экрана. Межсетевой экран позволяет:

- ✓ Блокировать хакерские атаки;
- ✓ Не допускать проникновение сетевых червей;
- ✓ Препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.

*Задание***.** В операционной системе Windows проверить выбранные объекты на наличие вредоносных объектов, выполнить лечение или удаление зараженных объектов

Порядок выполнения

1) Запустить на выполнение антивирусную программу.
2) Запустить обновление из контекстного меню.
3) Выполнить проверку съемного носителя.
4) Выполнить проверку локального диска.
5) Отчет о работе антивирусной содержит информацию о результатах проверки.

Содержание отчета

Отчет должен содержать:

- Название работы
- Цель работы
- Презентация с информацией о результатах проверки.

Контрольные вопросы

1. Приведите классификацию вредоносных программ?
2. Какие вредоносные программы наиболее распространены в Интернет?
3. Какие меры безопасности необходимы при работе в Интренерт?

Рекомендуемая литература

Основная

1. Костров Б.В. Сети и системы передачи информации: учебник для студентов учреждений среднего профессионального образования / Б.В. Костров, В.Н. Ручкин. –М.: Издательский центр «Академия», 2017г.

Дополнительная

12. Литвинская О.С. Основы теории передачи информации: учебное пособие / Литвинская О.С., Чернышев Н.И. — Москва: КноРус, 2021 — 168 с. — ISBN 978-5-406-08653-7. — URL: https://book.ru/book/940469 (дата обращения: 23.04.2021). —Текст: электронный.

ПРАКТИЧЕСКАЯ РАБОТА №13
Настройка брандмауэра

Цель работы
Приобрести навыки по настройке брандмауэра Windows.

Оборудование: компьютерный класс.

Задание

Сетевая защита и брандмауэр

Как бы ни была безопасна система, всегда есть риск, что кто-то извне по компьютерной сети будет пытаться ее взломать. Единственным решением, которое позволяет в большинстве случаев решить эту проблему является своевременное обновление версий программного обеспечения. Но и в этом случае можно найти какую-то особенность в функционировании программного обеспечения и использовать ее для взлома системы. Например: использование пользователем демонстрационной версии программного продукта или используемая версия программного обеспечения больше не поддерживается разработчиком. В этих ситуациях, если не использовать каких-либо дополнительных мер, пользователь может оказаться беззащитным от атак извне.

Понимая опасность таких ситуаций, многие исследовательские центры и частные компании занимались решением этой проблемы. Разработчики рассудили: раз сетевой взломщик не должен взломать компьютер пользователя, то он просто не должен получить к нему доступ, т.е. необходимо гарантированно закрыть доступ к компьютеру несанкционированным пользователям. Разработанный метод защиты похож на стену, окружающую со всех сторон компьютер, поэтому он и получил название *Firewall* (пожарная стена), иначе сетевой экран или фильтр, который отфильтровывает запросы сетевых пользователей к системе. В официальной русской версии *Windows XP* он переведен как *брандмауэр*.

Брандмауэр – это специальное программное обеспечение, поставляемое вместе с операционной системой или устанавливаемое пользователем, которое позволяет запретить любой доступ нежелательных пользователей из сети к системе. *Брандмауэр* помогает повысить безопасность компьютера. Он ограничивает информацию, поступающую на компьютер с других компьютеров, позволяя лучше контролировать данные на компьютере и обеспечивая линию обороны компьютера от людей или программ (включая вирусы и «черви»), которые несанкционированно пытаются подключиться к компьютеру. *Брандмауэр* – это пограничный пост, на котором проверяется информация (трафик), приходящая из Интернета или по локальной сети. В ходе проверки *брандмауэр* отклоняет или пропускает информацию на компьютер в соответствии с установленными параметрами.

В состав *Windows XP* входит встроенная версия *брандмауэра* (в пакет обновления *SP2* для *Microsoft Windows XP брандмауэр* включен по умолчанию), основной алгоритм работы которого обеспечивает защиту от несанкционированных пользователей. Практически невозможно найти уязвимость, которая бы обеспечивала проникновение взломщика на защищенную сетевым экраном систему. Функции, выполняемые *брандмауэром*:

- блокировка доступа на компьютер вирусам и «червям»;
- запрос пользователя о выборе блокировки или разрешения для определенных запросов на подключение;
- ведение журнала безопасности и по желанию пользователя запись разрешенных и заблокированных попыток подключения к компьютеру, журнал может оказаться полезным для диагностики неполадок.

Идея атак взломщиков основывается на работе низкоуровневых алгоритмов обработки сетевых запросов, в некоторых старых версиях программного обеспечения их можно было пытаться использовать для возможного проникновения через сетевой экран. В современных версиях *брандмауэра*, если грамотно его настроить, можно избежать любых атак взломщиков.

Когда на компьютер поступает непредусмотренный запрос (кто-то пытается подключиться из Интернета или по локальной сети), *брандмауэр* блокирует подключение. Если на компьютере ис-

пользуются программы передачи мгновенных сообщений или сетевые игры, которым требуется принимать информацию из Интернета или локальной сети, *брандмауэр* запрашивает пользователя о блокировании или разрешении подключения. Если пользователь разрешает подключение, *брандмауэр* создает исключение, чтобы в будущем не тревожить пользователя запросами по поводу поступления информации для этой программы. Предусмотрена так же возможность отключения *брандмауэра* для отдельных подключений к Интернету или локальной сети, но это повышает вероятность нарушения безопасности компьютера.

Настройка брандмауэра

Если *брандмауэр* подключен, то для его настройки следует:
- войти в систему под учетной записью системного администратора;
- открыть папку, в которой находятся сетевые подключения:

Пуск\Настройка\Панель управления\Сетевые подключения (рис.1.1.);

- выбрать строку, например, *Подключение по локальной сети* (рис.1.2.);
- во вкладке *Общие* сделать щелчок по кнопке *Свойства* (рис.1.2.);
- появится дополнительное окно *Свойства*, в котором выбрать вкладку *Дополнительно* (рис.1.2.);
- во вкладке *Дополнительно* нажать кнопку *Параметры* (рис.1.3.);
- появится окно программы *Брандмауэр Windows* (рис.1.3.).

Аналогичное окно появится при выборе программы *Брандмауэр Windows* из списка программ в *Панели управления*:

Пуск – Настройки – Панель управления – Брандмауэр Windows (рис.1.4.)

Для получения подробной информации в окне программы *Брандмауэр Windows* следует сделать щелчок по ссылке *Подробнее о Брандмауэре Windows*. Появится окно *Центр справки и поддержки,* в котором будет приведена вся информация о назначении и использовании *брандмауэра*.

