РОСЖЕЛДОР
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Ростовский государственный университет путей сообщения»
(ФГБОУ ВО РГУПС)
Филиал РГУПС в г. Воронеж

Утверждаю:
Заместитель директора по УПР филиала
РГУПС в г. Воронеж
_____ Гуленко П.И
«01» сентября 2023 г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 56e04e82f2d91c396292d43d4b4c48071
Владелец: Гуленко Петр Игоревич
Действителен: с 06.06.2023 по 29.08.2024

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

по МДК 05.01 Компьютерные и телекоммуникационные сети

Специальность: 09.02.01 Компьютерные системы и комплексы

Профиль: технический

Квалификация выпускника: техник по компьютерным системам

Форма обучения: очная

Воронеж 2023 г.

Авторы-составители преподаватели высшей категории
Толубаева Л.А., Русинова Е.С.
предлагают методические указания по выполнению практических работ
по МДК 05.01 Компьютерные и телекоммуникационные сети

Протокол № 04 от 01.09.2023 г.
Председатель цикловой комиссии_____ Русинова Е.С.
(подпись) (Ф.И.О.)

СОДЕРЖАНИЕ

1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические указания для проведения практических занятий составлены в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.01 Компьютерные системы и комплексы, учебным планом и рабочей программой ПМ.05 Компьютерные и телекоммуникационные сети. Методические указания предназначены для студентов и преподавателей средних профессиональных учебных заведений, изучающих МДК 05.01 Компьютерные и телекоммуникационные сети.

Данные указания содержат необходимый теоретический материал, задания, необходимые для выполнения практических работ.

Целью изучения МДК 05.01 Компьютерные и телекоммуникационные сети является освоение следующих компетенций:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК 5.1. Проектировать и администрировать локально-вычислительные сети.

ПК 5.2. Проводить контроль, диагностику и восстановление работоспособности компьютерных и вычислительных сетей.

ПК 5.3. Определять методы и основные принципы защиты информации от несанкционированного доступа.

ПК 5.4. Настраивать виды соединений в IP - телефонии и взаимодействие с компьютерной сетью.

В результате выполнения практических работ обучающийся должен

уметь:

- участвовать в проектировании, монтаже и эксплуатации и диагностике компьютерных сетей;
- правильно выявлять и оценивать угрозы безопасности информации;
- категорировать информацию в соответствии с действующим законодательством;
- определять сферу действия и использовать законодательство в области информацион-

ной безопасности;
- реализовывать технологии VPN и VLAN;
- правильно выбирать программные и/или аппаратные средства защиты информации от всех видов угроз по различным критериям;
- использовать оснастки политик безопасности различных операционных систем;

знать:

- типы сетей, серверов, сетевую топологию;
- типы передачи данных, стандартные стеки коммуникационных протоколов;
- установку и конфигурирование сетевого оборудования;
- принципы построения телекоммуникационных вычислительных сетей (ТВС);
- принципы построения беспроводного соединения;
- основы технологии IP – телефонии;
- технологию виртуальных частных сетей VPN;
- технологию виртуальных сетей;
- методы и средства обеспечения информационной безопасности;
- защиту от несанкционированного доступа, основные принципы защиты информации;
- технические методы и средства защиты информации.

2 ТЕМАТИЧЕСКИЙ ПЛАН

№№ п/п	Наименование темы	Количество часов
1	**2**	**3**
1.	Организация одноранговой сети.	2
2.	Изучение типов серверов и их настройка	2
3.	Изучение уровней управления модели OSI	2
4.	Методы передачи данных	2
5.	Стек протоколов ГСР/1Р, ipx/spx	2
6.	Настройка стека протоколов TCP/IP	2
7.	Изучение сетевого адаптера	2
8.	Сравнительная характеристика базовых технологий локальных сетей	2
9.	Расчет Ethernet - сетей , состоящих из сегментов различных технологий	2
10.	Команды обновления микропрограммного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов	2
11.	Анализ трафика компьютерной сети с помощью снифферов	2
12.	Основные команды коммутаторов. Управление коммутаторами	2
13.	Построение ЛВС. Структурированная кабельная система.	2
14.	Построение ЛВС. Структурированная кабельная система.	2
15.	Адресация в IP- сетях. Подсети и маски.	2
16.	Адресация в IP- сетях. Подсети и маски.	2
17.	Адресация в IP- сетях. Подсети и маски.	2
18.	Команды VLAN на основе портов и меток 802. Iq	2
19.	Изучение принципа работы маршрутизаторов	2
20.	Изучение принципа работы маршрутизаторов	2
21.	Изучение системы управления сетевым оборудованием. Протокол SNMP	2
22.	Изучение системы управления сетевым оборудованием. Протокол SNMP	2
23.	Протокол маршрутизации RIP	2
24.	Протокол маршрутизации OSPF. Построение маршрутных таблиц	2
25.	Изучение базовых элементов технологий WWW	2
26.	Настройка браузеров	2
27.	Элементы управления сетью. Общий доступ к ресурсам	2
28.	Построение составной сети	2
29.	Построение составной сети	2
30.	Сетевые утилиты	2
31.	Разграничение доступа	2
32.	Разграничение доступа	2
	Итого:	**64**

Практическая работа № 1

ОРГАНИЗАЦИЯ ОДНОРАНГОВОЙ СЕТИ

Цель работы: изучить характеристики одноранговой сети.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия

Подготовка к работе: Используя имеющийся теоретический материал, изучить характеристики одноранговой сети. Ответить на контрольные вопросы.

Общие сведения:

Особенности организации локальных сетей

Компьютерные сети, в том числе ЛВС, реализуют распределенную обработку данных. При этом обработка ведется, как правило, двумя объектами: клиентом и сервером.

Операционные системы

В одноранговой сети требования к производительности и к уровню защиты для сетевого программного обеспечения, как правило, ниже, чем в сетях с выделенным сервером. Выделенные серверы функционируют исключительно в качестве серверов, но не клиентов или рабочих станций (workstation). О них мы еще поговорим подробнее на этом занятии, но чуть позже.

Клиент — это задача, рабочая станция или пользователь сети. В процессе работы клиент может формировать запрос на сервер для выполнения сложных процедур, чтения файла, поиска информации в базе данных и т.д.

Сервер выполняет запрос клиента. Результаты выполнения запроса передаются клиенту.

Клиент обрабатывает полученные результаты работы сервера и выдает их пользователю. В принципе возможна обработка результатов и на сервере.

Для подобных систем приняты термины: система клиент—сервер, архитектура клиент—сервер (рис. 1). Архитектура клиент—сервер может использоваться как в одноранговых локальных сетях, так и в сетях с выделенным сервером. Настоящая лабораторная работа посвящена одноранговым сетям.

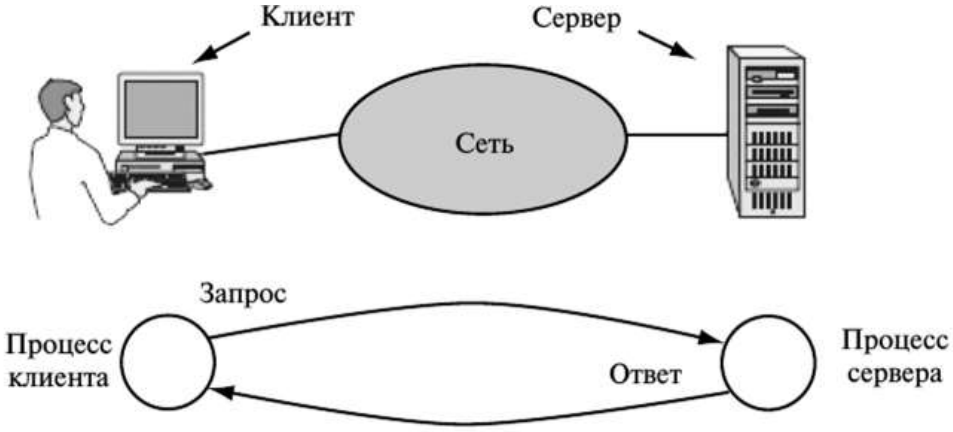


Рис. 1

В одноранговых сетях нет единого центра управления взаимодействием рабочих станций и нет единого устройства для хранения данных. Все компьютеры равноправны, каждый компьютер

функционирует и как клиент, и как сервер. Пользователи самостоятельно решают, какие данные на своем компьютере сделать общедоступными. Каждая рабочая станция может обслуживать запросы от других компьютеров и направлять свои запросы на обслуживание в сеть.

Пользователям сети могут быть доступны все устройства, подключенные к другим рабочим станциям: принтеры, диски, графопостроители, сканеры и т.п.

Одноранговая сеть характеризуется рядом стандартных решений:

- используется неспециализированная (клиентская) сетевая ОС;
- пользователи сами выступают в роли администраторов и обеспечивают защиту информации;
- для объединения компьютеров в сеть, как правило, применяется простая кабельная система.

Применение одноранговых ЛВС целесообразно в следующих случаях:

1) количество пользователей меньше 10;
2) пользователи расположены компактно;
3) вопросы защиты данных некритичны;
4) в обозримом будущем не ожидается значительного расширения предприятия и, следовательно, его компьютерной сети.

Достоинства одноранговых сетей:

- низкая стоимость;
- простота установки;
- высокая надежность.

Недостатки одноранговых сетей:

- зависимость эффективности работы от количества рабочих станций;
- сложность управления сетью;
- сложность обеспечения защиты информации;
- трудности обновления и изменения ПО рабочих станций.

Поддержка одноранговых сетей встроена в популярные ОС: Windows 98, Windows ME, Windows NT Workstation, Windows 2000 Standard, Windows XP, Windows Vista, Windows 7. Поэтому для установки одноранговых сетей дополнительного ПО, кроме установленной ОС, не требуется. Настоящая лабораторная работа предусматривает настройку сети под управлением ОС Windows 8. Несмотря на то что поддержка этой ОС компанией Microsoft уже не производится, Windows 8 в ряде случаев остается еще популярной благодаря своей компактности и нетребовательности к ресурсам компьютера. Это позволяет добиться удовлетворительных результатов при исследовании сетевых технологий в случае разворачивания на одном компьютере виртуальной информационной сети. В этом случае, кроме основной, хостовой ОС, должно быть инсталлировано несколько гостевых ОС, что резко ужесточает требования к ресурсам компьютера. Действительно, каждая гостевая ОС требует для своей работы столько же ресурсов, сколько и хосто- вая ОС. Поэтому развертывание на одном компьютере нескольких ОС Windows XP уже может быть проблематичным для компьютерных классов вузов среднего уровня, не говоря о последних версиях Windows Vista и Windows 7. Кроме того, исследования ОС Windows 8 позволяют проследить эволюцию и основные тенденции развития сетевой поддержки клиентскими ОС.

Протоколы для работы в сети

Для обеспечения взаимодействия между собой компьютеров и другого сетевого оборудования необходимы стандартизованные правила обмена информацией между ними. Такие своды правил и инструкций для информационных сетей называют протоколами. Как и дипломатический протокол, это свод санкционированных действий на предстоящий дипломатический раут. Компь-

ютерный протокол является утвержденным сводом правил обмена сообщениями между двумя компьютерами в предстоящем сеансе связи между ними.

Модель OSI предполагает независимую работу сетевого оборудования и ПО на семи уровнях (табл. 1). Каждый уровень независим от других, что при необходимости позволяет модернизировать его, не меняя остальных.

Таблица 1

Номер уровня	Название уровня
7	Прикладной (программы пользователя)
6	Представительный (управление представлением данных)
5	Сеансовый (управление сеансами связи)
4	Транспортный (управление передачей данных)
3	Сетевой (управление адресацией и маршрутом)
2	Канальный (управление логическим каналом передачи информации)
1	Физический (управление физическим каналом передачи информации)

Однако на практике семиуровневый стек протоколов OSI принят лишь в отдельных странах Европы. Это объясняется тем, что к моменту принятия модели OSI уже были созданы и успешно функционировали другие стеки протоколов: TCP/IP оборонного ведомства США; IPX/SPX компании Nowell; AppleTalk компании Apple.

Недостатком модели OSI также является, быть может, излишняя детализация уровней. Все другие практически применяемые стеки протоколов используют, как правило, деление на четыре-пять протокольных уровней. В настоящее время наиболее популярны стеки TCP/ IP и IPX/SPX, которые охватывают около 90% пользователей по всему миру соответственно.

В этой связи компания Microsoft в свои ОС включает поддержку стеков протоколов TCP/IP и IPX/SPX и не включает поддержку стека OSI. Компания Microsoft использует стек IPX/SPX под другим названием — NWLink. Таблица 2.2 иллюстрирует соответствие протоколов указанных стеков уровням модели OSI. Кроме стеков TCP/IP и IPX/SPX ОС Windows поддерживают еще ряд протоколов, в том числе фирменные протоколы компаний Microsoft и IBM: NetBIOS и NetBEUI, входящие в стек протоколов NetBIOS/SMB.

Таблица 2

Номер уровня	Стек OSI	Стек TCP/IP	Стек IPX/ SPX		Стек NetBIOS/ SMB
7	Прикладной				
6	Представительный	Telnet, HTTP, SMTP, FTP	SAP, NCP		SMB
5	Сеансовый				NetBIOS,
4	Транспортный	TCP, UDP	SPX	IPX	NetBEUI
3	Сетевой	IP, RIP, ARP	RIP		—
2	Канальный	Драйверы сетевой интерфейсной карты — NIC			
1	Физический	Коаксиал, витая пара, оптоволокно, радиоволны			

При желании пользователь может выбрать для себя удобный стек. Для этого перед включением в сетевую работу им должна быть настроена ОС. Указанная настройка входит в объем настоящей лабораторной работы. Выбор стека может определяться рядом факторов. По умолчанию в ОС Windows 8 устанавливается стек протоколов TCP/IP. Для большинства сетей такая установка является оправданной, поскольку, как правило, пользователям сети необходим выход в Интернет, а функционирование Интернета основано на стеке протоколов TCP/IP.

Стек IPX/SPX требует от компьютера и от сети меньшего количества ресурсов, чем стек TCP/IP. Поэтому, если нет необходимости выхода в Интернет, его использование может быть предпочтительным при применении в локальной сети компьютеров с ограниченными возможностями.

Стек протоколов NetBIOS/SMB широко применяется в продукции компаний IBM и Microsoft. Это достаточно эффективный стек, не требующий больших компьютерных ресурсов, однако он не поддерживает маршрутизацию и логически сегментированные сети, а также сети с числом компьютеров более 200. В этой связи его поддержка в последних версиях операционной системы Windows XP, Windows Vista исключена. Однако, когда в сетях используются унаследованные приложения и если сеть является простейшей, односегментной с малым числом компьютеров, добавление протоколов NetBIOS, NetBEUI может быть осуществлено в любую из ОС Windows.

Подчеркнем еще раз, что свое теоретическое значение эталонная модель OSI сохраняет. С ее помощью, как правило, всегда теоретически изучают вопросы взаимодействия открытых систем, поскольку модель OSI дает исчерпывающее описание уровней этого взаимодействия.

Контрольные вопросы:

1. Какие типы сетей распространены?
2. Характеристика одноранговой сети.
3. Характеристика сети с выделенным сервером.

Практическая работа № 2

ИЗУЧЕНИЕ ТИПОВ СЕРВЕРОВ И ИХ НАСТРОЙКА

Цель работы: изучить типы серверов.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия.

Подготовка к работе: Используя имеющийся теоретический материал, изучить типы серверов. Ответить на контрольные вопросы.

Общие сведения:

Специфика обслуживания сервера

Техническое обслуживание серверов и сопутствующего оборудования – важное условие качественной и стабильной работы информационных систем. Именно от него зависит сохранность информации и ее защищенность от несанкционированного доступа.

Полное комплексное обслуживание серверов включает в себя множество операций. В первуюочередь оно предполагает собственно монтаж, настройку и обслуживание серверов и серверного оборудования.

Перед тем как осуществить монтаж серверного оборудования, подвергаются серьезному анализу всетребования, которые имеются к технике. И на их основе выбирается именно тот вид оснащения и конфигурация системы, которые уместны в данном конкретном случае.

Потом осуществляется установка серверного оборудования, его конфигурирование. Затем его подключают и производят запуск. Устанавливается, тестируется, настраивается и начинает использоваться необходимое программное обеспечение.

Когда все необходимые операции будут произведены, в постоянном режиме обслуживания сервера производится:

- непрерывный мониторинг состояния системы и отдельных ее сервисов
- осуществляется поддержка ее работоспособности
- осуществляется проверка основного и резервного электропитания
- необходимо достаточно часто проверять и заменять аккумуляторы
- работу устройств ввода/вывода, к которым относятся клавиатура, мышь, монитор, свитчи для их подключения к системным блокам, провода и разъемы
- регулярно следует осматривать кабели на предмет внешних повреждений
- проверке также подвергается уровень нагрева тепловыделяющих компонентов аппаратуры и работа систем вентиляции и кондиционирования – в данном случае крайне важно, чтобы не было никаких помех для охлаждения оснащения

В операции по обслуживанию сервера также входит ремонт оснащения и замена комплектующих в том случае, если нагрузка на сервер будет повышаться.

Также осуществляется проверка правильности настройки сервера, обеспечение хорошей их работы с помощью частой проверки программных и аппаратных составляющих. Особое внимание уделяется управлению правом доступа к секретной информации и периодическое резервное копирование. В связи с этим происходит постоянная проверка работоспособности и износа оборудования резервного копирования.

Одной из целей выполняемых работ по обслуживанию серверов являются защита данных как от внешних опасностей, к примеру, от несанкционированного доступа и вредоносных программ, именуемых вирусами, так и от внутренних, к которым относятся сбои в работе программного обеспечения.

Помимо прочих вышеуказанных процедур при осуществлении обслуживания серверов, обязательных для совершения, также важно проводить периодическую чистку серверов.

В течение определенного времени в серверном корпусе и блоках питания собирается грязь и пыль, от которой крайне важно своевременно избавляться. В противном случае вы можете столкнуться с крайне неприятной ситуацией - перегревом системы. Также крайне важной процедурой является осмотр рабочей способности вентиляторов. Если не совершать вышеуказанные процедуры своевременно, в результате может существенно замедлиться работа серверного оснащения или оно даже придет в негодность. Для того чтобы подобная проблема не возникала, вам следует периодически осуществлять проводить проверку и чистку сервера.

Помимо прочих процедур, в перечень услуг, предоставляемых компаниями, занимающимися обслуживанием серверов, также включены работы:

- по диагностике и аудиту оснащения

Вряд ли для кого-то будет секретом тот факт, что по истечении определенного промежутка времени системы начинают работать медленнее, что становится заметно без определенных замеров времени.

В задачи аудита входит повышение производительности систем и произведение перенастройки и модернизации серверного оснащения. Постоянный контроль помогает осуществить диагностику на ранних этапах возникновения неполадок. Благодаря этому не возникают различные критические ситуации при работе системы.

К операциям по обслуживанию сервера причисляют обновление ОС (операционных систем), программ и контрольной панели.

В связи с этим специалист, занимающийся обслуживанием серверов, периодически осуществляет проверку наличия последних обновлений ПО. Важным направлением работы специалиста, занимающегося обслуживанием серверов, является:

- поддержка и администрирование корпоративной почты

К примеру, он будет заниматься образованием и изменением учетных записей почты, обеспечением ее приватности.

Благодаря обслуживанию серверов становится возможной проверка сроков окончания лицензий.

Чтобы определить, насколько хорошо будет работать сервер, специалист проверяет его скорость работы, целостность, приходящуюся на него среднюю и пиковую нагрузку, систему дублирования, резервирования и т. д.

В обслуживание серверов входит:

- оптимизация интернет-трафика, которая предполагает ее фильтрацию
- осуществляется проверка суммарного внешнего трафика, выясняется, какие порты являются открытыми, заполняются устройства массовой памяти.

Существует и такой вид обслуживания серверов, как удаленное администрирование.

Он включает в себя управление учетными записями и соответствующими сетевыми ресурсами. Данный вид работ предполагает обслуживание специализированных серверных ролей, к которым относятся Active Directory, Exchange Server, ISA, SQL и другие.

Организация файл-сервера предприятия на базе Free BSD или Linux

Для централизованного хранения данных, необходимых для работы предприятия, используется файловый сервер. Как правило, это выделенный компьютер, работающий под серверной операционной системой и имеющий быструю и надежную дисковую подсистему. Помимо хранения и организации доступа к документам, файловый сервер решает такую важную задачу, как разграничение прав доступа пользователей к информации. Каждый сотрудник может просматривать или вносить изменения только в те документы, на которые он имеет соответствующие права.

Хранение всех данных в одном месте сильно упрощает управление правами доступа пользователей.

Если в локальной сети присутствуют рабочие станции под управлением операционных систем семейства Windows, что характерно для большинства предприятий, то для общего доступа к файлам и принтерам используется протокол SMB.

Использование серверных продуктов от Microsoft не всегда может оказаться оправданным по экономическим соображениям. Тем более, когда есть альтернатива.

Экономичным и в то же время производительным и надежным решением может выступить операционная система Free BSD или Linux.

Для организации доступа к данным используется свободная реализация SMB протокола – Samba. Установка Samba позволяет использовать компьютер на базе Free BSD или Linux в качестве члена домена либо контроллера домена (PDC) в Windows сети. Так же Samba может стать частью домена Active Directory. Для того чтобы обеспечить общую систему безопасности Active Directory, используется протокол Kerberos. Поддержка данного протокола в FreeBSD может быть реализована при помощи программы heimdal.

Таким образом возможна организация сети предприятия, в которой клиентские машины работают под управлением Windows, в то время как для серверов используют Free BSD или Linux системы.

Несмотря на то, что у некоторых специалистов подобная идея может вызвать сомнение, совместную работу Windows и UNIX систем в одной сети настроить можно. Причем сложность подобного решения вовсе не так высока, как это может показаться на первый взгляд. Вместе с тем, настроить и в дальнейшем обслуживать сервер Linux / Free BSD будет более выгодно силами компаний профессионально занимающихся обслуживанием серверов.

Доступность веб-интерфейсов настройки печати и доступа к файлам, а также возможность настройки при помощи ACL управления правами доступа при помощи стандартного инструментария Windows делают администрирование подобной системы достаточно несложным. С текущим обслуживанием сервера может справиться любой сотрудник, имеющий минимальные навыки работы в операционных системах, схожих с UNIX. Опытный администратор или специализированная компания, предоставляющая услуги по обслуживанию серверов Linux / Free BSD понадобится только на этапе проектирования и внедрения системы.

К преимуществам серверов, работающих под управлением Free BSD или Linux систем, можно отнести:

- высокую производительность
- возможность гибкой настройки практически под любые задачи

– и высокую стабильность.

Системы Free BSD и Linux отличаются большой гибкостью настройки. Их можно адаптировать практические под любые задачи. На работающем сервере будут исполняться только те процессы, которые необходимы, что экономит системные ресурсы и снижает вероятность возникновения программного сбоя.

Обслуживание файлового сервера на основе Free BSD с установленной Samba может осуществляться путем внесения изменений в файл конфигурации smb.conf, оторый после инсталляции Samba должен находиться по адресу /usr/local/etc/smb.conf. Его можно создать либо воспользоваться образцом smb.conf.sample, куда вносятся все необходимые изменения. Для облегчения процесса настройки Samba можно использовать веб-интерфейс SWAT. К преимуществам его использования, помимо графического интерфейса, можно отнести хорошую систему справки по всем параметрам настройки.

Порой возникает ситуация, когда руководителю или ответственному сотруднику необходимо изменить права доступа к отдельным файлам и папкам. Если администратор отсутствует, это может оказаться затруднительным. Ведь далеко не все пользователи имеют навыки работы в Free BSD или Linux системах. Для того чтобы организовать возможность настройки прав доступа к файлам и каталогам при помощи проводника Windows, можно использовать списки доступа ACL (Access Control Lists). Поддержка ACL реализована в большинстве актуальных версий Free BSD или Linux на уровне ядра – все, что необходимо, - это включить ее для выбранных файловых систем.

Нередко, помимо хранения и предоставления доступа к документам, файл-сервер выполняет и некоторые другие функции. Достаточно часто файловый сервер является и сервером печати, то есть организует возможность работать с принтерами для всех рабочих станций сети предприятия. В случае при обслуживании сервера с установленной операционной системы Free BSD используется система печати CUPS. Для упрощения процедуры настройки доступен веб-интерфейс.

Кроме того, именно на файл-сервер обычно ложится организация резервного копирования.

Собранные в одном месте данные, без которых работа предприятия в нормальном режиме попросту невозможна, очень уязвимы.

Причин повреждения данных может быть множество – это аппаратная неисправность, проблемы с электропитанием, воздействия вредоносного ПО или пожар, но все они могут принести предприятию значительные убытки. Для того чтобы предотвратить потерю данных, необходимо при выполнении регулярного обслуживания сервера делать резервные копии всех важных документов и хранить их в надежном, желательно удаленном от сервера месте.

Существует три основных типа серверов удалённого доступа:

– серверы удаленного управления
– серверы удаленных узлов
– и терминальные серверы

Серверы удаленных узлов выступают в роли маршрутизаторов, или шлюзов, выполняя лишь транспортный сервис, тем самым соединяя клиентов с центральной сетью. Обслуживание серверов происходит при использовании протоколов IP, IPX или NetBIOS.

Серверы удаленного управления помогают обеспечить транспортный сервис, а также способны запускать от имени клиента различные приложения на компьютерах, подсоединённых к центральной сети, на экране удаленного компьютера создают образ графической среды этого приложения. Как правило, серверы удалённого управления работают с системой Windows.

Терминальные серверы работают аналогично, но при использовании многотерминальных операционных систем, таких как Unix, VAX VMS, IBM VM.

Терминальный сервер обеспечивает клиентов вычислительными ресурсами: память, процессорное время и пр. С технической стороны вопроса терминальный сервер – это мощный компьютер высокой производительности, который способен обслужить одновременно несколько пользователей. Расположение терминального сервера для работы не имеет значения – он может находиться как в соседней комнате, так и в другой стране.

Доступ к серверу и обслуживание сервера обеспечивают специальные терминальные клиенты – программы, которые в течение работы воспроизводят данные по работе сервера.

Обслуживание сервера контроллера доменов Для того чтобы повысить эффективность любой ИТ-инфраструктуры, очень важно правильно выполнить все необходимые настройки на базе вашей операционной системы.

Качественная настройка и обслуживание сервера включает в себя:

- настройку всех основных служб для работы сети
- таких как контроллер домена
- сервер баз данных
- файл-сервер
- почтовый и прокси-серверы и т. д.

Сервер терминалов достаточно часто используется при совместной работе в программе 1С. Это позволяет не только значительно повысить производительность программного обеспечения 1С, но и обеспечить высокую надежность программы и возможный удаленный доступ к 1С через Интернет.

При необходимости в некоторой степени экономить интернет-траффик при полном контроле доступа в глобальную сеть в офисе хорошим решением становится установка интернет-шлюза и прокси-сервера и дальнейшее обслуживание северов этих типов. При настройке ограничения доступа в глобальную сеть Интернет появляется возможность намного эффективнее использовать рабочее время ваших сотрудников.

При установке важно убедиться в том, что сервер, на который устанавливается Active Directory, имеет специальный раздел с файловой системой NTFS. Также перед установкой важно убедиться в том, что служба DNS правильно настроена. Обратите внимание на то, что сервер может вести себя по-разному, что следует учитывать при обслуживании сервера, в зависимости от версии и выпуска установленной операционной системы, а также прав и разрешений учетной записи и настроек меню.

Какое же оборудование может понадобиться для установки сервера на предприятии?
К нему относятся:

- коммутаторы
- маршрутизаторы
- принт-серверы и прочее

А для того чтобы оборудование не выходило из строя, требуется своевременное обслуживание сервера.

Благодаря своевременному обслуживанию сервера появляется возможность значительно увеличить срок его службы, а также избежать его внезапного выхода из строя. Оперативно устранять ошибки в программной части сервера возможно даже при удаленном обслуживании сервера. Если вы являетесь владельцем малого или среднего бизнеса и используете на фирме небольшое

количество серверов, то чаще всего содержать в штате высококвалифицированного, а, следовательно, и высокооплачиваемого специалиста для настроек и обслуживания сервера довольно часто экономически нецелесообразно. Поэтому обслуживание серверов логичнее и более экономически выгодно поручить компании, которая специализируется по данному профилю.

Обслуживание серверов windows 2003 и windows 2008

Сегодня практически каждая компания старается оборудовать свой офис различными видами оргтехники, первое место среди которой занимает компьютер. Компьютеризировать офис – это всего лишь пол дела, надо научиться грамотно обслуживать дорогостоящую технику. Корректная настройка позволяет повысить эффективность деятельности хозяйствующего субъекта. Столь популярные на сегодняшний день автоматизированные системы и программные продукты, позволяющие облегчить ведение учета и контроля за теми или иными процессами. Но для их полноценного функционирования необходимо создание определенных условий, в частности это касается операционной системы и набора дополнительных программных модулей. На сегодняшний день многие компании для повышения эффективности ИТ-инфраструктуры устанавливают и настраивают сервера именно на базе операционной системы Windows Server.

Обслуживание компьютеров, обслуживание сервера windows 2003 или обслуживание сервера windows 2008 считается одной из важных расходных статей для любой компании. Обслуживание техники заключается не только в поддержке оборудования в рабочем состоянии, но и в эффективных методах борьбы с вредоносными программами, обновлении базы данных, переустановке операционной системы и пр.

Сегодня сервера – это надёжное обеспечение как на аппаратном, так и на программном уровне.

Однако не стоит забывать, что своевременное обслуживание сервера windows 2003 и обслуживание сервера windows 2008 позволит увеличить его работоспособность и значительно продлить срок службы. Обслуживание сервера windows 2003 и обслуживание сервера windows 2008 возможное в виде удаленного обслуживания указанных серверов позволит оперативно исправлять большое количество ошибок в программной части серверов.

Качественная настройка и обслуживание сервера windows 2008, windows 2003 подразумевает комплексную настройку основных служб для работы внутренней сети предприятия, т.е. подключение интернет-шлюза, файл-сервера, сервера баз данных, почтового сервера, DNS, DHCP, VPN и пр.

Данная система предназначена для серверного использования, в домашних условиях её применяют крайне редко. Конечно, при большом желании и грамотном обслуживании сервера windows 2003, вполне возможно использовать и на домашнем ПК эту операционную систему, но лучше для таких целей предназначены другие операционные системы.

Ещё одна операционная система от компании Microsoft, которая отлично подходит для использования на предприятии - Windows Server 2008.

Гибкая и надёжная операционная система Windows Server 2008 включает в свой состав новые технологии, к примеру, режим Server Core, командная оболочка Windows PowerShell и др.