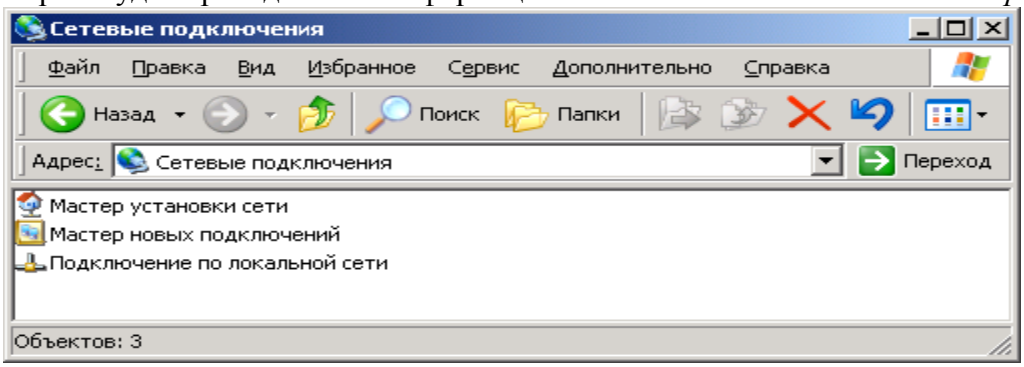


Рисунок 1.1. Окно программы *Сетевые подключения*

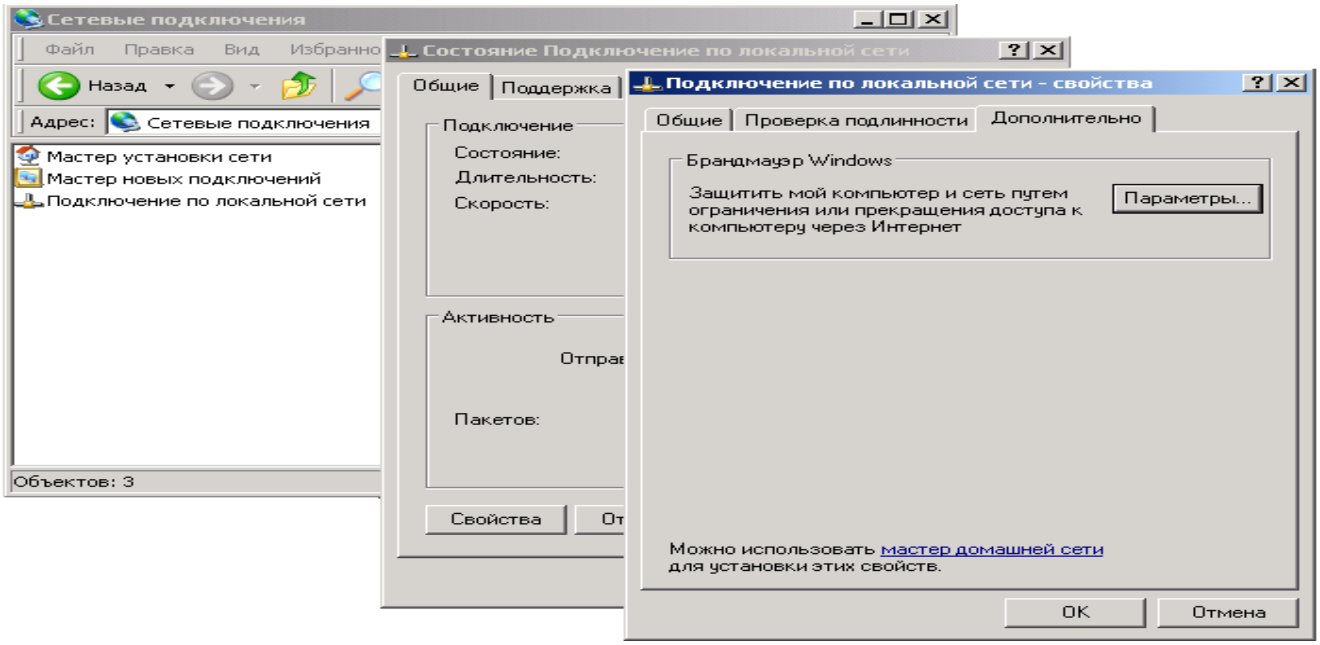


Рисунок 1.2. Окна программы *Подключение по локальной сети*

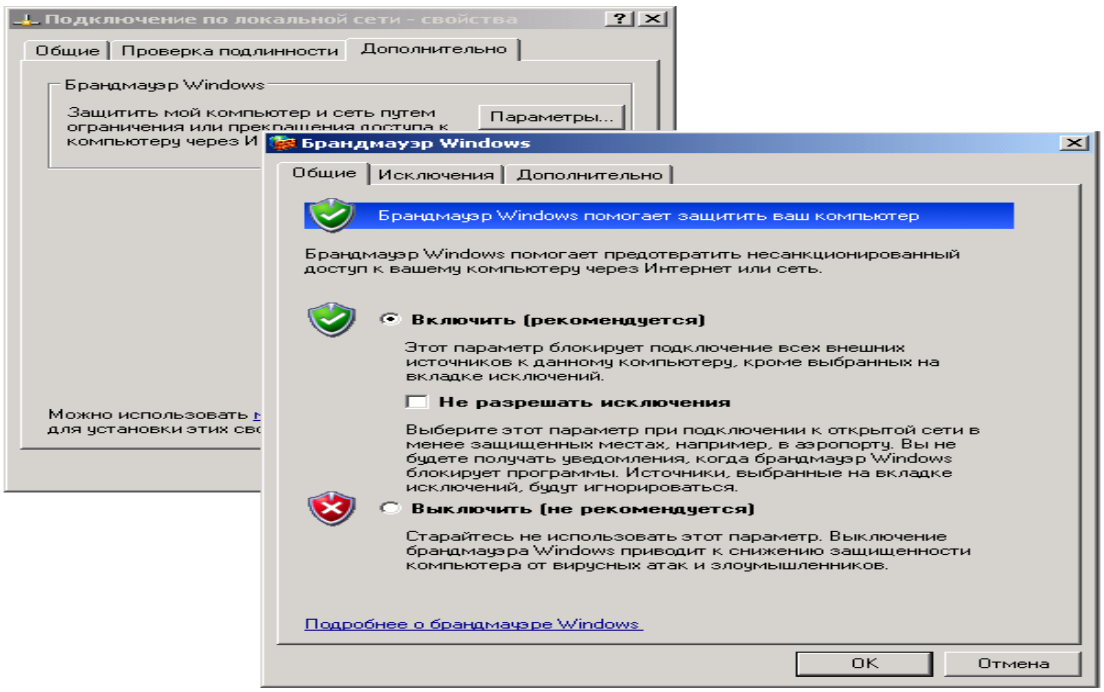


Рисунок 1.3. Окно вкладки *Дополнительно* и окно программы *Брандмауэр*

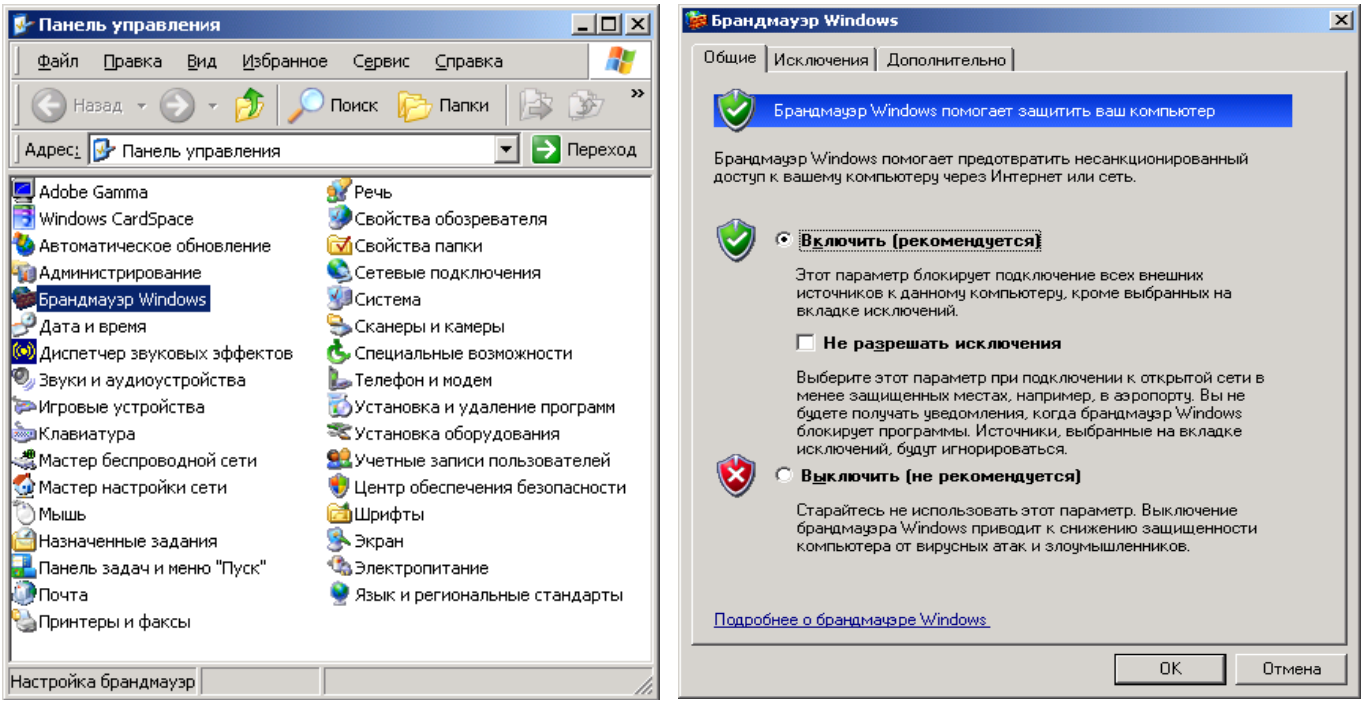


Рисунок 1.4. Окно *Панель управления*
и окно программы *Брандмауэр Windows*

Закладка *Общие* окна настроек *брандмауэра* является главной, по умолчанию *брандмауэр* включен (рис.1.4.). Закладка содержит ряд опций.

Опция *Включить (рекомендуется)* включает *брандмауэр*. Опция *Не разрешать исключения* может использоваться только вместе с опцией *Включить (рекомендуется)*. Она позволяет повысить уровень безопасности системы в случае ее использования в публичных местах, таких как аэропорты, кафе, кинотеатры и пр., оборудованные доступом в Интернет. Уровень безопасности будет увеличен за счет запрета работы программ, к которым разрешается получать доступ из сети, прегражденной сетевым фильтром. Сообщения об отказе доступа пользователям к таким приложениям система генерировать не будет.

Опция *Выключить (не рекомендуется)* полностью выключает *брандмауэр*. В этом случае система оказывается совершенно незащищенной от атак извне. Единственный случай, когда это может быть оправдано, это когда нужно кратковременно протестировать работу какого-либо приложения, которое не хочет работать с активным сетевым экраном.

Брандмауэр Windows блокирует входящие сетевые подключения, исключая программы и службы, выбранные пользователем. Добавление исключений улучшает работу некоторых программ, но повышает риск безопасности. Закладка *Исключения* позволяет указать программы и сервисы, к которым могут быть осуществлены соединения пользователей со стороны Интернета (рис.1.5.). Фактически, для этих программных продуктов сетевой фильтр работать не будет, пропуская все запросы к ним через себя.

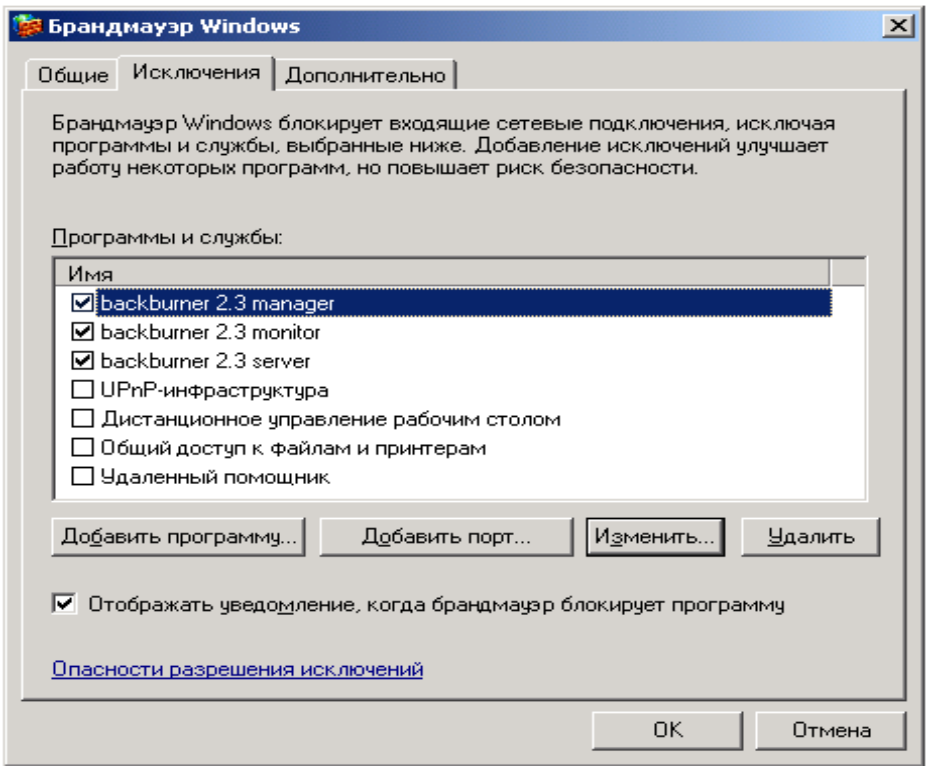


Рисунок 1.5. Закладка *Исключения*

Закладка *Исключения* представляет собой список программ и сервисов, к которым можно разрешить доступ со стороны Интернета, посредством установки рядом с ними флажка. Опция *Отображать уведомление, когда брандмауэр блокирует программу*, в случае ее активизации, заставляет *Windows* выдавать сообщение о попытке доступа из сети. По умолчанию опция включена, т.к. она помогает лучше понять процессы, происходящие внутри системы. Если на закладке *Общие* установлена опция *Не разрешать исключения* сообщение выдаваться не будет.

Для удаления программы или сервиса из списка разрешенных объектов к обращению из сети Интернет следует выделить объект из списка окна и нажать кнопку *Удалить*. Данную операцию стоит проводить с программами или сервисами, которые больше не должны быть доступны для пользователей из Интернета.

Для редактирования определенного объекта из списка программ и сервисов, разрешенных к обращению из Интернета следует выделить редактируемый объект и нажать кнопку *Изменить*, появится окно *Изменение программы* (рис.1.6). Диалоговое окно содержит имя редактируемой программы и путь к ее исполняемому файлу. Кнопка *Изменить область* позволяет указать, каким именно сетевым компьютерам будет доступна выбранная программа или сервис. В данном окне можно указать три режима, в соответствии с которыми будет осуществляться доступ из сети к программе или сервису, расположенному в системе.

Режим *Любой компьютер (включая из Интернета)* указывает, что доступ к данной программе будет возможен со всех сетевых компьютеров, включая расположенные в Интернете. Не рекомендуется выбирать режим без особой необходимости, т.к. будет предоставлена возможность любому пользователю извне пробовать подключаться к определенному программному обеспечению. А в случае наличия в нем уязвимостей, пользователь может получить доступ к системе или нарушить ее нормальное функционирование.

Режим *Только локальная сеть (подсеть)* позволяет сделать возможным доступ к программному обеспечению только из сети, в которой находится система, что значительно снижает риск взлома даже при наличии уязвимостей в программном обеспечении. Если нужно разрешить доступ только с некоторых сетевых компьютеров, рекомендуется использовать третью опциею.

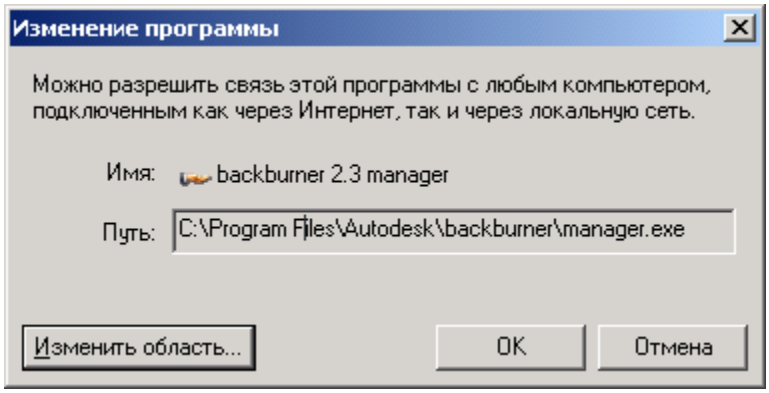


Рисунок 1.6. Диалоговое окно *Изменение программы*

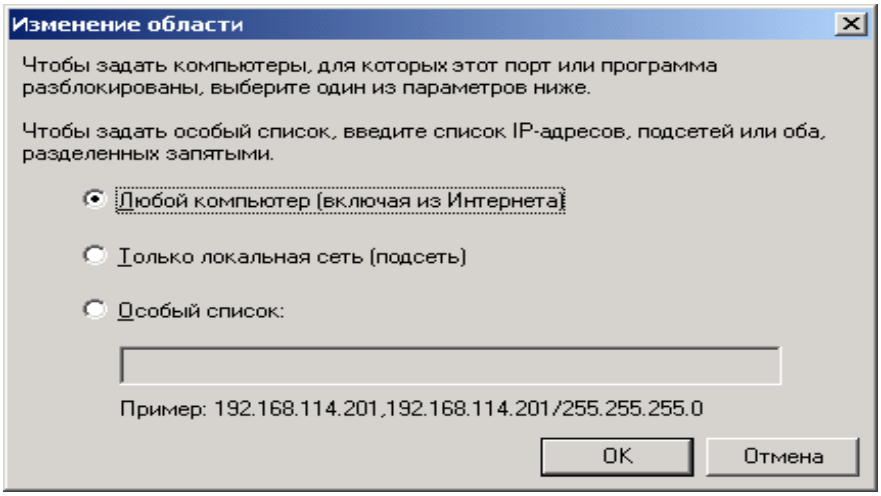


Рисунок 1.7. Диалоговое окно *Изменение области*

Режим *Особый список* позволяет указать в нижележащем поле ввода список *IP-адресов* (сетевой адрес вида *a.b.c.d*) компьютеров, которым будет разрешен доступ к выбранному сервису или программе. Это наиболее удобный и безопасный способ осуществления разрешения на доступ из сети, так как в этом случае всегда можно контролировать компьютеры, которые его получают, и быть уверенными в том, что система надежно защищена от атак. Рекомендуется использовать данный режим (если позволяет ситуация), как самый оптимальный из всех. Кнопка *ОК* сохраняет внесенные изменения в окне, кнопка *Отмена* – их отменяет.