Модернизированные сетевые технологии Windows Server 2008 повышают управляемость и доступность серверной инфраструктуры. Качественное и выгодное обслуживание сервера windows 2008 разрешает сэкономить время и значительно сократить затраты.

Если обслуживание сервера windows 2008 проводится качественно, то данная ОС позволяет реализовать заложенный в ней потенциал, существенно улучшая и расширяя возможности по администрированию, диагностике, управлению службами и сервисами.

Значительно повысить эффективность использования оборудования и улучшить доступность серверов помогает встроенная технология виртуализации Windows Server 2008. Кроме того, Windows Server 2008 считается самым защищённым из всех аналогичных продуктов. Повышенную безопасность операционной системе гарантируют защита сетевого доступа, контроллер домена только для чтения и федеративные службы управления правами. Обслуживание сервера windows 2008 на предприятии позволяет полностью обезопасить бизнес в целом.

Стоит отметить, что серверы Windows Server 2008 могут быть использованы в качестве терминального сервера в том случае, если это редакции Standard, Enterprise и Datacenter, содержащие службы Terminal Services. Обслуживание сервера windows 2008 подразумевает обеспечение каждого пользователя лицензией Windows CAL, а также отдельной клиентской лицензией на доступ к серверу терминалов.

Контрольные вопросы:

1. Понятие сервера.
2. Типы серверов.
3. ОС для серверов

Практическая работа № 3

ИЗУЧЕНИЕ УРОВНЕЙ УПРАВЛЕНИЯ МОДЕЛИ OSI

Цель работы: изучить методы коммутации**,** аппаратные и программные средства компьютерных сетей.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия.

Подготовка к работе: Используя имеющийся теоретический материал, изучить методы коммутации**,** аппаратные и программные средства компьютерных сетей. Ответить на контрольные вопросы.

Общие сведения:

Сетевая система конструируется по слоям или уровням. Каждый уровень выполняет определенный набор присущих ему функций. В результате объединения уровней образуется сетевая архитектура. Сетевая архитектура выделяет функции связи по определенным логическим группам — уровням, что в значительной степени упрощает стандартизацию. Главной чертой открытой сетевой архитектуры является то, что правила взаимодействия уровней не представляют закрытую информацию или собственность какой-либо организации, а открыты для всеобщего изучения и использования.

Каждый уровень имеет свои определенные правила и процедуры, которые называются протоколами. Протоколы регулируют активность в пределах уровня и характер взаимодействия между уровнями. Допускается взаимодействие как между соседними уровнями по вертикали в пределах одного сетевого устройства, так и между однотипными уровнями разных сетевых устройств. В результате этого происходит передача и преобразование данных между уровнями в пределах одного сетевого устройства и между различными сетевыми устройствами. Уровни независимы друг от друга в том смысле, что изменение одного уровня или его внутренних протоколов не влечет изменения протоколов в соседних уровнях.

Разделение на уровни очень удобно и позволяет следующее:

- упростить конструирование сети и структурировать ее функции;
- расширить набор приложений, ориентированных на пользователей сети;
- обеспечить наращивание сети в процессе ее развития.

Наибольшую популярность в мире получила открытая сетевая архитектура, использующая в своей основе эталонную модель взаимодействия открытых систем или ЭМВОС (Open Systems Interconnection/Reference Model), или кратко модель OSI (ВОС).

Эта семиуровневая модель была разработана в 1977 г. совместно ISO и CCITT (современное название ITU-T) и на сегодняшний день составляет основу для развития международных стандартов в области компьютерных коммуникаций, табл. 5.4 .

Таблица 5.4. Уровни модели OSI и их основные функции

Уровень (layer)	Назначение
1 Физический (Physical)	Ответственен за физические, электрические характеристики линии связи, между узлами (коаксиальные кабели; витые пары; волоконно-оптические кабели; разъемы, например RJ-45, AUI, DB-9, MIC, ST, SC; повторители; транн сиверы и т.д.).
2 Канальный (Data Unk)	Обеспечивает надежную передачу данных по физическим линиям связи. На этом уровне (эвена данных) происходит исправление ошибок передачи, ко^ дирование и декодирование отправляемых или принимаемых битовых последовательностей. Канальный уровень подразделяется на подуровень Medium Access Control (MAC) — Управление доступом к среде и на подуровень Logical Link Control (LLC) — Управление логическим каналом.
	Уровень MAC -определяет характер доступа к среде — детерминированный доступ с передачей маркера (Arcnet, Token Ring, FDDI, 100VG AnyLAN) или множественный доступ с распознаванием коллизий (Ethernet — IEEE 802.3). Уровень LLC -верхний подуровень -. посылает и получает сообщения с полезными данными.
3 Сетевой , (Network)	Обеспечивает для верхних уровней независимость от стандарта передачи данных (прозрачность), оперирует с такими протоколами, как IPX, TCP/IP и др., а также отвечает за адресацию и доставку сообщений.
4 Транспортный (Transport)	Управляет упорядочиванием компонентов сообщений и регулирует входящий поток, если на обработку приходит два или более пакетов одновременно. Дублированные пакеты распознаются этим уровнем и лишние дубликаты фильтруются.
5 Сессионный (Session)	Открывает соединение (сессию или сеанс), поддерживает диалог, т.е. управляет отправкой сообщений туда и обратно, и закрывает сессии. Этот уровень позволяет прикладным программам, работающим на разных сетевых устройствах, координировать свое взаимодействие в рамках отдельных сессий (сеансов).
6 Представительный (Presentation)	Осуществляет преобразования данных из внутреннего числового формата, присущего данному сетевому устройству, в стандартный коммуникационный формат. Примеры: кодирование, сжатие, переформатирование текста.
7 Прикладной (Application)	Предоставляет программисту интерфейс к модели OSi. Примеры: сервер транзакций, протокол FTP, сетевое администрирование.

Уровни с меньшим номером принято называть низкими уровнями, а уровни с большим Номером — высокими.

Стандарты IEEE 802

Сетевые протоколы и стандарты, охватывающие два нижних уровня модели OSI (физический и канальный) были разработаны комитетом IEEE 8802 (сокращенно IEEE 802). Получила распространение несколько различных вариантов построения этих уровней. Причем у канального уровня только его нижний подуровень — MAC (управление доступом к среде) — был выделен и объединен с физическим уровнем для организации сетевого стандарта. Таким образом, протоколы подуровня LLC (канального уровня) и более высоких уровней 3, 4 и т.д. остались независимыми от сетевых стандартов, Следует отметить, что стандарт FDDI, несмотря на то, что был разработан другой организацией, также включен в эту группу сетевых стандартов, так как он выполнен в полном соответствии с эталонной моделью OSI/IEEE 802.

Контрольные вопросы:

1. Уровни модели OSI.
2. Понятие протокола.
3. На что ориентированы протоколы 1-3 уровня в 7-ми уровневой модели OSI?
4. На что ориентированы протоколы 5-7 уровня в 7-ми уровневой модели OSI?
5. К каким уровням относится транспортный уровень?

Практическая работа № 4

МЕТОДЫ ПЕРЕДАЧИ ДАННЫХ

Цель работы: изучить методы коммутации**,** аппаратные и программные средства компьютерных сетей.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия

Общие сведения:

Типы адресов стека TCP/IP

В стеке **TCP/IP** используются **три типа адресов**:

1. **локальные** (называемые также аппаратными)
2. **IP-адреса**
3. **символьные доменные имена**

Локальные адреса

Локальный адрес в терминологии TCP/IP - это такой тип адреса, который используется средствами базовой технологии для доставки данных в пределах подсети, которая сама является элементом составной интерсети.

В разных подсетях допустимы разные сетевые технологии, разные стеки протоколов, поэтому при создании стека TCP/IP уже заранее предполагалось наличие разных типов локальных адресов.

Если подсетью интерсети является локальная сеть, то локальный адрес - это MAC - адрес.

MAC - адрес назначается сетевым адаптерам и сетевым интерфейсам маршрутизаторов.

MAC - адреса назначаются производителями оборудования и являются уникальными, так как управляются централизованно.

Для всех существующих технологий локальных сетей MAC - адрес имеет формат 6 байт, например 11-AO-17-3D-BC-01.

Надо отметить, что поскольку протокол IP может работать и над протоколами более высокого уровня. В этом случае локальными адресами для протокола IP соответственно будут адреса соответствующих протоколов более высокого уровня.

Следует учесть, что компьютер в локальной сети может иметь несколько локальных адресов даже при одном сетевом адаптере. И наоборот, некоторые сетевые устройства вообще не име-

ют локальных адресов. Например, к таким устройствам относятся глобальные порты маршрутизаторов, предназначенные для соединений типа "точка-точка".

IP-адреса - основной тип адресов сетевого уровня.

На основании IP-адресов сетевой уровень передает пакеты между сетями. IP-адреса состоят из 4 байт.

IP-адрес назначается администратором во время конфигурирования компьютеров и маршрутизаторов.

IP-адрес состоит из двух частей: номера сети и номера узла.

Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Internet Network Information Center, InterNIC) , если сеть должна работать как составная часть Internet. Обычно поставщики услуг Internet получают диапазоны адресов у подразделений InterNIC, а затем распределяют их между своими абонентами.

Номер узла в протоколе IP назначается независимо от локального адреса узла!

Маршрутизатор по определению входит сразу в несколько сетей. Поэтому каждый порт маршрутизатора имеет собственный IP-адрес.

Конечный узел также может входить в несколько IP-сетей. В этом случае компьютер должен иметь несколько IP-адресов, по числу сетевых связей.

Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение. Напоминаю, что мы поговорим об этом немного позже более подробно.

Символьные имена

Символьные имена имеют символьный вид и в IP-сетях называются доменными.

Доменные имена строятся по иерархическому признаку. Полное символьное имя в IP-сетях состоит из нескольких составляющих, которые разделяются точкой. Они перечисляются в следующем порядке (сдева-направо):

- сначала простое имя конечного узла
- затем имя группы узлов (например, имя организации)
- затем имя более крупной группы (поддомена)

И так до имени домена самого высокого уровня (например, домена объединяющего организации по географическому принципу: UA - Украина, RU - Россия, UK - Великобритания, SU - США)

Примеров доменного имени может служить имя base2.sales.zil.ru. Между доменным именем и IP-адресом узла нет никакого соответствия, поэтому необходимо использовать какие-то дополнительные таблицы или службы, чтобы узел интерсети однозначно мог определяться в сети, как по доменному имени, так и по IP-адресу.

IP адреса. Классы IP адресов

Самое первое, что надо сразу уяснить - IP-адреса назначаются не узлам составной сети. IP адреса назначаются сетевым интерфейсам узлов составной сети.

Очень многие (если не большинство) компьютеров в IP сети имеют единственный сетевой интерфейс (и как следствие один IP адрес). Но компьютеры и другие устройства могут иметь несколько (если не больше) сетевых интерфейсов - и каждый интерфейс будет иметь свой собственный IP адрес.

Так устройство с 6 активными интерфейсами (например, маршрутизатор) будет иметь 6 IP адресов - по одному на каждый интерфейс в каждой сети, к которой он подключен.

Итак, IP адрес определяет однозначно сеть и узел, который подключен к данной сети. IP адрес имеет длину 4 байта (8 бит), это дает в совокупности 32 бита доступной информации.

Для улучшения читабельности, IP адрес записывается в виде четырех чисел, разделенных точками:

например, 128.10.2.30 - десятичная форма представления адреса - 4 (десятичных) числа, разделенных (.) точками, а 10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса. 4-ре 8-ми разрядных числа (октета)

Так как каждое из четырех чисел - это десятичное представление 8-битного байта, то каждое число может принимать значения от 0 до 255 (что дает 256 уникальных значений - помните, ноль - это тоже величина).

Десятичная форма записи IP-адреса используется в основном при в операционных системах, как наиболее удобная при настройке.

Кроме двоичной формы, встречается шестнадцатеричная форма записи IP-адреса: C0.94.1.3

Для сведения: использование 32-разрядных двоичных чисел позволяет создавать 4 294 967 296 уникальных IP-адресов - более чем достаточно для любой частной интрасети (хотя сеть Internet скоро может начать испытывать нехватку уникальных адресов).

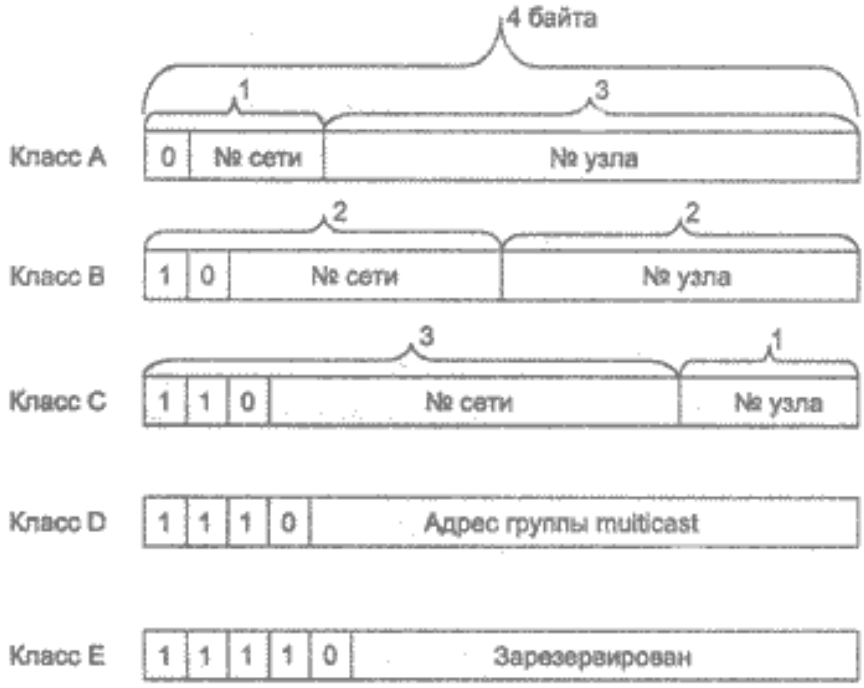
IP адрес состоит из двух логических частей - номера сети и номера узла в сети.

Конечно же, сразу возникает вопрос: а как определить в одном адресе, где номер сети, а где номер узла? Можно условится использовать, например, первые 8 бит адреса для номера сети, остальные для номеров узлов в той сети, или первые 16 бит, или первые 24 бита. Но в таком случае адресация получается абсолютно не гибкой, мы будем иметь или много маленьких сетей и мало больших, или наоборот.

Для того чтобы более рационально определиться с величиной сети и при том разграничить какая часть IP-адреса относится к номеру сети, а какая - к номеру узла условились использовать систему классов. Система классов использует значения первых бит адреса.

Но, таким образом, что значения этих первых бит адреса являются признаками того, к какому классу относится тот или иной IP-адрес.

Классы IP-адресов:



Итак, давайте в отдельной таблице приведем диапазоны номеров сетей и максимальное число узлов, соответствующих каждому классу сетей:

Класс	**Первые биты**	**Наименьший адрес сети**	**Наибольший адрес сети**	**Максимальное количество узлов**
A	**0**	1.0.0.0	126.0.0.0	2^{24} (16 777 216-2)
B	**10**	128.0.0.0	191.255.0.0	2^{16} (65536-2)
C	**110**	192.0.1.0	223.255.255.0	2^{8} (256-2)
D	**1110**	224.0.0.0	239.255.255.255	Multicast
E	**11110**	240.0.0.0	247.255.255.255	зарезервирован

Сети класса C являются наиболее распространенными.

- Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast.

Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес. Но об этом мы еще поговорим ниже.

- Если адрес начинается с последовательности 11110, то это значит, что данный адрес относится к классу E. Адреса этого класса зарезервированы для будущих применений.

Таким образом, можно однозначно определить, что:

Большие сети получают адреса класса A, средние - класса B, а маленькие - класса C. В зависимости от того к какому классу (A B C) принадлежит адрес, номер сети может быть представлен первыми 8, 16 или 24 разрядами, а номер хоста - последними 24, 16 или 8 разрядами.

Такова традиционная система классов, но и она не достаточно гибко определяет границы между номером сети и номером узла. С использованием классов границы проходят по границам байтов. Существует другой метод, который может проводить разделение границы между номером сети и номером узла в одном IP-адресе по границам битов! Но всему свое время, и прежде чем,

познакомится с этим способом, мы должны рассмотреть следующий, очень немаловажный момент, который касается "правил исключений" в IP - адресации.

Особые IP-адреса

Существуют некоторые значения IP-адресов, которые зарезервированы заранее, то есть существуют IP-адреса, которые предназначены для особых целей. Для каких?

1) Если весь IP-адрес состоит только из двоичных нулей, то он обозначает адрес того узла, который сгенерировал этот пакет;

0 0 0 0 ..... 0 0 0 0

этот режим используется только в некоторых сообщениях протокола межсетевых управляющих сообщений ICMP.

2) Если в поле номера сети стоят только нули, то по умолчанию считается, что узел назначения принадлежит той же самой сети, что и узел, который отправил пакет.

0 0 0 0 .....0 Номер узла

IP-адрес с нулевым номером хоста используется для адресации ко всей сети. Например, в сети класса С с номером 199.60.32 IP-адрес 199.60.32.0 обозначает сеть в целом.

3) Если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета.

1 1 1 1 .....1 1

Такая рассылка называется ограниченным широковещательным сообщением (limited broadcast) .

4) Если в поле номера узла назначения стоят только единицы, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером сети. Например, пакет с адресом 192.190.21.255 доставляется всем узлам сети 192.190.21.0.

Номер сети 1111.....11

Такая рассылка называется широковещательным сообщением (broadcast).

Предположим, например, что один из хостов в сети класса С с сетевым адресом 199.60.32.0 собирается направить сообщение всем остальным хостам, находящимся в той же сети. В этом случае сообщение должно быть передано на адрес 199.60.32.255.

При адресации хостов интерсети администратор должен обязательно учитывать все ограничения, которые вносятся особым назначением некоторых IP-адресов.

Таким образом, каждый администратор должен знать, что ни номер сети, ни номер узла не может состоять только из одних двоичных единиц или только из одних двоичных нулей. Отсюда следует, что максимальное количество узлов, приведенное в таблице для сетей каждого класса, на практике должно быть уменьшено на 2.

Особый смысл имеет IP-адрес, первый октет которого равен 127. Этот адрес зарезервирован для тестирования программ и взаимодействия процессов в пределах одной машины.

Когда программа посылает данные по IP-адресу 127.0.0.1, то образуется как бы "петля".

Данные не передаются по сети, а возвращаются модулям верхнего уровня, как только что принятые.

Поэтому в IP-сети запрещается присваивать машинам IP-адреса, начинающиеся со 127! Этот адрес имеет название loopback.

Можно отнести адрес 127.0.0.0 ко внутренней сети модуля маршрутизации узла, а адрес 127.0.0.1 - к адресу этого модуля на внутренней сети.

На самом деле любой адрес сети 127.0.0.0 служит для обозначения своего модуля маршрутизации, а не только 127.0.0.1, например 127.0.0.3.

В протоколе IP нет понятия широковещательности в том смысле, в котором оно используется в протоколах канального уровня локальных сетей, когда данные должны быть доставлены абсолютно всем узлам.

Как ограниченный широковещательный IP-адрес, так и широковещательный IP-адрес имеют свои пределы распространения в интерсети.

- они ограничены либо сетью, к которой принадлежит узел-источник пакета, либо сетью, номер которой указан в адресе назначения. Поэтому деление сети с помощью маршрутизаторов на части локализует широковещательный шторм пределами одной из составляющих общую сеть частей просто потому, что нет способа адресовать пакет одновременно всем узлам всех сетей составной сети.

Нами уже упоминалась выше в таблице форма группового IP-адреса - multicast. Так вот именно IP адрес multicast означает, что данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса.

Узлы сами идентифицируют себя, то есть определяют, к какой из групп они относятся. Один и тот же узел может входить в несколько групп. Члены какой-либо группы multicast не обязательно должны принадлежать одной сети. В общем случае они могут распределяться по совершенно различным сетям, находящимся друг от друга на произвольном количестве хопов.

Групповой адрес не делится на поля номера сети и узла и обрабатывается маршрутизатором особым образом.

Основное назначение multicast-адресов - распространение информации по схеме "один-комногим".

Она работает следующим образом: хост, который хочет передавать одну и ту же информацию многим абонентам, с помощью специального протокола IGMP (Internet Group Management Protocol) сообщает о создании в сети новой мультивещательной группы с определенным адресом.

Машрутизаторы, поддерживающие мультивещательность, распространяют информацию о создании новой группы в сетях, подключенных к портам этого маршрутизатора.

Хосты, которые хотят присоединиться к вновь создаваемой мультивещательной группе, сообщают об этом своим локальным маршрутизаторам и те передают эту информацию хосту, инициатору создания новой группы.

Чтобы маршрутизаторы могли автоматически распространять пакеты с адресом multicast по составной сети, необходимо использовать в конечных маршрутизаторах специальные модифицированные протоколы обмена маршрутной информацией.

В общем, групповая адресация была предназначена для экономичного распространения в Internet или большой корпоративной сети аудио- или видеопрограмм, предназначенных сразу большой аудитории слушателей или зрителей.

Надо сказать, что если такие средства найдут широкое применение (сейчас они представляют в основном небольшие экспериментальные островки в общем Internet), то Internet сможет создать серьезную конкуренцию радио и телевидению.

Ну что ж, давайте, сделаем итог, который закрепит наше представление о том, что означает IP-адрес:

IP адрес может означать одно из трех:

1. Адрес IP сети (группа IP устройств, имеющих доступ к общей среде передаче - например, все устройства в сегменте Ethernet). Сетевой адрес всегда имеет биты интерфейса (хоста) адресного пространства установленными в 0 (если сеть не разбита на подсети - как мы еще увидим);

2. Широковещательный адрес IP сети (адрес для 'разговора' со всеми устройствами в IP сети). Широковещательные адреса для сети всегда имеют хостовые биты адресного пространства установленными в 1 (если сеть не разбита на подсети - опять же, как мы вскоре увидим).

3. Адрес интерфейса (например Ethernet-адаптер или PPP интерфейс хоста, маршрутизатора, сервера печать итд). Эти адреса могут иметь любые значения хостовых битов, исключая все нули или все единицы - чтобы не путать с адресами сетей и широковещательными адресами.

Для сети класса A ...
(один байт под адрес сети, три байта под номер хоста)
10.0.0.0 сеть **класса A**, потому что **все хостовые биты равны 0**.
10.0.1.0 адрес хоста в этой сети
10.255.255.255 широковещательный адрес этой сети,
поскольку все сетевые биты установлены в **1**

Для сети класса B...
(два байта под адрес сети, два байта под номер хоста)
172.17.0.0 сеть **класса B**
172.17.0.1 адрес хоста в этой сети
172.17.255.255 сетевой широковещательный адрес

Для сети класса C...
(три байта под адрес сети, один байт под номер хоста)
192.168.3.0 адрес сети **класса C**
192.168.3.42 хостовый адрес в этой сеть
192.168.3.255 сетевой **широковещательный адрес**
Едва ли не все доступные сетевые **IP** адреса принадлежат **классу C**.

Маски в IP адресации

Итак, рассмотрена традиционная схема деления **IP-адреса** на **номер сети**, и **номер узла**, которая основана на понятии **класса**. **Класс** определяется значениями нескольких **первых бит адреса**. Теперь, например, можно определить, что поскольку первый байт адреса **185.23.44.206** попадает в диапазон **128-191**, то этот адрес относится к **классу B**, а значит, номером сети являются первые два байта, дополненные двумя нулевыми байтами - **185.23.0.0**, а номером узла - **0.0.44.206**.

Очевидно, что определение **номеров сети** по первым байтам адреса также не вполне гибкий механизм для адресации. А что если использовать какой-либо другой признак, с помощью которого можно было бы более **гибко** устанавливать границу между **номером сети** и **номером узла**?

В качестве такого признака сейчас получили широкое распространение **маски**.

Маска - это тоже **32-разрядное** число, она имеет такой же вид, как и **IP-адрес**. Маска **используется в паре с IP-адресом**, но не совпадает с ним.

Принцип отделения **номера сети** и **номера узла** сети с использованием **маски** состоит в следующем:

Двоичная запись маски содержит *единицы* в тех разрядах, которые в IP-адресе должны представляться как номер сети и *нули* в тех разрядах, которые представляются как номер хоста.

Каждый класс **IP-адресов** (**A, B и C**) имеет свою **маску**, используемую по умолчанию.

Поскольку **номер сети** является цельной частью адреса, **единицы в маске** также должны представлять непрерывную последовательность.

Таким образом, для стандартных **классов сетей маски** имеют следующие значения:

- **класс А - 11111111. 00000000. 00000000. 00000000 (255.0.0.0)** ;
- **класс В - 11111111. 11111111. 00000000. 00000000 (255.255.0.0)** ;
- **класс С - 11111111.11111111.11111111.00000000 (255.255.255.0)** .

Например:

Если адресу **185.23.44.206** назначить **маску 255.255.255.0**, то смотрим, что единицы в маске заданы в трех байтах, значит **номер сети** будет **185.23.44.0**, а не **185.23.0.0**, как это определено правилами системы классов.

Для записи **масок** используются и другие форматы, например, удобно интерпретировать значение **маски**, записанной в **шестнадцатеричном коде**:

FF.FF.00.00 - маска для адресов класса В.

Часто встречается и такое обозначение: IP-адрес/префикс сети. Например, **185.23.44.206/16** - эта запись говорит о том, что **маска** для этого адреса содержит **16 единиц** (префикс сети), или что в указанном **IP-адресе** под **номер сети** отведено **16** двоичных разрядов.

Нотация с префиксом сети также известна как бесклассовая междоменная маршрутизация (Classless Interdomain Routing - CIDR).

Таким образом, очень легко, снабжая каждый IP-адрес произвольной маской **(**не обязательно кратной 8**)**, отказаться от понятий **классов адресов** и тем самым сделать более гибкой систему IP адресации.

Рассмотрим пример: для IP-адреса **129.64.134.5** назначим **маску 255.255.128.0,** что в двоичном виде будет выглядеть так:

IP-адрес 129.64. 134.5 - 10000001.01000000.1 0000110.00000101
Маска 255.255.128.0 - 11111111.11111111.1 0000000.00000000

Здесь **17 последовательных единиц в маске**, "накладываются" на IP-адрес, и определяют номер сети : **10000001. 01000000. 10000000. 00000000** или **129.64.128.0**,

а номер узла **0000110.00000101** или **0.0.6.5**.

Механизм масок очень широко распространен в **IP-маршрутизации**, причем **маски** могут использоваться для самых разных целей. С их помощью администратор может структурировать свою сеть, **не требуя от поставщика услуг дополнительных номеров сетей!**

На основе этого же механизма поставщики услуг могут **объединять адресные пространства нескольких сетей** путем введения так называемых **"префиксов"** с целью уменьшения объема **таблиц маршрутизации**, и повышения за счет этого производительности маршрутизаторов. (Создание надсетей).

Маски при записи всегда "неразлучны" с соответствующими адресами, **IP-адрес маска подсети** - именно так теперь и мы будем описывать адрес любого хоста сети.

Порядок назначения IP адресов. Автономные IP адреса. Автоматизация назначения IP адресов

Номера сетей могут назначаться либо **централизованно**, если сеть является частью **Internet**, либо **произвольно**, если сеть работает **автономно**. **Номера узлов** и в том и в другом случае администратор назначает самостоятельно по своему усмотрению, не выходя, разумеется, из разрешенного для этого класса сети диапазона.

Главную роль в **централизованном распределении IP-адресов** до некоторого времени играла организация **InterNIC** (Network Information Center), однако с ростом сети задача распределения адресов стала слишком сложной. **InterNIC** делегировала часть своих функций другим организациям и крупным поставщикам услуг **Internet - провайдерам**. В частности распределением **IP-адресов** для подключения к сети Internet теперь занимаются **провайдеры**.

С тех пор, как появилась и стала широко распространяться сеть **Internet**, уже прошло не мало времени. И теперь уже становится актуальным вопрос о **дефиците IP-адресов**. Если говорить о реальной обстановке при распределении адресов для пользователей **Internet**, то сейчас очень трудно получить адрес **класса B** и уже практически невозможно стать обладателем адреса **класса A**! При этом всем надо сказать, что **дефицит IP-адресов** вызван не совсем постоянным ростом сетей, а просто нерациональным их использованием. Очень часто владельцы сети **класса C** расходуют лишь небольшую часть из имеющихся у них **254 адресов**.

Рассмотрим пример, когда две сети необходимо соединить глобальной связью.

В таких случаях в качестве канала связи используют два маршрутизатора, соединенных по схеме **"точка-точка"**.

В ситуации, которая приведена в примере, для вырожденной сети, образованной каналом, связывающим порты двух смежных маршрутизаторов, приходится выделять **отдельный номер сети**, хотя в этой сети имеются всего **2 узла**.

Давайте рассмотрим другую ситуацию: какие **IP-адреса** может использовать администратор, если провайдер услуг **Internet** не назначил ему никакого адреса? Если, к примеру, мы точно знаем, что сеть, которую мы администрируем никогда в будущем не будет подключаться к **Internet** (работает в **"автономном режиме"**), тогда мы можем использовать любые **IP-адреса**, соблюдая правила их назначения, о которых шла речь выше. Для простоты можно использовать адреса **класса C**: в этом случае не придется вычислять значение **маски** подсети и вычислять адрес для каждого хоста.

В этом случае мы должны будем просто назначить каждому сегменту нашей локальной сети его собственный сетевой номер **класса C**.

Если все сегменты нашей локальной сети имеют собственные сетевые номера **класса C**, то в каждом сегменте можно создать по **254** номера хостов.

Однако если у нас есть хотя бы небольшая вероятность того, что когда-либо в будущем наша сеть может быть подключена к Internet, не следует использовать такие IP-адреса! Они могут привести к конфликту с другими адресами в Internet. Чтобы избежать таких конфликтов, нужно использовать IP-адреса, **зарезервированные для частных сетей**.

Для этой цели зарезервированы специально несколько блоков **IP-адресов**, которые называются **автономными**.

Автономные IP адреса

Автономные адреса зарезервированы для использования **частными сетями**. Они обычно используются организациями, которые имеют свою частную большую сеть - **intranet** (локальные сети с архитектурой и логикой **Internet**), но и маленькие сети часто находят их полезными.

Эти адреса не обрабатываются маршрутизаторами Internet, ни при каких условиях. Эти адреса выбраны из разных классов.