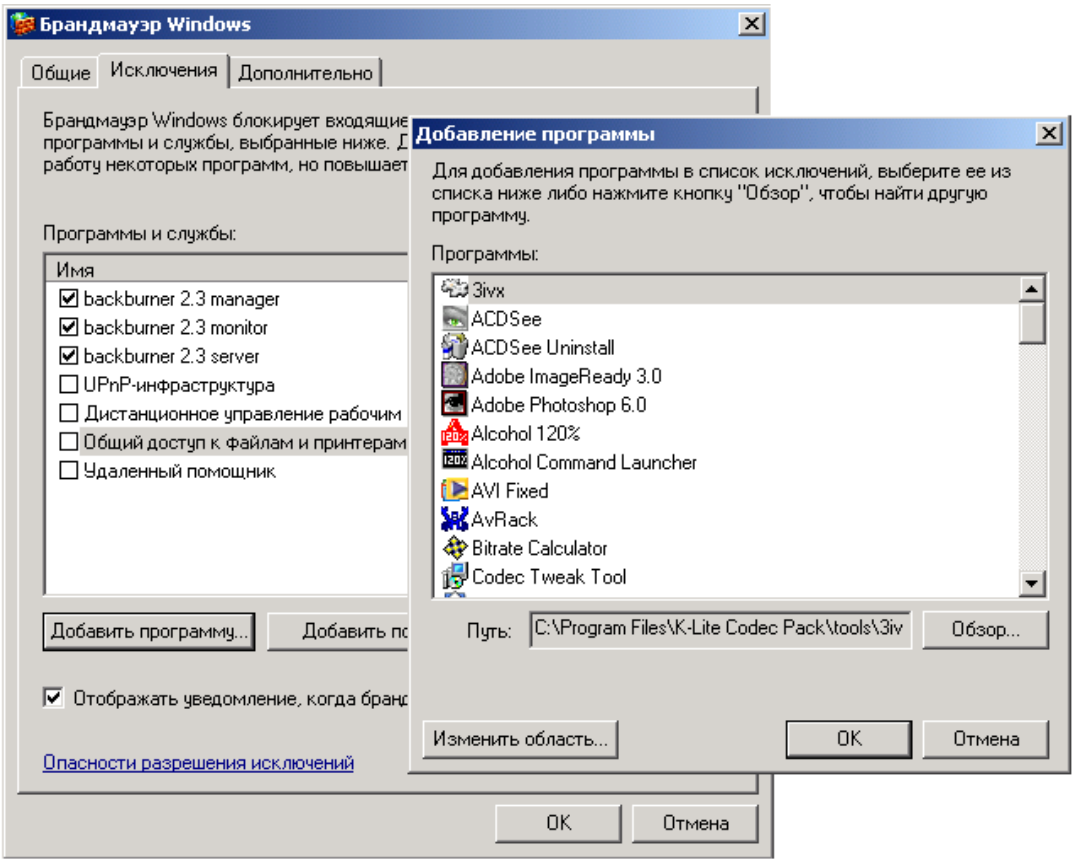


Рисунок 1.8. Диалоговое окно *Добавление программы*

В закладке *Исключения* кнопка *Добавить программу* позволяет добавить программы, к которым следует разрешить доступ со стороны сети (рис.1.8.). Из предлагаемого списка требуется выбрать нужное приложение или воспользоваться кнопкой *Обзор* и указать его исполняемый файл в файловой системе компьютера. С помощью кнопки *Изменить область* можно указать с каких сетевых компьютеров будет возможен доступ к данному приложению. Кнопка *ОК* сохраняет внесенные изменения, закрывая окно добавления программы, кнопка *Отмена* приводит к отмене всех дополнений сделанных в окне.

В закладке *Исключения* нажатие кнопки *Добавить порт* выводит диалоговое окно *Добавление порта* (рис.1.9.). Номер порта представляет собой канал, выраженный целочисленным десятичным числом, по которому приложения могут обмениваться информацией. Если используемому приложению требуется открыть определенный канал, то в поле *Имя* следует ввести имя приложения, в поле *Номер порта* – номер порта, сообщенный приложением. Флажковые опции *TCP* и *UDP* позволяют указать какой порт требуется приложению. Если необходимо создать два порта с одинаковыми номерами, но разными типами (*TCP* или *UDP*), то следует дважды воспользоваться функцией дополнения порта (кнопкой *Добавить порт*) (рис.1.9.), и с помощью кнопки *Изменить область* указать с каких сетевых компьютеров будет возможен доступ к данному порту. Кнопка *ОК* сохраняет внесенные изменения, кнопка *Отмена* приводит к отмене всех дополнений сделанных в окне.

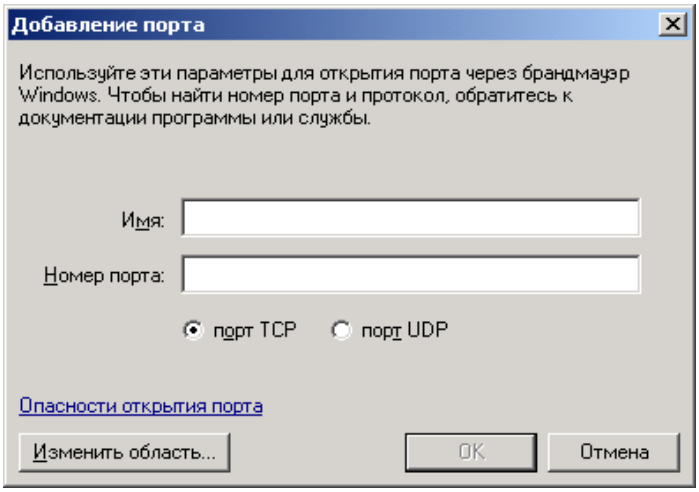


Рисунок 1.9. Диалоговое окно *Добавление порта*

Дополнительные параметры брандмауэра

В окне настроек брандмауэра в закладке *Дополнительно* находятся некоторые важные настройки (рис.1.10).

Первая группа элементов управления *Параметры сетевого подключения* позволяют избирательно использовать *брандмауэр* для сетевых интерфейсов системы. Сетевой фильтр включен только для интерфейсов, отмеченных флажками в списке *Службы* (рис.1.10.). Кнопка *Параметры* вызывает окно для настройки доступа сетевых пользователей к *сетевым сервисам* для выбранного сетевого соединения. *Сетевыми сервисами* называют программное обеспечение, запросы на обработку к которому поступают по сети. В этом случае компьютеры, от которых поступают запросы, называются *клиентами*, а компьютеры, которые их обрабатывают – *серверами*.

По умолчанию в окне представлено несколько наиболее часто используемых в Интернете сервисов. В случае их использования можно разрешить к ним доступ сетевых пользователей. Например, если используется в системе *FTP-* или *Web-сервер*, то можно разрешить к ним доступ пользователей из сети. Для этого необходимо установить флажки в режимах, соответственно, *с FTP-сервер* и *Веб-сервер* (*HTTP*) (рис.1.10.).

После установки флажка в любом из пунктов появится диалоговое окно, в котором система поинтересуется, на каком компьютере установлен сервис, к которому нужно разрешить доступ. По умолчанию предлагается адрес системы, на которой осуществляется настройка *брандмауэра* (рис.1.11.).

В поле ввода *Имя или IP-адрес компьютера вашей сети, на котором располагается эта служба (например, 192.168.0.12)* нужно ввести адрес компьютера, на котором расположен сервис (если он отличается от адреса системы с настраиваемым *брандмауэром*). Нажатие кнопки *ОК* приводит к закрытию окна *Параметры службы*, а в окне *Дополнительные параметры* (рис.1.10.) рядом с соответствующим пунктом появляется флажок. Кнопки *Добавить* и *Изменить* в окне *Дополнительные параметры* (рис.1.10.) приводят, соответственно к добавлению или редактированию существующего сервиса (рис.1.11.)