Класс	От IP-адреса	До IP-адреса	Всего узлов адресов в диапазоне
A	10.0.0.0	10.255.255.255	16 777 216-2
B	172.16.0.0	172.31.255.255	65 536-2
C	192.168.0.0	192.168.255.255	256-2

Эти адреса являются зарезервированными для **частных сетей**. Таким образом, если в будущем мы решим все-таки подключить свою сеть к **Internet**, то даже если трафик с одного из хостов в нашей сети и попадет каким-либо образом в **Internet**, конфликта между адресами произойти не должно. Маршрутизаторы в **Internet** запрограммированы так, чтобы не транслировать сообщения, направляемые с зарезервированных адресов или на них.

Надо сказать, что использование **автономных** IP-адресов имеет и недостатки, которые состоят в том, что если мы будем подключать свою сеть к **Internet**, то нам придется заново настроить конфигурацию хостов, соединяемых с **Internet**.

Можно сказать, что **подсеть** - это метод, состоящий в том, чтобы взять **сетевой IP адрес** и **локально** разбить его так, чтобы этот **один сетевой IP адрес** мог в действительности **использоваться в нескольких взаимосвязанных локальных сетях**.

О**дин сетевой IP адрес может использоваться только для одной сети! Самое важное**: разбиение на **подсети** - это **локальная настройка**, она не видна "снаружи". Разбиение одной большой сети на **подсети**, значительно разгружает общий трафик и позволяет повысить безопасность всей сети в целом.

Алгоритм разбиения сети на **подсети**

1) Устанавливаем физические соединения (сетевые кабели и сетевые соединители - такие как маршрутизаторы);

2) Принимаем решение насколько большие/маленькие **подсети** вам нужны, исходя из количества устройств, которое будет подключено к ним, то есть, сколько **IP адресов** требуется использовать в каждом сегменте сети.

3) Вычисляем соответствующие **сетевые маски** и **сетевые адреса**;

4) Раздаем каждому интерфейсу в каждой сети свой **IP адрес** и соответствующую **сетевую маску**;

5) Настраиваем каждый маршрутизатор и все сетевые устройства;

6) Проверяем систему, исправляем ошибки.

Сейчас наша задача разобраться с тем, как выполнить 2-й и 3-й шаги.

Пример 1

Предположим, что мы хотим разбить нашу сеть на подсети, но имеем только один **IP-адрес сети 210.16.15.0**.

Решение:

IP-адрес 210.16.15.0 - это адрес **класса С**. Сеть **класса С** может иметь до **254** интерфейсов (хостов) плюс **адрес сети (210.16.15.0)** и **широковещательный адрес (210.16.15.255)**.

Первое: определить **"размер" подсети**.

Существует зависимость между количеством создаваемых **подсетей** и "потраченными" **IP адресами**.

Каждая отдельная **IP сеть** имеет **два адреса, неиспользуемые для интерфейсов (хостов)**:

- IP адрес собственно сети и широковещательный адрес.

При разбивке на подсети **каждая подсеть требует свой собственный уникальный IP адрес сети и широковещательный адрес** - и они должны быть корректно выбраны из диапазона адресов **IP сети**, которую мы делим на **подсети**.

Итак, если при разбивке **IP сети** на **подсети**, в каждой из которых есть **два сетевых адреса** и **два широковещательных адреса** - надо помнить, что каждая из них уменьшит количество используемых интерфейсных (хостовых) адресов на два.

Это мы должны всегда учитывать при вычислении **сетевых номеров**. Следующий шаг - **вычисление маски подсети и сетевых номеров**.

Сетевая маска - это то, что выполняет все логические манипуляции по разделению **IP сети на подсети**.

Для всех трех классов **IP сетей** существуют стандартные сетевые **маски**:

- **Класс А** (8 сетевых битов) : **255.0.0.0**
- **Класс В** (16 сетевых битов): **255.255.0.0**
- **Класс С** (24 сетевых бита): **255.255.255.0**

Чтобы создать **подсеть**, нужно изменить маску подсети для данного класса адресов.

Номер подсети можно задать, позаимствовав нужное для нумерации подсетей количество разрядов в номере хоста. Для этого берутся левые (старшие) разряды из номера хоста, в маске же взятые разряды заполняются единицами, чтобы показать, что эти разряды теперь нумеруют не узел а подсеть. Значения в остающихся разрядах маски подсети оставляются равными **нулю**; это означает, что оставшиеся разряды в номере хоста в **IP-адресе** должны использоваться как новый (меньший) номер хоста.

Например, чтобы **разбить сетевой адрес** на **две** подсети, мы должны позаимствовать **один хостовый бит**, установив **соответствующий бит в сетевой маске первого хостового бита в 1**.

Если нам нужно **четыре подсети** - используем **два хостовых бита**, если **восемь подсетей** - **три бита** и т.д. Однозначно, что если нам нужно **пять подсетей**, то мы будем использовать **три хостовых бита**. Соответствующим образом изменяется и **маска подсети**:

Для адресов **класса С**, при разбиении на **2 подсети** это дает **маску** -

11111111.11111111.11111111.10000000 или **255.255.255.128**

при разбиении на **4 подсети** маска в двоичном виде -

11111111.11111111.11111111.11000000, или в десятичном **255.255.255.192**. и т.д.

Для нашего адреса сети класса С **210.16.15.0**, можно определить следующих несколько способов разбивки на **подсети**: -

Число подсетей	Число хостов	Сетевая маска
2	126	255.255.255.128 (11111111.11111111.11111111.10000000)
4	62	255.255.255.192 (11111111.11111111.11111111.11000000)
8	30	255.255.255.224 (11111111.11111111.11111111.11100000)
16	14	255.255.255.240 (11111111.11111111.11111111.11110000)
32	6	255.255.255.248 (11111111.11111111.11111111.11111000)
64	2	255.255.255.252 (11111111.11111111.11111111.11111100)

Теперь нужно решить вопрос об **адресах сетей и широковещательных адресах,** и о диапазоне **IP адресов** для каждой из этих сетей.

Снова, принимая во внимание только сетевые адреса **класса С.** и показав только последнюю (хостовую) часть адресов, мы имеем:

Сетевая маска	Подсети	Сеть	Broadcast	MinIP	MaxIP	Хосты	Всего хостов
128	2	0	127	1	126	126	
		128	255	129	254	126	252
192	4	0	63	1	62	62	
		64	127	65	126	62	
		128	191	129	190	62	
		192	255	193	254	62	248
224	8	0	31	1	30	30	
		32	63	33	62	30	
		64	95	65	94	30	
		96	127	97	126	30	
		128	159	129	158	30	
		160	191	161	190	30	
		192	223	193	222	30	
		224	255	225	254	30	240

Из этой таблицы сразу можем увидеть, что увеличение количества подсетей сокращает общее количество доступных хостовых адресов. Теперь, вооруженные этой информацией, мы готовы назначать хостовые и сетевые IP адреса и сетевые маски.

Пример 2

Определим, сколько нужно подсетей для нашей сети **класса С**, чтобы разбить ее на подсети по **10 хостов** в каждой.

Решение:

Сеть **класса С** может обслуживать всего **254** хоста плюс адрес сети и широковещательный адрес.

Для адресации **10-ти** хостов **3-х** разрядов недостаточно, поэтому необходимо **4-е** разряда. Итак, из восьми возможных для класса **С**, нам нужно только **4** разряда для адресации **10** хостов, остальные можно использовать как сетевые для адресации **подсетей**. Мы уже знаем, что каждая подсеть уменьшает количество возможных хостовых адресов в два раза.

Для адресации **16 подсетей** необходимо использовать **4 разряда**. Итак, посчитаем теперь количество узлов в каждой из **16 подсетей**: 2^4 **- 2 = 14 хостов**. Это количество с запасом удовлетворяет условие задачи.

Вычислим **маску подсети**, в этом случае она имеет вид:

11111111.11111111.11111111.11110000 или

255.255.255.240

Мы должны будем указать эту маску при настройке конфигурации каждого хоста в нашей сети (независимо от того, в какой подсети находится хост).

Теперь, например, мы можем сказать, адрес **192.168.200.246** с маской **255.255.255.240** - означает номер сети **192.168.200.240** и номер узла **0.0.0.6**.

Пример 3

Теперь, для всех трех классов определим соответственно маски подсети, и максимальное количество узлов возможное в каждой из этих подсетей, если необходимо разбить соответственно сеть **класса А**, сеть **класса В**, сеть **класса С** на отдельные **4 подсети**.

Решение:

Для сети **класса А**:

Максимальное количество узлов **16 777 216**. Для адресации 4-х подсетей необходимо **2** разряда, значит остается **22 разряда** для адресации **хостов**. Таким образом, каждая из четырех подсетей способна обслуживать $2^{22} - 2 = 4\ 194\ 302$ хоста в каждой из подсетей.

Число подсетей	Число хостов	Сетевая маска
4	4 194 302	255.192.0.0 (11111111. 11000000.00000000.00000000)

Для сети **класса В**

Максимальное количество узлов - **65 536**. Для адресации **4-х** подсетей в сетевом адресе **класса В** также нужно использовать **2 разряда**, но теперь свободными остается **14 разрядов**. Таким образом, каждая из подсетей может обслуживать $2^{14} - 2 = 16\ 382$ хостов.

Число подсетей	Число хостов	Сетевая маска
4	16 382	255.255.192.0 (11111111.11111111. 11000000.00000000)

Пример с сетью **класса С** мы уже рассматривали. Итак, теперь самое главное уметь в **двоичном виде** читать **IP адреса**, а с помощью маски легко можно определить **номер сети** и **номер узла**. Вот теперь, можно сказать, теория заканчивается, для нашей работы очень важно "окрепнуть" в навыках работы с **IP адресами**, уметь разделять сети на **подсети**, вычислять **маски подсети**, и назначать возможные **адреса сетей**, и **адреса хостов** - это прямая обязанность сетевых администраторов.

Надо сказать, что назначение **IP-адресов** узлам сети даже при не очень большом размере сети представляет для администратора очень утомительную процедуру. Поэтому сразу вторым шагом в **IP адресации** разработчики решили автоматизировать этот процесс.

С этой целью был разработан протокол **Dynamic Host Configuration Protocol (DHCP)**, который освобождает администратора от этих проблем, **автоматизируя процесс назначения IP-адресов**.

DHCP может поддерживать способ **автоматического динамического распределения адресов**, а также **более простые способы ручного и автоматического статического назначения адресов**. **Протокол DHCP** работает в соответствии с моделью **клиент-сервер**.

Во время старта системы компьютер, являющийся **DHCP-клиентом**, посылает в сеть **широковещательный запрос** на получение **IP-адреса**. **DHCP - сервер** откликается и посылает сообщение-ответ, содержащее **IP-адрес**. Предполагается, что **DHCP-клиент и DHCP-сервер находятся в одной IP-сети**.

При **динамическом** распределении адресов **DHCP-сервер** выдает адрес клиенту на **ограниченное время**, оно называется **временем аренды (lease duration)** . Это дает возможность впоследствии повторно использовать этот **IP-адрес** для назначения **другому** компьютеру.

Основное преимущество DHCP - автоматизация рутинной работы администратора по конфигурированию стека TCP/IP на каждом компьютере. Иногда **динамическое** разделение адресов позволяет строить **IP-сеть**, количество узлов которой превышает количество имеющихся в распоряжении администратора **IP-адресов**.

В **ручной процедуре** назначения **статических адресов** активное участие принимает администратор, который предоставляет **DHCP - серверу** информацию о **соответствии IP-адресов физическим адресам** или другим идентификаторам клиентов. **DHCP-сервер**, пользуясь этой информацией, всегда выдает определенному клиенту назначенный администратором адрес.

При **автоматическом статическом** способе **DHCP-сервер** присваивает **IP-адрес** из **пула наличных IP-адресов** без вмешательства оператора. А границы **пула назначаемых адресов** задает администратор при конфигурировании **DHCP-сервера**.

Адрес дается клиенту из **пула** в **постоянное пользование**, то есть с **неограниченным сроком аренды**. Между **идентификатором клиента** и его **IP-адресом** по-прежнему, как и при **ручном** назначении, существует постоянное соответствие. Оно устанавливается в момент **первого** назначения **DHCP-сервером IP-адреса** клиенту. При всех последующих запросах сервер возвращает тот же самый **IP-адрес**.

DHCP обеспечивает надежный и простой способ конфигурации сети **TCP/IP**, **гарантируя отсутствие дублирования адресов за счет централизованного управления их распределением**.

Администратору в этом случае остается только управляет **процессом назначения адресов** с помощью параметра **"продолжительность аренды"**, которая определяет, как долго компьютер может использовать назначенный **IP-адрес**, перед тем как снова запросить его от **DHCP-сервера** в аренду.

Задания

1) **IP-адрес 190.235.130.N** (где N-номер варианта согласно таблице, данной ниже), сетевая маска **255.255.192.0**. Определите, **адрес сети** и **адрес узла.**

2) Определите **маски подсети** для случая разбиения сети с номером **192.0.0.0** на **32 подсети**.

3) Существует единая корпоративная сеть, количество узлов сети - **50 450**. Этой сети выделен адрес для выхода в **Internet 192.124.0.0**. Вы решили не требовать от провайдера дополнительных адресов и организовать **8** филиалов в этой сети. Спрашивается:

- Какое максимальное количество узлов может быть в каждом из филиалов? Вычислите **сетевые маски** и возможный диапазон **адресов хостов** для каждого из филиалов.

4) Вы являетесь администратором корпоративной сети из **6 подсетей**, в каждой подсети по 25 компьютеров. Необходимо используя один номер сети **класса С 192.168.10.0**, определить правильно ли выбран **размер подсети**, и назначить маски и возможные **IP-адреса** хостам сети.

5)Разделить IP-сеть на подсети в соответствии с вариантом из таблицы. Для каждой подсети указать широковещательный адрес.

Таблица 5.

Вариант	**Сеть**	**Подсети**
1.	192.168.16.0/24	5 подсетей с 100, 20, 10, 6 и 40 узлами
2.	194.45.27.0/24	5 подсетей с 34, 20, 62,10 и 40 узлами
3.	56.1.1.0/16	4 подсети с 65, 22, 10 и 30 узлами

4.	147.168.0.0/16	5 подсетей с 56, 16, 10 и 70 узлами
5.	193.68.61.0/24	5 подсетей с 100, 20, 10 и 40 узлами
6.	192.100.0.0/24	4 подсети с 80, 20, 12 и 20 узлами
7.	195.18.11.0/24	4 подсети с 110, 11, 10 и 40 узлами
8.	207.15.0.0/24	4 подсети с 28, 80, 10 и 40 узлами
9.	222.11.0.0/24	4 подсети с 110, 20, 10 и 50 узлами
10.	200.2.2.0/24	4 подсети с 100, 20, 10 и 40 узлами
11.	201.111.32.0/16	5 подсетей с 170, 590, 1500, 800 и 254 узлами
12.	128.200.1.0/16	5 подсетей с 115, 300, 200, 128 и 420 узлами
13.	53.11.0.0/16	5 подсетей с 165, 222, 128, 110 и 430 узлами
14.	146.77.0.0/16	5 подсетей с 550, 116, 200, 256 и 170 узлами
15.	194.54.45.0/24	4 подсети с 103, 39, 10 и 16 узлами
16.	142.51.0.0/16	4 подсети с 180, 120, 12 и 30 узлами
17.	43.0.0.0/16	4 подсети с 151, 211, 16 и 70 узлами

Контрольные вопросы:

1. Чем первичная сеть снабжает вторичные сети?
2. Что предоставляют пользователям системы электросвязи?
3. Какой уровень обеспечивает связь со средой передачи?
4. Какой уровень прокладывает путь через сеть?
5. Какой уровень обеспечивает обнаружение и исправление ошибок?
6. Какой уровень определяет процедуру представления передаваемой информации в нужную сетевую форму?

Практическая работа № 5

СТЕКИ ПРОТОКОЛОВ TCP/IP, IPX/SPX

Цель работы: изучить стеки протоколов.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия, ПК.

Подготовка к работе: Используя имеющийся теоретический материал, изучить стеки протоколов. Ответить на контрольные вопросы.

Общие сведения:

Так как стек TCP/IP был разработан до появления модели взаимодействия открытых систем ISO/OSI, то, хотя он также имеет многоуровневую структуру, соответствие уровней стека TCP/IP уровням модели OSI достаточно условно.

Структура протоколов TCP/IP приведена на рисунке . Протоколы TCP/IP делятся на 4 уровня.

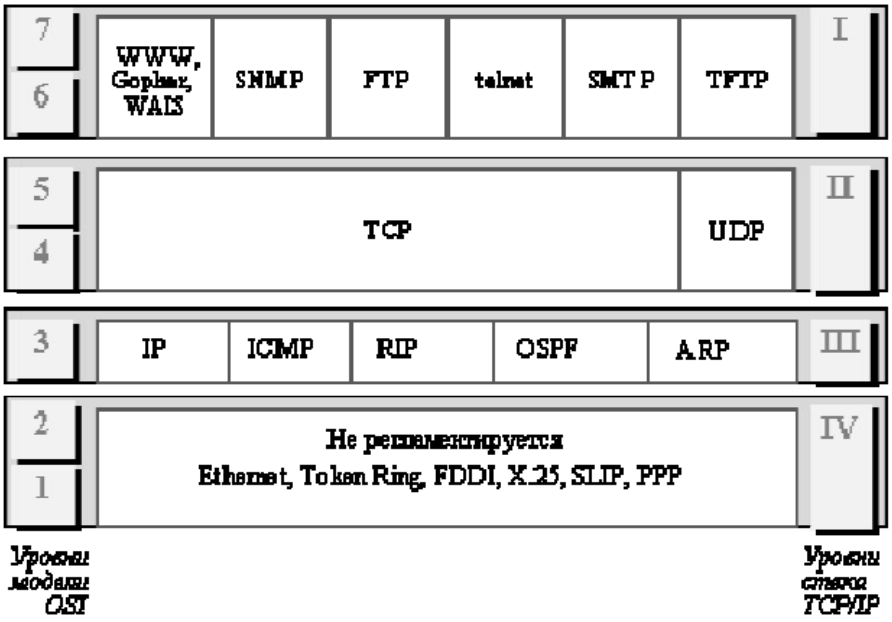


Рис. Стек TCP/IP

Диагностические утилиты TCP/IP.

В состав TCP/IP входят диагностические утилиты, предназначенные для проверки конфигурации стека и тестирования сетевого соединения.

Утилита	**Применение**
hostname	Выводит имя локального хоста. Используется без параметров.
ipconfig	Выводит значения для текущей конфигурации стека TCP/IP: IP-адрес, маску подсети, адрес шлюза по умолчанию, адреса WINS (Windows Internet Naming Service) и DNS (Domain Name System)
ping	Осуществляет проверку правильности конфигурирования TCP/IP и проверку связи с удаленным хостом.
tracert	Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP (Internet Control

	Message Protocol). Выводит маршрут прохождения пакетов на удаленный компьютер.
arp	Выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol - определяет локальный адрес по IP-адресу)
route	Модифицирует таблицы маршрутизации IP. Отображает содержимое таблицы, добавляет и удаляет маршруты IP.
netstat	Выводит статистику и текущую информацию по соединению TCP/IP.
nslookup	Осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов хостов, а также информации операционной системы, путем запросов к серверам DNS.
telnet	Осуществляет соединение с другим хостом по протоколу эмуляции терминала TELNET. Используется для проверки работоспособности сетевых служб, использующих tcp-порты (например, возможности соединения с почтовым сервером по протоколам POP3 и SMTP).

Задание:

Упражнение 1. Получение справочной информации.

Выведите на экран справочную информацию по всем рассмотренным утилитам Для этого в командной строке введите имя утилиты без параметров или с /?. Для получения справочной информации по nslookup необходимо войти в командный режим, набрав nslookup без параметров, и ввести команду help. Изучите ключи, используемые при запуске утилит.

Упражнение 2. Получение имени хоста.

Выведите на экран имя локального хоста с помощью команды hostname.

Упражнение 3. Изучение утилиты ipconfig.

Проверьте конфигурацию TCP/IP с помощью утилиты ipconfig. Заполните таблицу:

Имя хоста	
IP-адрес	
Маска подсети	
Основной шлюз	
Используется ли DHCP (адрес DHCP-сервера)	
Описание адаптера	
Физический адрес сетевого адаптера	

Контрольные вопросы:

1. Назначение протоколов
2. Работа протоколов: Компьютер – отправитель, Компьютер - получатель
3. Маршрутизируемые и немаршрутизируемые протоколы
4. Протоколы в многоуровневой архитектуре
5. Стеки протоколов
6. Привязка к сетевому адаптеру
7. Стандартные стеки протоколов: набор протоколов ISO/OSI; IBM System Network Architecture (SNA); Digital DECnet™; Novell NetWare; Apple AppleTalk®; набор протоколов Интернета, TCP/IP.
8. Прикладные протоколы
9. Транспортные протоколы
10. Сетевые протоколы
11. Транспортные протоколы
12. IEEE-протоколы физического уровня
13. Распространенные протоколы: TCP/IP, NetBEUI, X.25, IPX/SPX и NWLink, APPC, AppleTalk, Набор протоколов OSI, эмуляцию терминала, DECnet.
14. Прикладные протоколы
15. Транспортные протоколы
16. Сетевые протоколы

Практическая работа №6

НАСТРОЙКА СТЕКА ПРОТОКОЛОВ TCP/IP

Цель работы: Изучить способы диагностики настроек стека протоколов TCP/ IP; получить сведения о настройке TCP/IP.

Оборудование и программное обеспечение: методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия, ПК

Общие сведения:

1. Проверка правильности конфигурации TCP/IP с помощью ipconfig.

При устранении неисправностей и проблем в сети TCP/IP следует сначала проверить правильность конфигурации TCP/IP. Для этого используется утилита ipconfig.
Эта команда полезна на компьютерах, работающих с DHCP (Dynamic Host Configuration Protocol), так как дает пользователям возможность определить, какая конфигурация сети TCP/IP и какие величины были установлены с помощью DHCP.

Синтаксис:

ipconfig [/all | /renew[adapter] | /release]

Параметры:

all выдает весь список параметров. Без этого ключа отображается только IP-адрес, маска и шлюз по умолчанию;

renew[adapter] обновляет параметры конфигурации DHCP для указанного сетевого адаптера;

release[adapter] освобождает выделенный DHCP IP-адрес;

adapter – имя сетевого адаптера;

displaydns выводит информацию о содержимом локального кэша клиента DNS, используемого для разрешения доменных имен.

Таким образом, утилита ipconfig позволяет выяснить, инициализирована ли конфигурация и не дублируются ли IP-адреса:

- если конфигурация инициализирована, то появляется IP-адрес, маска, шлюз;
- если IP-адреса дублируются, то маска сети будет 0.0.0.0;
- если при использовании DHCP компьютер не смог получить IP-адрес, то он будет равен 0.0.0.0 .

2.Тестирование связи с использованием утилиты ping.

Утилита ping (Packet Internet Grouper) используется для проверки конфигурирования TCP/IP и диагностики ошибок соединения. Она определяет доступность и функционирование конкретного хоста. Использование ping лучший способ проверки того, что между локальным компьютером и сетевым хостом существует маршрут. Хостом называется любое сетевое устройство (компьютер, маршрутизатор), обменивающееся информацией с другими сетевыми устройствами по TCP/IP.
Команда ping проверяет соединение с удаленным хостом путем посылки к этому хосту эхо- пакетов ICMP и прослушивания эхо-ответов. Ping ожидает каждый посланный пакет и печатает количество переданных и принятых пакетов. Каждый принятый пакет проверяется в соответствии с

переданным сообщением. Если связь между хостами плохая, из сообщений ping станет ясно, сколько пакетов потеряно.

По умолчанию передается 4 эхо-пакета длиной 32 байта (возможны и другие варианты значения по умолчанию) - периодическая последовательность символов алфавита в верхнем регистре. Ping позволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использует, какую величину времени жизни (ttl) устанавливать, можно ли фрагментировать пакет и т.д.. При получении ответа в поле time указывается, за какое время (в миллисекундах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как значение по умолчанию для ожидания отклика равно 1 секунде, то все значения данного поля будут меньше 1000 миллисекунд. Если вы получаете сообщение «Request time out» (Превышен интервал ожидания), то, возможно, если увеличить время ожидания отклика, пакет дойдет до удаленного хоста. Это можно сделать с помощью ключа –w.

Ping можно использовать для тестирования как имени хоста (DNS или NetBIOS), так и его IP-адреса. Если ping с IP-адресом выполнилась успешно, а с именем – неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

Утилита ping используется следующими способами:

1) Для проверки того, что TCP/IP установлен и правильно сконфигурирован на локальном компьютере, в команде ping задается адрес петли обратной связи (loopback address): ping 127.0.0.1

Если тест успешно пройден, то вы получите следующий ответ:

Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128

Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128

Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128

Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128

2) Чтобы убедиться в том, что компьютер правильно добавлен в сеть и IP-адрес не дублируется, используется IP-адрес локального компьютера:

ping IP-адрес_локального_хоста

3) Чтобы проверить, что шлюз по умолчанию функционирует и что можно установить соединение с любым локальным хостом в локальной сети, задается IP-адрес шлюза по умолчанию:

4) Для проверки возможности установления соединения через маршрутизатор в команде ping задается IP-адрес удаленного хоста:

ping IP-адрес_удаленного хоста

Синтаксис:

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j host-list] |

[-k host-list]] [-w timeout] destination-list

Параметры:

-t выполняет команду ping до прерывания. Control-Break - посмотреть статистику и продолжить. Control-C - прервать выполнение команды;

-a позволяет определить доменное имя удаленного компьютера по его IP-адресу;

-n count посылает количество пакетов ECHO, указанное параметром count;

-l length посылает пакеты длиной length байт (максимальная длина 8192 байта);

-f посылает пакет с установленным флагом «не фрагментировать». Этот пакет не будет фрагментироваться на маршрутизаторах по пути своего следования;

-i ttl устанавливает время жизни пакета в величину ttl (каждый маршрутизатор уменьшает ttl на единицу);

-v tos устанавливает тип поля «сервис» в величину tos;

-r count записывает путь выходящего пакета и возвращающегося пакета в поле записи пути. Count - от 1 до 9 хостов;

-s count позволяет ограничить количество переходов из одной подсети в другую (хопов). Count задает максимально возможное количество хопов;

-j host-list направляет пакеты с помощью списка хостов, определенного параметром host-list. Последовательные хосты могут быть отделены промежуточными маршрутизаторами (гибкая статическая маршрутизация). Максимальное количество хостов в списке, позволенное IP, равно 9;

-k host-list направляет пакеты через список хостов, определенный в host-list. Последовательные хосты не могут быть разделены промежуточными

В случае невозможности проверить доступность хоста утилита выводит информацию об ошибке. Ниже приведен пример ответа утилиты ping при попытке послать запрос на несуществующий хост.

3. Изучение маршрута между сетевыми соединениями с помощью утилиты *tracert*.

Tracert - это утилита трассировки маршрута. Она использует поле TTL (time-to-live, время жизни) пакета IP и сообщения об ошибках ICMP для определения маршрута от одного хоста до другого.

Утилита tracert может быть более содержательной и удобной, чем ping, особенно в тех случаях, когда удаленный хост недостижим. С помощью нее можно определить район проблем со связью (у Internet-провайдера, в опорной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран звездочки (*), либо сообщения типа «Destination net unreachable», «Destination host unreachable», «Request time out», «Time Exeeded».

Утилита tracert работает следующим образом: посылается по 3 пробных эхо-пакета на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет (Его можно изменить с помощью параметра - w). Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает величину TTL на единицу.

Таким образом, время жизни является счетчиком точек промежуточной доставки (хопов). Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер- источник сообщение ICMP “Time Exeeded” (Время истекло). Маршрут определяется путем посылки первого эхо-пакета с TTL=1. Затем TTL увеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо будет достигнута максимально возможная величина TTL (по умолчанию 30, задается с помощью параметра -h).
Маршрут определяется путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами.

Синтаксис:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] имя_целевого_хоста

Параметры:

-d	указывает, что не нужно распознавать адреса для имен хостов;
-h maximum_hops	указывает максимальное число хопов для того, чтобы искать цель;
-j host-list	указывает нежесткую статическую маршрутизацию в соответствии с host-list;
-w timeout	указывает, что нужно ожидать ответ на каждый эхо-пакет заданное число мсек.

Задание:

Упражнение 1. Тестирование связи с помощью утилиты ping.

1. Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.
2. Проверьте, правильно ли добавлен в сеть локальный компьютер и не дублируется ли IP-адрес.
3. Проверьте функционирование шлюза по умолчанию, послав 5 эхо-пакетов длиной 64 байта.
4. Проверьте возможность установления соединения с удаленным хостом.
5. С помощью команды ping проверьте перечисленные ниже адреса и для каждого из них отметьте время отклика. Попробуйте изменить параметры команды ping таким образом, чтобы увеличилось время отклика. Определите IP-адреса узлов.
   a) stg-m.ru
   b) router.auditory.ru
   c) любой узел из локальной сети

Упражнение 2. Определение пути IP-пакета.

С помощью команды tracert проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Время жизни установить равным 10. Отметьте их:

a) 195.82.146.114
b) yandex.ru
c) 213.247.189.211

Упражнение 3: Просмотр ARP-кэша.

С помощью утилиты arp просмотрите ARP-таблицу локального компьютера. Внести в кэш локального компьютера любую статическую запись.

Упражнение 4: Просмотр локальной таблицы маршрутизации.
С помощью утилиты route просмотреть локальную таблицу маршрутизации.

Упражнение 5. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.
С помощью утилиты netstat выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

Контрольные вопросы:

1. Раскрыть термины: хост, шлюз, хоп, время жизни пакета, маршрут, маска сети.
2. Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?
3. Каким образом команда ping проверяет соединение с удаленным хостом?
4. Сколько промежуточных маршрутизаторов сможет пройти IP пакет, если его время жизни равно 30?
5. Как работает утилита tracert?
6. Каково назначение протокола ARP?
7. Как утилита ping разрешает имена узлов в IP-адреса .
8. Какие могут быть причины неудачного завершения ping и tracert?

Практическая работа №7

ИЗУЧЕНИЕ СЕТЕВОГО АДАПТЕРА

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

Оборудование и программное обеспечение: методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия, ПК, подключенный к локальной вычислительной сети (ЛВС), сетевой адаптер.

Общие сведения:

Сетевой адаптер (сетевая карта) — периферийное устройство, позволяющее компьютеру взаимодействовать с другими устройствами сети. Сетевые адаптеры
работают на втором уровне модели OSI. Адаптеры различаются по типу интеграции с компьютером (PCI, USB, PCMCIA, встроенные), по виду используемой среды передачи данных (витая пара, оптоволокно), а также по поддерживаемым технологиям (Ethernet 10Mbit/100Mbit/1Gbit).
Совместно со своим драйвером, сетевая карта реализует на конечном узле
(компьютере) физический и канальный уровень модели OSI, причем подуровень
LLC (Logical Link Control. Каковы его функции?) реализуется как правило
средствами операционной системы. В задачи сетевого адаптера в совокупности
с драйвером входит прием и отправка кадров в сеть.