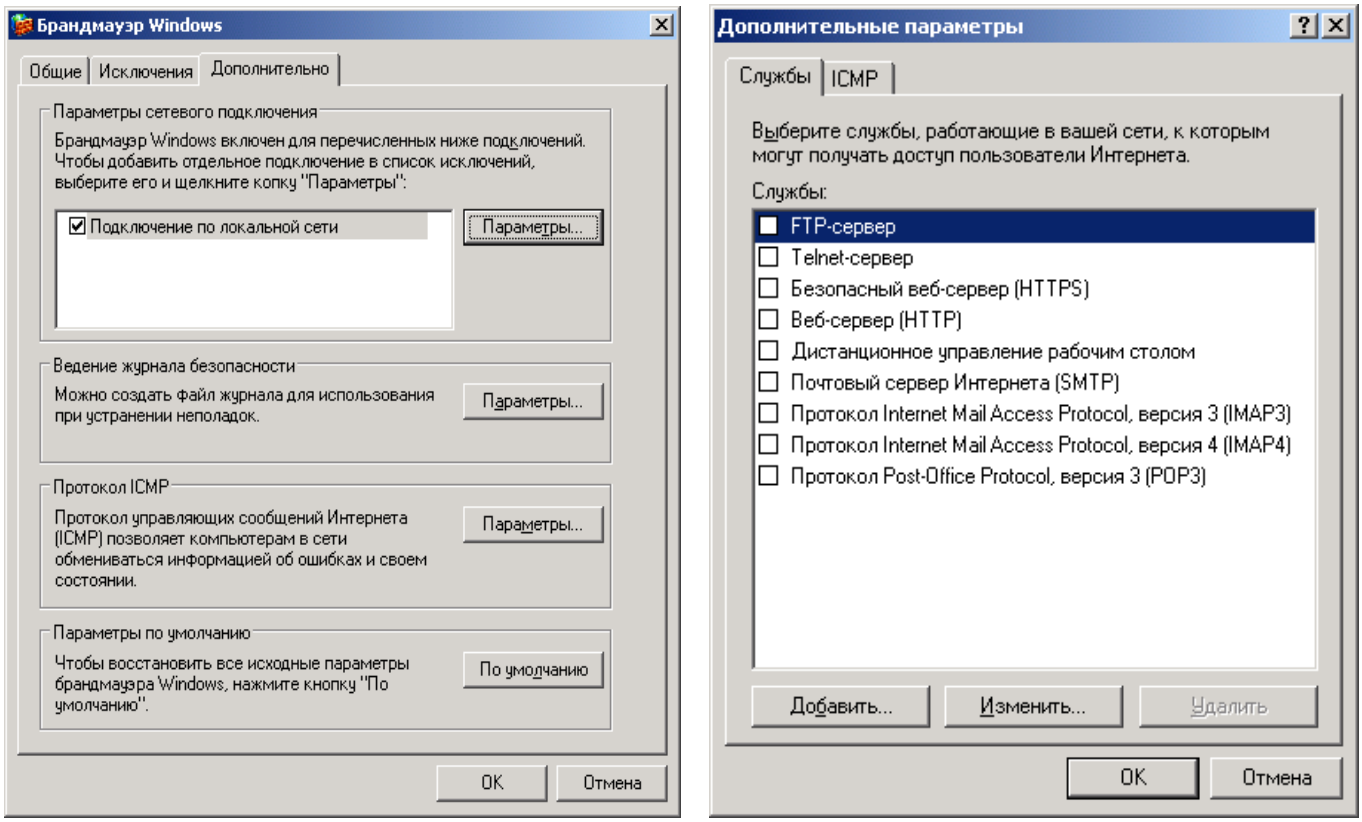


Рисунок 1.10. Закладка *Дополнительно* и окно выбора дополнительных параметров сетевого подключения

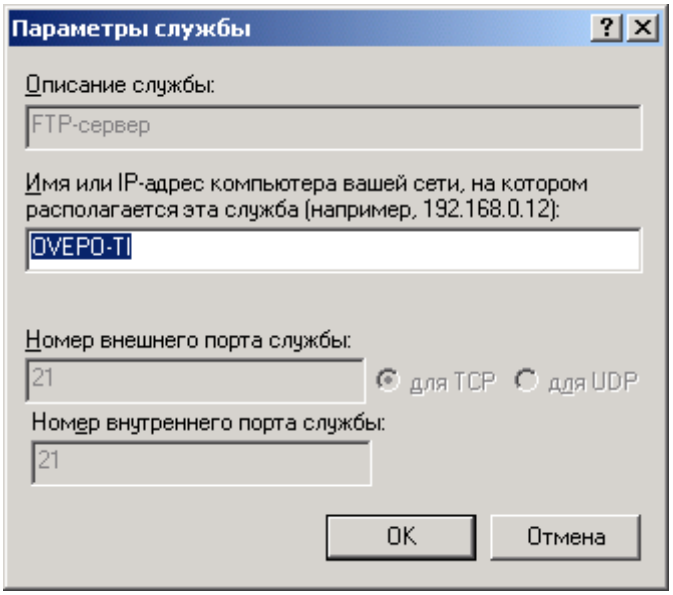


Рисунок 1.11. Установка адреса системы, на которой расположен сервис, доступ к которому открывается для сетевых пользователей

Закладка *ICMP* окна *Дополнительные параметры* позволяет установить доступность сетевых сервисов, выполняющих служебные функции (рис. 1.12.). *ICMP* (*Internet Control and Message Protocol*) означает отношение приведенных в окне *Дополнительные параметры – закладка ICMP* сервисов к протоколу обмена контрольной информацией в Интернете. Данный протокол предназначен для технических целей и поддерживает корректную работу компьютерной сети, а также может использоваться при поиске неисправности, неизбежно возникающих в сложных сетевых вычислительных структурах. Он реализован с помощью ряда программных сервисов, которые перечислены в списке данного окна.

Вышеперечисленные сервисы предназначены для решения только технических задач. Но существует, как минимум, два пути нарушения нормальной работы системы или причинения ей значительного вреда, если указанные сервисы не будут установлены.

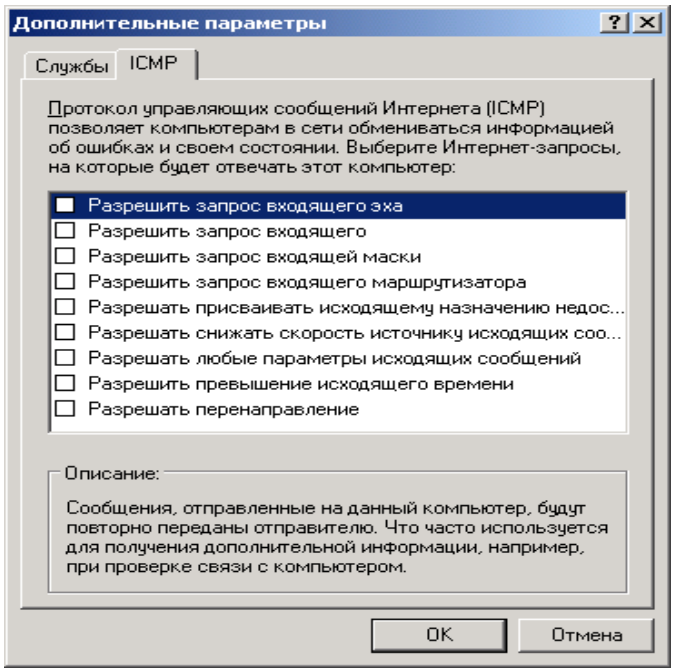


Рисунок 1.12. Закладка *ICMP*

Во-первых, возможен запрос взломщиков со стороны сети на выполнение системой различных действий для достижения определенных технических целей. Например, они могут послать системе запрос о ее существовании на определенный сетевой адрес. Если система находится по указанному адресу и функционирует нормально, то она может ответить на запрос. Взломщики могут послать множество таких запросов. Система будет отвечать на них, в результате чего ее производительность для полезных задач резко упадет, т.о. достигается атака *Отказ в обслуживании* (*DoS, Denied of Service*).

Также существуют методы посылки специфических запросов, которые будут вынуждать ОС расточительно использовать свои системные ресурсы, вследствие чего наступит момент, когда система перестанет функционировать и ее придется перезагружать.

Во-вторых, возможна атака, целью которой является получение контроля над системой. Она может иметь самые различные алгоритмы. Наиболее вероятным сценарием взлома является посылка специфического запроса системе, который не может быть корректно обработан и вызовет запуск определенной программы, содержащейся в нем (запросе). Эта программа может что-нибудь уничтожить в системе или открыть к ней доступ из Интернета для взломщиков.

Вышеприведенные ситуации говорят о том, что нужно очень осторожно относиться ко всей информации, приходящей из сети, даже если она содержится в служебных запросах. Поэтому все служебные сервисы *по умолчанию* заблокированы сетевым экраном.

Второй раздел элемента управления *Ведение журнала безопасности* вкладки *Дополнительно* (рис.1.10.) позволяет задавать настройки, позволяющие отслеживать и сохранять в файле состояние сетевого экрана. При нажатии кнопки *Параметры* появится окно настроек протоколирования работы *брандмауэра* (рис.1.13.).