Операция передачи данных обычно состоит из следующих этапов:

1. Прием LLC кадра
2. Оформление MAC-кадра
3. Кодирование с избыточностью и скремблирование
4. Выдача сигналов в кабель с помощью линейных кодов (Манчестер, NRZI и.т.п.)

Прием кадра из сети фактически повторяет данную последовательность, но в
обратном порядке.

1. Прием сигналов
2. Выделение сигналов на фоне шума и дескремблирование
3. Подсчет контрольной суммы кадра. Если контрольная сумма неверна, то кадр отбрасывается и происходит отправка LLC сообщения с кодом ошибки.

В соответствие с периодами функционального развития сетевых адаптеров, производят их разделение на 4 поколения. Сейчас используются адаптеры четвертого поколения, которые характеризуются высокой скоростью передачи данных (Gigabit Ethernet), собственным процессором для обработки кадров, а так же реализацией большого числа высокоуровневых функций (например, удаленного мониторинга).

Настройка параметров сетевого адаптера

Настройка параметров сетевого адаптера в операционной системе Linux производится с помощью консольных утилит ifconfig, ethtool и mii-tool.

Вывод общей информации о настройках сетевого адаптера производится с
помощью команды

ethtool eth0

Где eth0 — символьное имя сетевого интерфейса в операционной системе (полный список интерфейсов доступен с помощью команды ifconfig -a).
Получить информацию об используемом драйвере можно с помощью команды ethtool -i <имя_интерфейса>
Перед изменением какого-либо из параметров адаптера рекомендуется
отключать его командой ifconfig <имя_интерфейса> down.
После изменения нового параметра адаптер следует включить командой
ifconfig <имя_интерфейса> up
7
Settings for eth0:
Supported ports: [TP]
Supported link modes: 10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
1000baseT/Full
Supports auto-negotiation: Yes
Advertised link modes: 10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
1000baseT/Full
Advertised pause frame use: No
Advertised auto-negotiation: Yes
Speed: 100Mb/s
Duplex: Full
Port: Twisted Pair
PHYAD: 2
Transceiver: internal
Auto-negotiation: on
MDI-X: off
Supports Wake-on: pumbag
Wake-on: d
Current message level: 0x00000001 (1)
drv
Link detected: yes
Листинг 1: Вывод информации о сетевом адаптере командой ethtool
8
Значения некоторых полей вывода представлено в следующей таблице.
Параметр Значение
Supported link modes Поддерживаемые режимы связи
Supported auto-negotiation Поддержка режима авто-согласования
Speed Текущая скорость приема/передачи
Duplex Режим двухстороннего обмена
Transceiver Тип передатчика
Auto-negotiation Состояние режима авто-согласования
Link detected Состояние соединения
Таблица 3: Значения параметров вывода ethtool
Режим авто-согласования

Режим авто-согласования предполагает, что сетевое устройство само определяет присутствует ли двусторонний обмен и сколько мегабит он составляет, поэтому при установке собственных параметров сетевого адаптера, отличных от стандартных (определенных в ходе авто-согласования) следует отключать данный режим.

Существует два режима двухстороннего обмена:

- Дуплекс (полный) — устройства принимают и передают данные по двум разделенным физически каналам. Из этого следует отсутствие коллизий.
- Половинный (полу-дуплекс) — устройства в каждый момент времени могут либо передавать либо только принимать данные. Принимающее данные устройство не может при этом ничего передавать вынуждено дожидаться окончания приема.

Изменить режим двухстороннего обмена можно командой

ethtool -s <имя_интерфейса> duplex <half|full> autoneg off

Чтобы получить подробную статистику по интерфейсу воспользуйтесь

Командой ethtool -S <имя_интерфейса>

Информацию о прочих параметрах команды ethtool можно получить с

помощью утилиты man.

Задание:

1. Получить информацию о драйвере сетевого адаптера, скорости соединения и режиме двухстороннего обмена.

Изучение сетевой карты, вынутой из ПК.

Сетевая карта – плата, устройство, устанавливается в материнскую плату (рис. 1.1). Другое название сетевой карты – сетевой адаптер. Сетевая карта служит для соединения компьютера с другими компьютерами по локальной сети или для подключения к сети Интернет. Современные материнские платы имеют встроенную сетевую карту.

Рис. 1.1 Сетевая карта на чипе Realtek

Выбор производителя сетевой карты важен по следующим параметрам:

- надежность работы
- поддержка драйверами
- скорость

Когда речь идет о построении надежной и быстрой сети с богатыми возможностями мониторинга и управления, лидерами являются компании Intel и 3Com. Параметры сетевых карт определяются используемыми в них чипами. В современных картах обычно есть один большой чип, выполняющий функции контроллера шины и собственно сети. Среди других микросхем карты - приемопередатчик, энергонезависимая память, возможно ПЗУ для удаленной загрузки. Производителей чипов сетевых контроллеров гораздо меньше, чем производителей сетевых карт. При этом

одни практически монополизируют выпуск карт на своих чипах (3Com, Intel), а другие (Realtek, Via) занимаются исключительно выпуском микросхем и их продажей.

1.Осмотрите сетевую карту, вынутую из ПК. Определите тип шины (интерфейс), к которой она подключается. Для этого посмотрите на ту часть сетевой карты, которая имеет контакты. Если длина этой стороны менее 10 см, то карта подключается к шине PCI.

Кроме типа интерфейса у сетевых карт есть несколько других, менее важных параметров:

- поддержка Boot ROM (загрузка ПК без жесткого диска по сети)
- поддержка Wake On Lan (включение ПК по сети)
- поддержка режима Full Duplex (одновременные прием и передача информации, требуют поддержки этого режима от всего остального оборудования сегмента сети)
- количество индикаторов на задней панели

2. Определите тип физической среды (кабеля), с которой работает сетевая карта. Посмотрите на металлическую пластину, к которой крепится карта. Круглый коннектор свидетельствует о том, что эта карта для коаксиального кабеля; разъем RJ-45 – для работы с витой парой. Найдите в Интернет ответ на вопрос о коннекторе для оптического кабеля самостоятельно.

Изучение сетевой карты, вставленной в ПК

В Windows XP выполните команду Пуск-Панель управления-Система-Оборудование-Диспетчер устройств и раскройте список Сетевые платы (рис. 1.2).

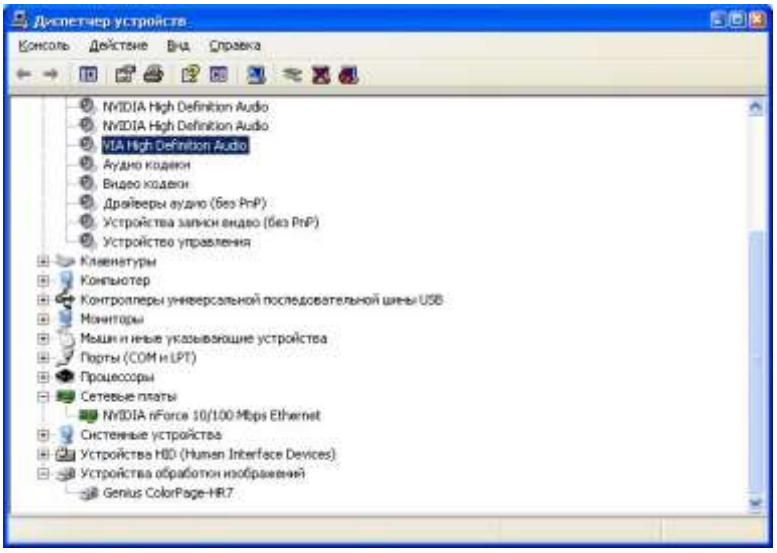


Рис. 1.2. В ПК установлена только одна сетевая плата

В Windows 7 выполните команду Пуск-Панель управления-Оборудование и звук-Диспетчер устройств и раскройте список Сетевые адаптеры (рис. 1.3).

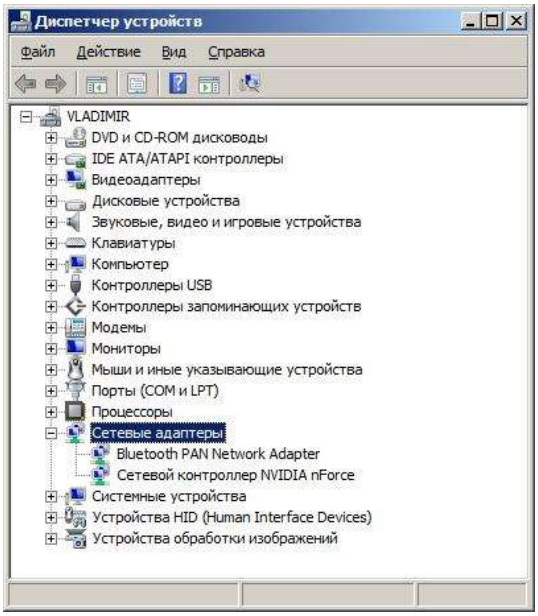


Рис. 1.3. В ПК установлено два сетевых адаптера

Примечание

Если у вас на сетевой плате нет желтых восклицательных знаков и красных крестиков, то ее драйвер установлен и работает корректно. Если напротив сетевого адаптера отображен восклицательный знак на фоне желтого круга, то драйвер конфликтует с другим устройством. Если напротив сетевой карты появился красный крестик, то драйвера вообще нет и его следует искать и устанавливать.

Определите физический (MAC) адрес адаптера. Для этого в Windows XP (или Windows 7) выполните команду Пуск-Все программы-Стандартные-Командная строка и введите команду ipconfig/all. Выведенный командой результат выглядит примерно так (рис. 1.4).

Рис. 1.4. Физический адрес и есть MAC-адрес сетевого адаптера

2. Переключить сетевой адаптер в режим half-duplex, загрузить предложенный тестовый файл и вывести статистику. Далее, переключить адаптер в режим full-duplex, загрузить тот же файл, вывести статистику. Сравнить полученные значения, а так же скорость загрузки файла.

3. Используя справку по утилите ethtool для получения соответствующих параметров команд проведите:

a) Online тестирование сетевого адаптера.

b) Получите информацию о параметрах управления высокой нагрузкой

(offload) сетевого адаптера. Попробуйте самостоятельно описать
каждый из параметров.
c) Выведите дамп состояния регистров сетевого устройства. Насколько полезной может быть полученная информация?

Контрольные вопросы:

1. Для чего служат сетевые адаптеры?
2. Перечислите основные функции СА.
3. На каких уровнях модели OSI работают СА?
4. По каким признакам могут различаться сетевые адаптеры?
5. Как можно определить тип шины (интерфейс) адаптера?
6. Как определить физический (MAC) адрес адаптера?

Практическая работа №8

СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА БАЗОВЫХ ТЕХНОЛОГИЙ ЛОКАЛЬНЫХ СЕТЕЙ

Цель работы: научиться сравнивать базовые технологии.

Оборудование и программное обеспечение: методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия, ПК

Общие сведения:

Программные продукты Packet Tracer дают возможность создавать сетевые топологии из широкого спектра маршрутизаторов и коммутаторов компании Cisco, рабочих станций и сетевых соединений типа Ethernet, Serial, ISDN, Frame Relay. Эта функция может быть выполнена как для обучения, так и для работы. Например, чтобы сделать настройку сети ещё на этапе планирования или чтобы создать копию рабочей сети с целью устранения неисправности.

Для запуска Cisco Packet Tracer необходимо вызвать исполняемый файл, PacketTracer52.exe. Общий вид программы можно увидеть на рис.4.1.

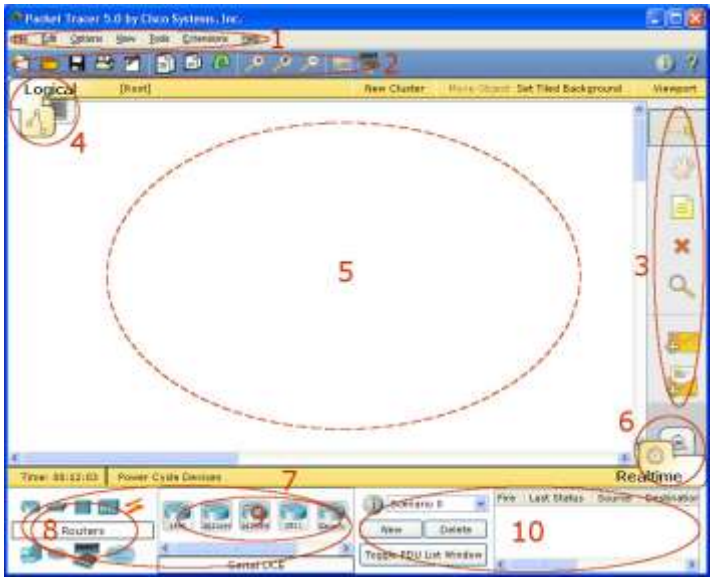


Рис.4.1. Общий вид программы Packet Tracer.

Рабочая область окна программы состоит из следующих элементов:

1. Menu Bar - Панель, которая содержит меню File, Edit, Options, View, Tools, Extensions, Help.
2. Main Tool Bar содержит графические изображения ярлыков для доступа к командам меню File, Edit, View и Tools, а также кнопку Network Information.
3. Common Tools Bar - Панель, которая обеспечивает доступ к наиболее используемым инструментам программы: Select, Move Layout, Place Note, Delete, Inspect, Add Simple PDU и Add Complex PDU.
4. Logical/Physical Workspace and Navigation Bar - Панель, которая дает возможность переключать рабочую область: физическую или логическую, а также позволяет перемещаться между уровнями кластера.
5. Workspace - Область, в которой происходит создание сети, проводятся наблюдения за симуляцией и просматривается разная информация и статистика.

6. Realtime/Simulation Bar - С помощью закладок этой панели можно переключаться между режимом Realtime и режимом Simulation. Она также содержит кнопки, относящиеся к Power Cycle Devices, кнопки Play Control и переключатель Event List в режиме Simulation.

7. Network Component Box - Это область, в которой выбираются устройства и связи для размещения их на рабочем пространстве. Она содержит область Device-Type Selection и область Device-Specific Selection.

8. Device-Type Selection Box - Эта область содержит доступные типы устройств и связей в Packet Tracer. Область Device-Specific Selection изменяется в зависимости от выбранного устройства

9. Device-Specific Selection Box - Эта область используется для выбора конкретных устройств и соединений, необходимых для постройки в рабочем пространстве сети.

10. User Created Packet Window - Это окно управляет пакетами, которые были созданы в сети во время симуляции сценария.

Для создания топологии необходимо выбрать устройство из панели Network Component, а затем из панели Device-Type Selection выбрать тип выбранного устройства. После этого нужно нажать левую кнопку мыши в поле рабочей области программы (Workspace). Также можно переместить устройство прямо из области Device-Type Selection, но при этом будет выбрана модель устройства по умолчанию.

Для быстрого создания нескольких экземпляров одного и того же устройства нужно, удерживая кнопку Ctrl, нажать на устройство в области Device-Specific Selection и отпустить кнопку Ctrl. После этого можно несколько раз нажать на рабочей области для добавления копий устройства.

В Packet Tracer представлены следующие типы устройств:

- Маршрутизаторы;
- Коммутаторы (в том числе и мосты);
- Хабы и повторители;
- Конечные устройства – ПК, серверы, принтеры, IP-телефоны;
- Беспроводные устройства: точки доступа и беспроводной маршрутизатор;
- Остальные устройства – облако, DSL-модем и кабельный модем.