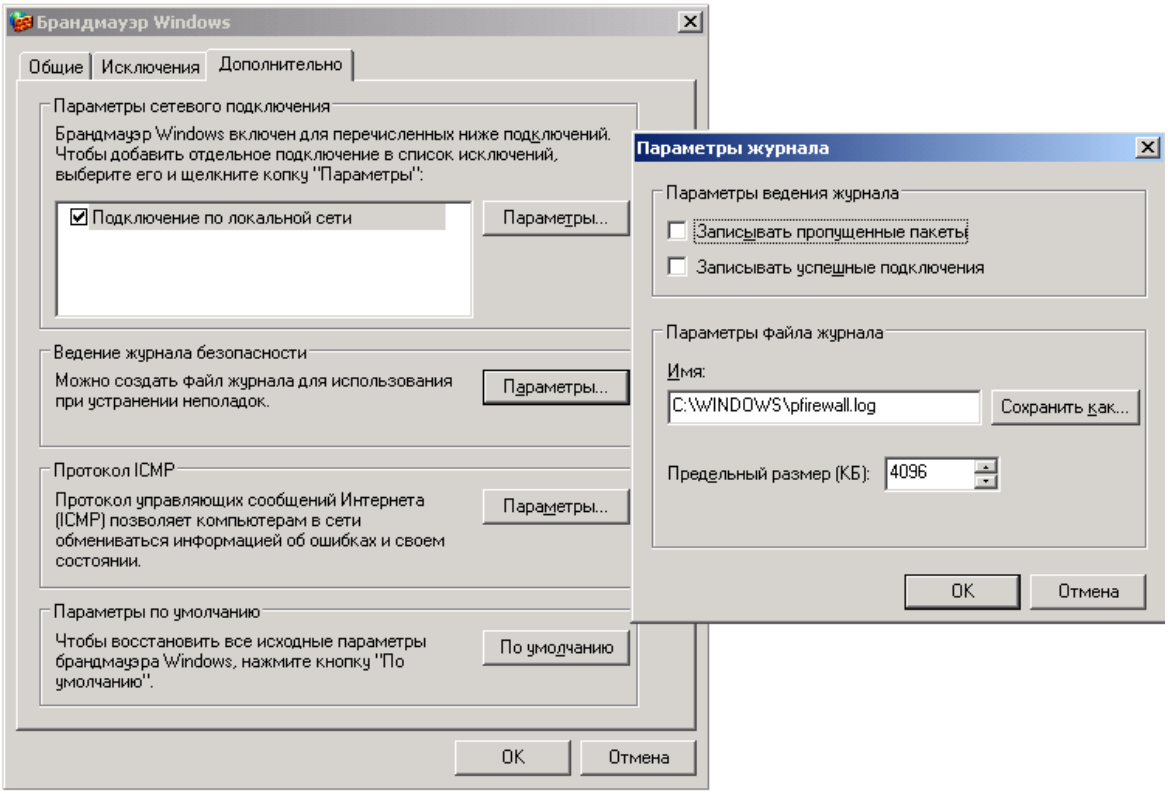


Рис.1.13. Окно настроек протоколирования работы сетевого экрана

Режим *Записывать пропущенные пакеты* в случае установки флажка позволяет системе сохранять в файле *C:\WINDOWS\pfirewall.log* все пакеты, отклоненные системой, что необходимо для просмотра возможных атак из сети или запрещенных адресов.

Режим *Записывать успешные подключения* в случае установки флажка, позволяет производить запись всех удачных соединений, произведенных с системой.

В разделе *Параметры файла журнала* находятся опции, в которых указывается имя файла для протоколирования действий *брандмауэра* и его максимальный размер. При указании пути и имени этого файла в поле ввода *Имя* следует учесть, чтобы данный файл не был доступен простым пользователям, которые могут использовать его по своему усмотрению. Поле *Предельный размер (КБ)* позволяет указать максимальный размер этого файла в килобайтах, по умолчанию установлен размер четыре мегабайта. Нажатие кнопки *ОК* сохраняет внесенные изменения и приводит к закрытию окна.

Третий раздел элемента управления *Протокол ICMP* (рис.1.13.) задает настройки, позволяющие отслеживать обработку системой *ICMP-запросов* сети. При нажатии кнопки *Параметры* появится диалоговое окно *Параметры ICMP*. Рекомендуется разрешать работу для сетевых пользователей только необходимых сервисов. По умолчанию разработчиками системы заданы настройки, подходящие для большинства пользователей.

Для восстановления принятых по умолчанию параметров *брандмауэра* предлагается нажать кнопку *По умолчанию* (рис. 1.13.).

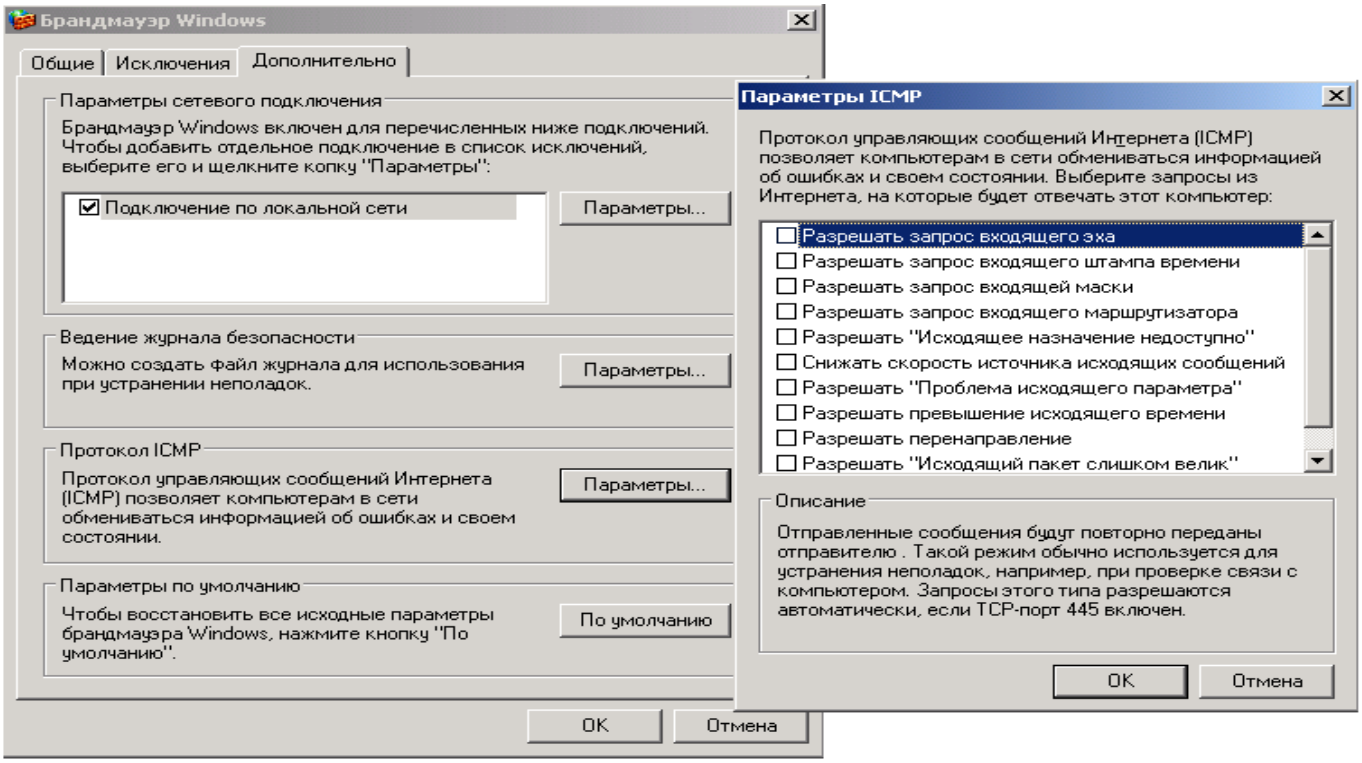


Рис.1.13. Окно настроек *Протокола ICMP*

Удаленные сеансы пользователей

Пользователям, у которых возникают вопросы по работе с системой, *Windows XP* предлагает помощь в виде развитой системы файлов помощи и в виде интерактивной помощи, одним из видов которой является помощь пользователей друг другу. Специальный механизм *Удаленные сеансы* позволяет пользователям помогать друг другу:

Пуск\Программы\Удаленный помощник (1.14.)

Настройка входа в систему удаленных пользователей:

- войти в систему под учетной записью администратора;
- в *Панели управления* выбрать программу *Система*:

Пуск\Настройка\Панель управления\Система (рис.1.15.)

- в появившемся окне *Свойства системы* выбрать закладку *Удаленные сеансы* (рис.1.16.)

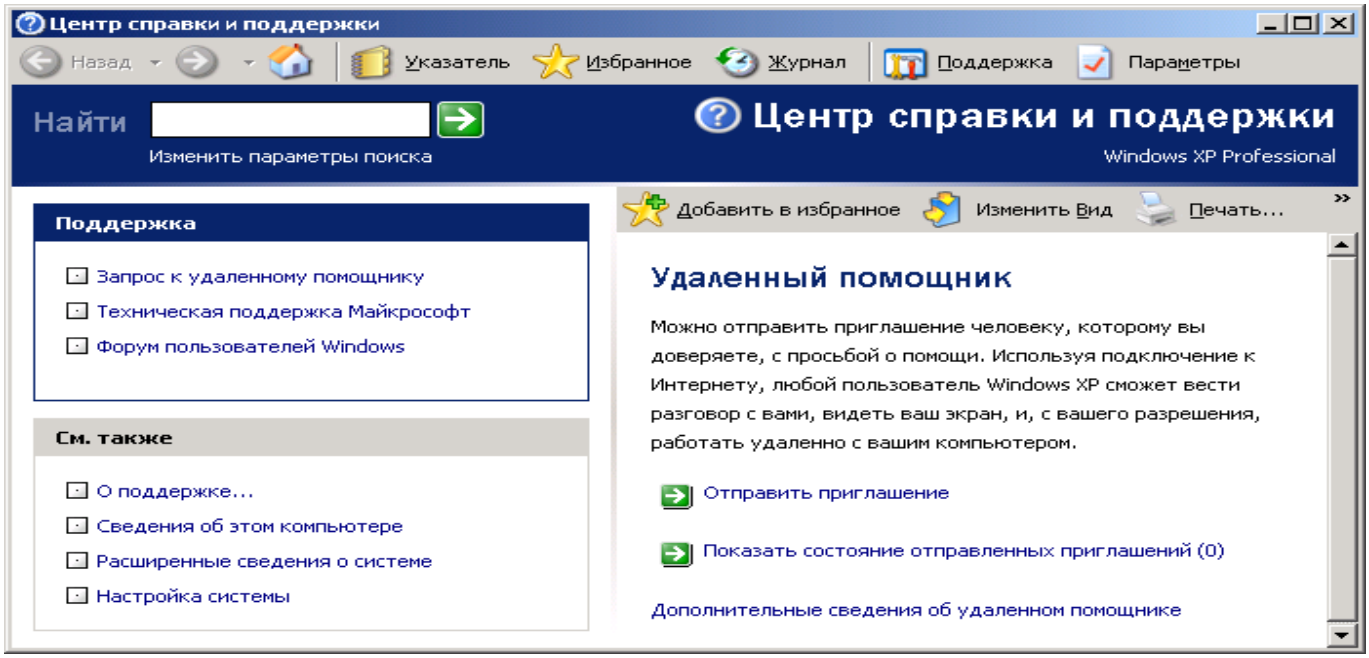


Рисунок 1.14. Окно программы *Удаленный помошник*

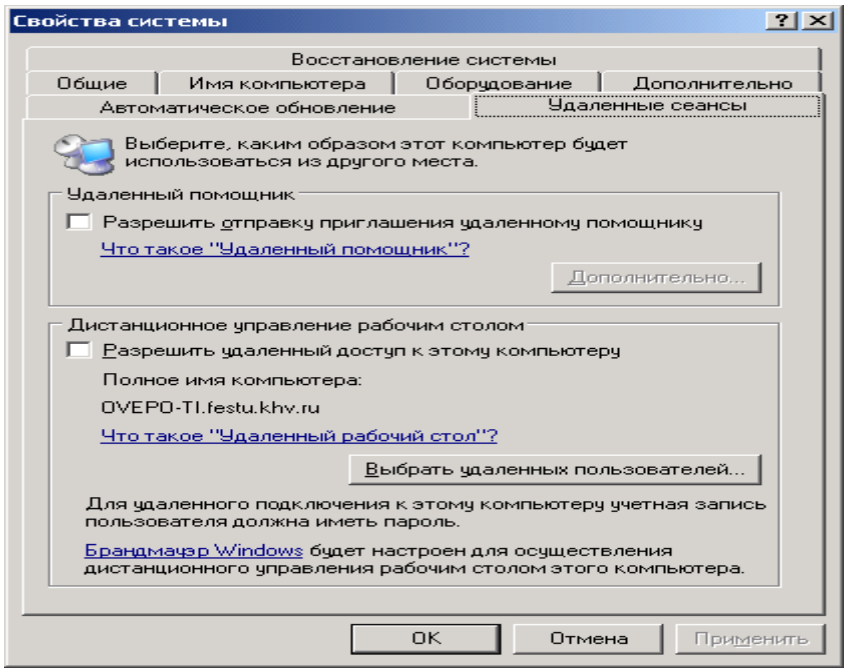


Рис. 1.15. Закладка *Удаленные сеансы* программы *Система*

Для дезактивации механизма удаленной помощи нужно убрать флажок в режиме *Разрешить отправку приглашений удаленному помощнику*, для использования механизма удаленной помощи нужно поставить флажок в данном режиме и нажать кнопку *Дополнительно* (рис.1.16.). Для осуществления полноценной процедуры поддержки пользователем (к которому нужно обратиться за помощью), следует установить флажок в режиме *Разрешить удаленное управление этим компьютером*. Следует осторожно относиться к данному режиму, т.к. он дает возможность выбранному пользователю управлять компьютером удаленно, поэтому, если намерения пользователя не ясны, то лучше этого не делать.

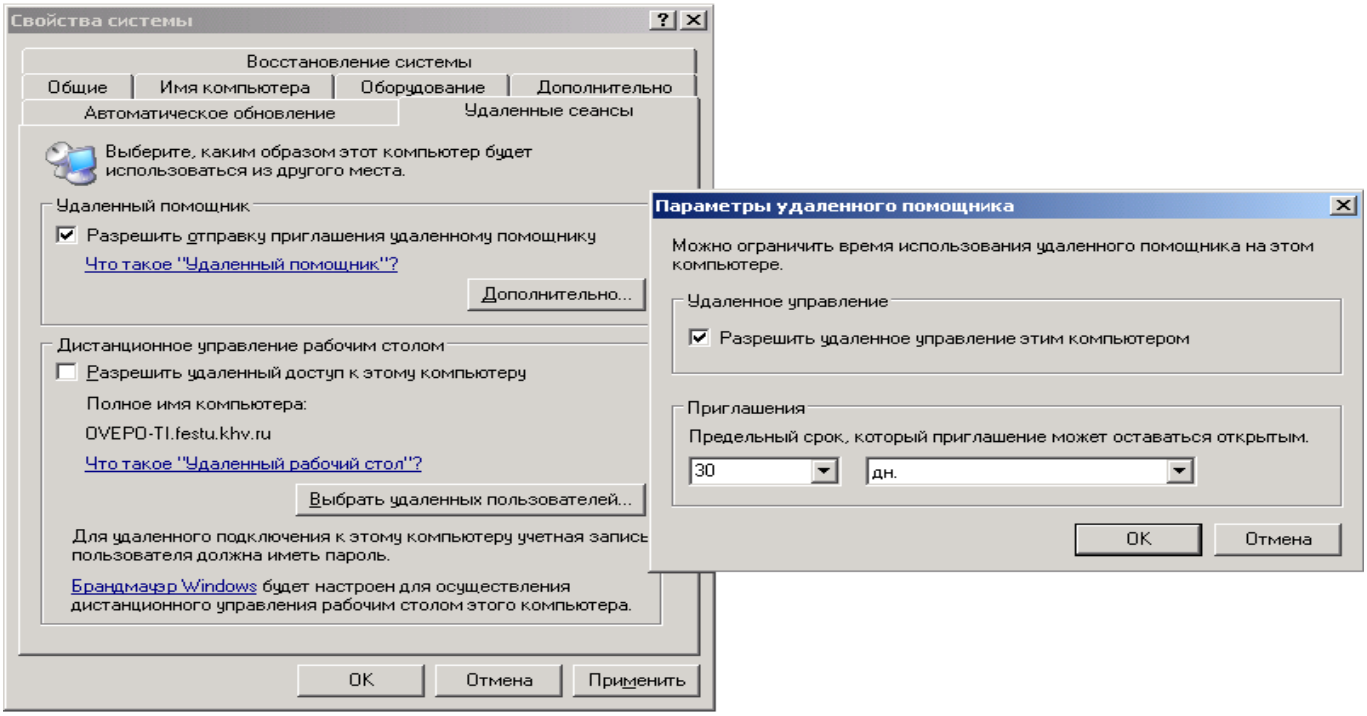


Рисунок 1.16. Окно настройки удаленной помощи

Последний режим определяет интервал времени, в течение которого запрос о помощи остается в силе для других пользователей. Нажатие кнопки *ОК* приводит к активизации выбранных настроек.

В целях безопасности рекомендуется запрещать механизм удаленной помощи, лучше обратиться в техническую поддержку *Microsoft*.

Удаленные пользователи

Если необходимо временно разрешить удаленный вход в систему сетевых пользователей с получением полного доступа следует:

- войти в систему под учетной записью администратора;
- в *Панели управления* выбрать программу *Система*:

Пуск\Настройка\Панель управления\Система (рис.1.15.)

- в появившемся окне *Свойства системы* выбрать закладку *Удаленные сеансы* (рис.1.16.);
- в поле *Дистанционной управление рабочим столом* поставить флажок в режиме *Разрешить удаленный доступ к этому компьютеру* (рис.1.17.);
- для уточнения пользователей, которым разрешен доступ сделать щелчок по кнопке *Выбрать удаленных пользователей* (рис.1.17.);
- появится диалоговое окно *Пользователи удаленного рабочего стола* в котором с помощью кнопок *Добавить* и *Удалить* можно, соответственно, добавлять и удалять пользователей;
- для добавления пользователей сделать щелчок по кнопке *Добавить*;
- в появившемся диалоговом окне *Выбор: Пользователи* сделать щелчок по кнопке *Дополнительно* (рис.1.18.);
- появится дополнительное окно со списком пользователей, которым разрешен доступ;
- щелчком выбрать имя пользователя, после чего окно закроется;
- для сохранения установленных настроек нажать кнопку *ОК*, для отмены – кнопку *Отмена*;
- после возврата к окну *Пользователи удаленного доступа* нажатие кнопки *ОК* приведет к тому, что все пользователи, отображенные в списке, получат возможность удаленно входить в систему и пользоваться ее интерфейсом, приложениями и документами, соответствующими учетной записи, под которой они входят в систему; все они должны быть локально прописанными в системе.

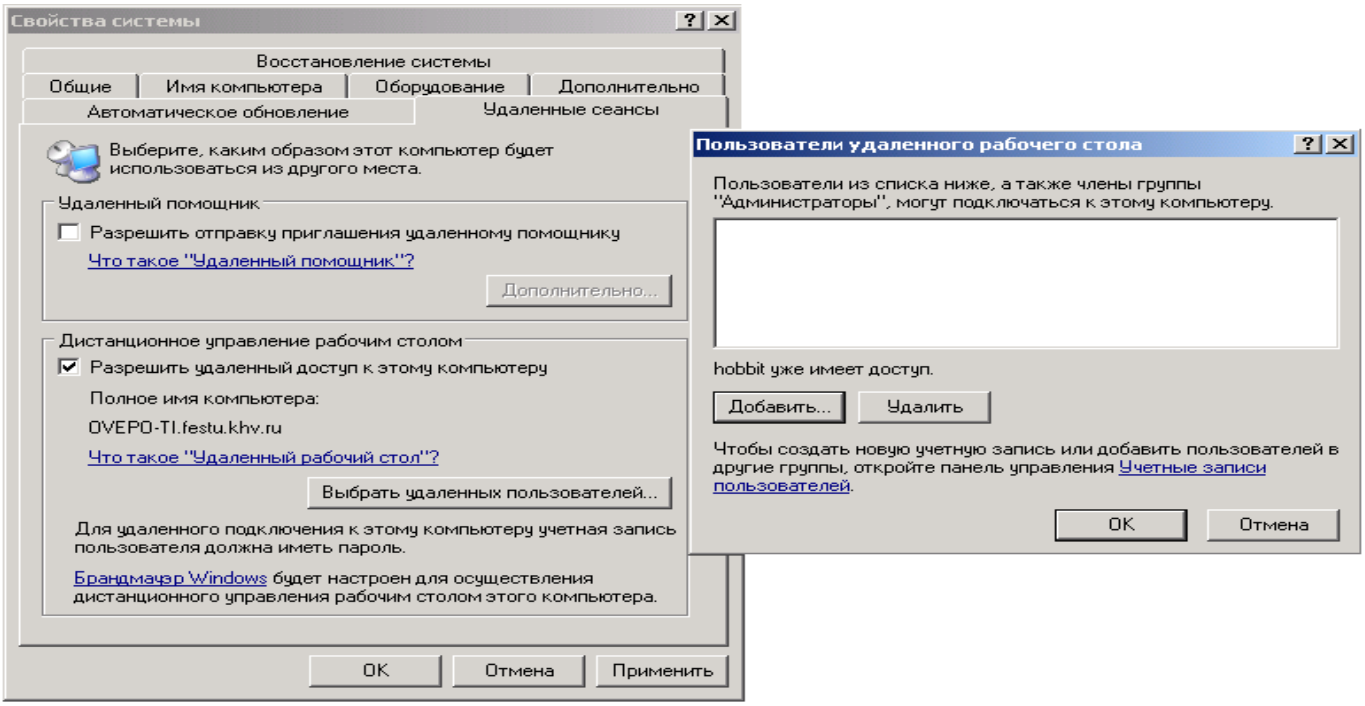


Рисунок 1.17. Окно определения пользователей,
имеющих права работать удаленно

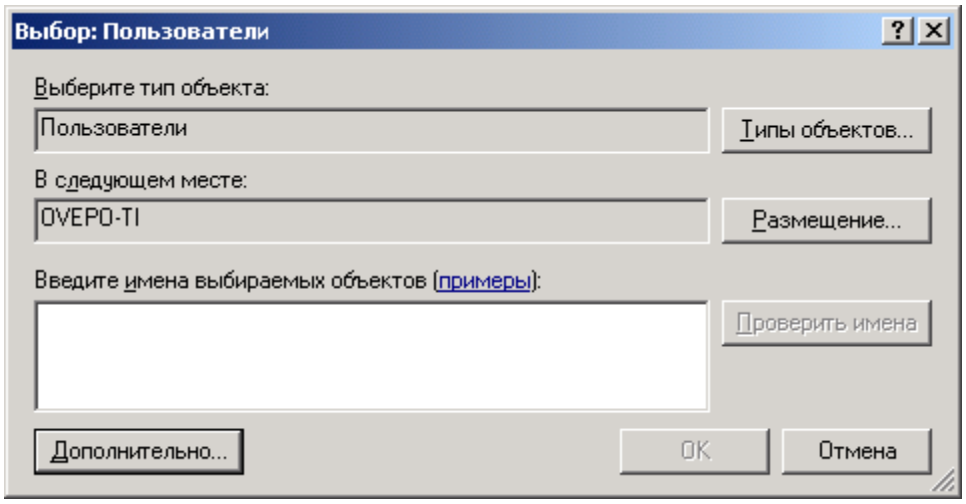


Рисунок 1.18. Выбор пользователей

Порядок выполнения

1.Произвести настройку *Брандмауэра* на своем ПК.
2.Произвести настройку механизма *Windows* «*Удаленные сеансы*» на своем ПК.
3.Произвести настройку механизма *Windows* «*Удаленные пользователи*» на своем ПК.

Содержание отчета

Отчет должен содержать:

- Название работы
- Цель работы
- Схему сетевой карты
- Описание технологии установки сетевой карты.

Контрольные вопросы

1. Определите назначение программы *Брандмауэр*.
2. Перечислите функции, выполняемые программой *Брандмауэр*.
3. На работе каких алгоритмов основывается работа взломщиков?
4. Опишите работу программы *Брандмауэр*.
5. Как настроить программу *Брандмауэр*?
6. Какие опции рекомендуется включать, а какие выключать в программе *Брандмауэр*?
7. Каким образом исключить программу или сервис из списка с запрещенным доступом в программе *Брандмауэр*?
8. В каком случае активизация опции *Отображать уведомление, когда брандмауэр блокирует программу* не даст результата в программе *Брандмауэр*?
9. Определите назначение режима *Только локальная сеть (подсеть)* в программе *Брандмауэр*.
10. Определите назначение режима *Особый список* в программе *Брандмауэр*.
11. Перечислите дополнительные параметры настройки *Брандмауэра*.
12. Определите назначение механизма *Windows* «*Удаленные сеансы».*
13. Как настроить механизм *Удаленные сеансы* в *Windows?*
14. Определите назначение механизма *Windows* «*Удаленные пользователи».*
15. Как настроить механизм *Удаленные пользователи* в *Windows*?

Рекомендуемая литература

Основная

1. Костров Б.В. Сети и системы передачи информации: учебник для студентов учреждений среднего профессионального образования / Б.В. Костров, В.Н. Ручкин. –М.: Издательский центр «Академия», 2017г.

Дополнительная

13. Литвинская О.С. Основы теории передачи информации: учебное пособие / Литвинская О.С., Чернышев Н.И. — Москва: КноРус, 2021 — 168 с. — ISBN 978-5-406-08653-7. — URL: https://book.ru/book/940469 (дата обращения: 23.04.2021). —Текст: электронный.