Добавим необходимые элементы в рабочую область программы так, как показано на рис.4.2.

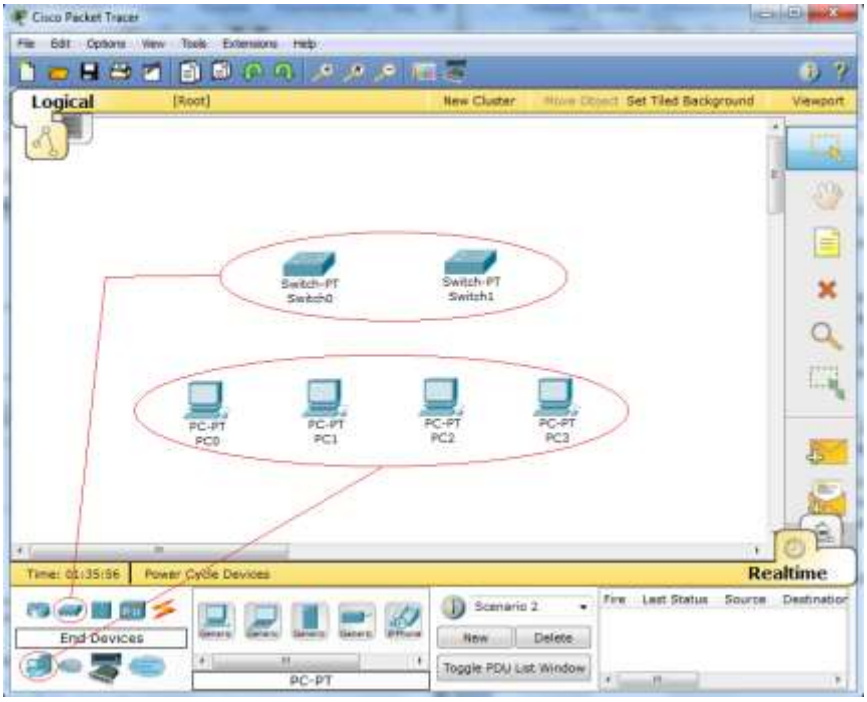


Рис.4.2. Добавление элементов сети.

При добавлении каждого элемента пользователь имеет возможность дать ему имя и установить необходимые параметры. Для этого необходимо нажать на нужный элемент левой кнопкой мыши (ЛКМ) и в диалоговом окне устройства перейти к вкладке Config.

Диалоговое окно свойств каждого элемента имеет две вкладки:

- Physical – содержит графический интерфейс устройства и позволяет симулировать работу с ним на физическом уровне.
- Config – содержит все необходимые параметры для настройки устройства и имеет удобный для этого интерфейс.

Также в зависимости от устройства, свойства могут иметь дополнительную вкладку для управления работой выбранного элемента: Desktop (если выбрано конечное устройство) или CLI (если выбран маршрутизатор) и т.д.

Для удаления ненужных устройств с рабочей области программы используется кнопка Delete (Del).

Свяжем добавленные элементы мы с помощью соединительных связей. Для этого необходимо выбрать вкладку Connections из панели Network Component Box. Мы увидим все возможные типы соединений между устройствами. Выберем подходящий тип кабеля. Указатель мыши изменится на курсор “connection” (имеет вид разъема). Нажмем на первом устройстве и выберем соответствующий интерфейс, с которым нужно выполнить соединение, а затем нажмем на второе устройство, выполнив ту же операцию. Можно также соединить с помощью Automatically Choose Connection Type (автоматически соединяет элементы в сети). Выберем и нажмем на каждом из устройств, которые нужно соединить. Между устройствами появится кабельное соединение, а индикаторы на каждом конце покажут статус соединения (для интерфейсов которые имеют индикатор).

Рис. 4.3. Поддерживаемые в Packet Tracer типы кабелей.

Packet Tracer поддерживает широкий диапазон сетевых соединений (см. табл. 1). Каждый тип кабеля может быть соединен лишь с определенными типами интерфейсов.

Типы соединений в Packet Tracer Таблица 1.

Тип кабеля	Описание
 Console	Консольное соединение может быть выполнено между ПК и маршрутизаторами или коммутаторами. Должны быть выполнены некоторые требования для работы консольного сеанса с ПК: скорость соединения с обеих сторон должна быть одинаковая, должно быть 7 бит данных (или 8 бит) для обеих сторон, контроль четности должен быть одинаковый, должно быть 1 или 2 стоповых бита (но они не обязательно должны быть одинаковыми), а поток данных может быть чем-угодно для обеих сторон.
 Copper Straight-through	Этот тип кабеля является стандартной средой передачи Ethernet для соединения устройств, который функционирует на разных уровнях OSI. Он должен быть соединен со следующими типами портов: медный 10 Мбит/с (Ethernet), медный 100 Мбит/с (Fast Ethernet) и медный 1000 Мбит/с (Gigabit Ethernet).
 Copper Cross-over	Этот тип кабеля является средой передачи Ethernet для соединения устройств, которые функционируют на одинаковых уровнях OSI. Он может быть соединен со следующими типами портов: медный 10 Мбит/с (Ethernet), медный 100 Мбит/с (Fast Ethernet) и медный 1000 Мбит/с (Gigabit Ethernet).
 Fiber	Оптоволоконная среда используется для соединения между оптическими портами (100 Мбит/с или 1000 Мбит/с).
 Phone	Соединение через телефонную линию может быть осуществлено только между устройствами, имеющими модемные порты. Стандартное представление модемного соединения - это конечное устройство (например, ПК), дозванивающееся в сетевое облако.
 Coaxial	Коаксиальная среда используется для соединения между коаксиальными портами, такие как кабельный модем, соединенный с облаком Packet Tracer.
  Serial DCE and DTE	Соединения через последовательные порты, часто используются для связей WAN. Для настройки таких соединений необходимо установить синхронизацию на стороне DCE-устройства. Синхронизация DTE выполняется по выбору. Сторону DCE можно определить по маленькой иконке “часов” рядом с портом. При выборе типа соединения Serial DCE, первое устройство, к которому применяется соединение, становится DCE-устройством, а второе - автоматически станет стороной DTE. Возможно и обратное расположение сторон, если выбран тип соединения Serial DTE.

После создания сети ее нужно сохранить, выбрав пункт меню File -> Save или иконку Save на панели Main Tool Bar. Файл сохраненной топологии имеет расширение *.pkt .

Packet Tracer дает нам возможность симулировать работу с интерфейсом командной строки (ИКС) операционной системы IOS, установленной на всех коммутаторах и маршрутизаторах компании Cisco.

Подключившись к устройству, мы можем работать с ним так, как за консолью реального устройства. Симулятор обеспечивает поддержку практически всех команд, доступных на реальных устройствах.

Подключение к ИКС коммутаторов или маршрутизаторов можно произвести, нажав на необходимое устройство и перейдя в окно свойств к вкладке CLI.

Для симуляции работы командной строки на конечном устройстве (компьютере) необходимо в свойствах выбрать вкладку Desktop, а затем нажать на ярлык Command Prompt.

Работа с файлами в симуляторе

Packet Tracer дает возможность пользователю хранить конфигурацию некоторых устройств, таких как маршрутизаторы или свичи, в текстовых файлах. Для этого необходимо перейти к свойствам необходимого устройства и во вкладке Config нажать на кнопку “Export…” для экспорта конфигурации Startup Config или Running Config. Так получим диалоговое окно для сохранения необходимой конфигурации в файл, который будет иметь расширение *.txt . Текст файла с конфигурацией устройства running-config.txt (имя по умолчанию) аналогичен тексту информации полученной при использовании команды show running-config в IOS-устройствах.

Необходимо отметить, что конфигурация каждого устройства сохраняется в отдельном текстовом файле. Пользователь также имеет возможность изменять конфигурацию в сохраненном файле вручную с помощью произвольного текстового редактора. Для предоставления устройству сохраненных или отредактированных настроек нужно во вкладке Config нажать кнопку “Load...” для загрузки необходимой конфигурации Stàrtup Config или кнопку “Merge…” для загрузки конфигурации Running Config.

Практическая часть

Добавим на рабочую область программы 2 комутатора Switch-PT. По умолчанию они имеют имена – Switch0 и Switch1.Добавим на рабочее поле четыре компьютера с именами по умолчанию PC0, PC1, PC2, PC3. Соединим устройства в сеть Ethernet , как показано на рис.5.4. Сохраним созданную топологию, нажав кнопку Save (в меню File -> Save).

Откроем свойства устройства PC0, нажав на его изображение. Перейдем к вкладке Desktop и симулируем работу run, нажав Command Prompt.

Список команд получим, если введем «?» и нажмем Enter. Для конфигурирования компьютера воспользуемся командой ipconfig из командной строки, например:

ipconfig 192.168.1.2 255.255.255.0

IP адрес и маску сети также можно вводить в удобном графическом интерфейсе устройства (см. рис.4.4). Поле DEFAULT GATEWAY – адреса шлюза не важно, так как создаваемая сеть не требует маршрутизации.

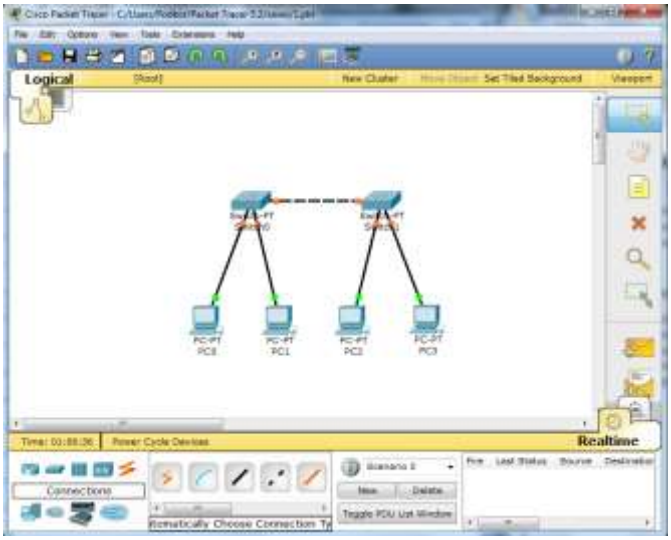


Рис.4.4. Экспериментальная модель сети

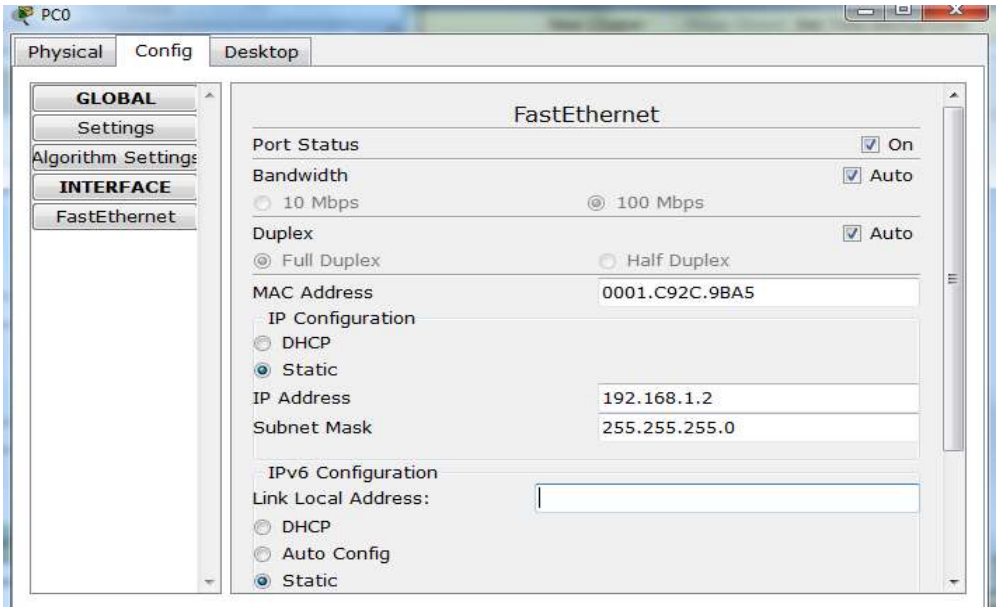


Рис.4.5.Настройка узла

Таким же путем настроим каждый компьютер.

Таблица 2

Устройство	**IP ADRESS**	**SUBNET MASK**
PC0	192.168.1.2	255.255.255.0
PC1	192.168.1.3	255.255.255.0
PC2	192.168.1.4	255.255.255.0
PC3	192.168.1.5	255.255.255.0

На каждом компьютере посмотрим назначенные адреса командой ipconfig без параметров.

В Packet Tracer 5.2 предусмотрен режим моделирования, в котором подробно описывается и показывается, как работает утилита Ping. Поэтому необходимо перейти в данный режим, нажав на одноименный значок в нижнем левом углу рабочей области, или по комбинации клавиш Shift+S. Откроется «Панель моделирования» (рис. 4.6.), в которой будут отображаться все события, связанные с выполнения ping-процесса.

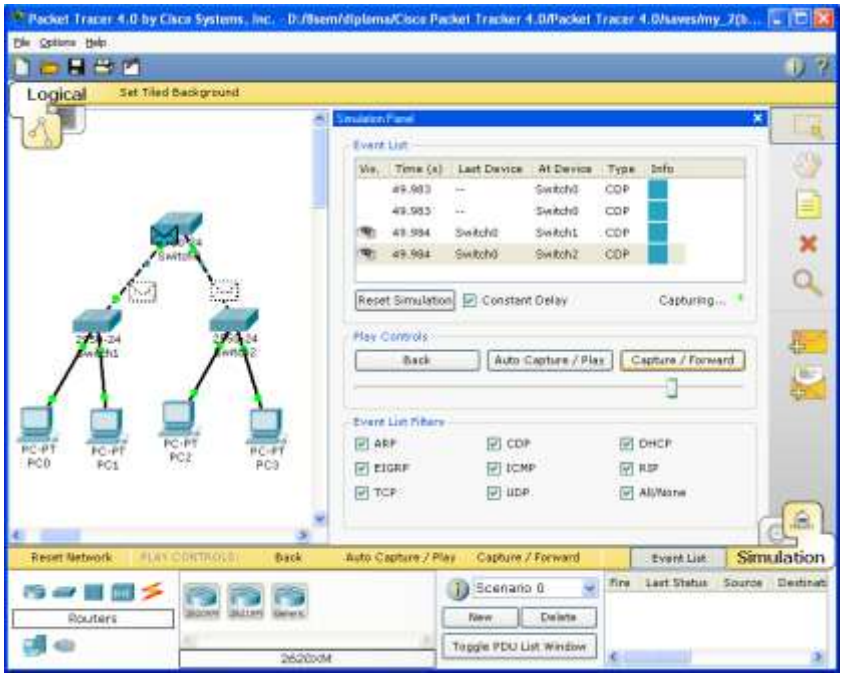


Рис.4.6. «Панель моделирования»

Теперь необходимо повторить запуск ping-процесса. После его запуска можно сдвинуть «Панель моделирования», чтобы на схеме спроектированной сети наблюдать за отправкой/приемкой пакетов.

Кнопка «Автоматически» подразумевает моделирование всего ping-процесса в едином процессе, тогда как «Пошагово» позволяет отображать его пошагово.

Чтобы узнать информацию, которую несет в себе пакет, его структуру, достаточно нажать правой кнопкой мыши на цветной квадрат в графе «Информация».

Моделирование прекращается либо при завершении ping-процесса, либо при закрытии окна «Редактирования» соответствующей рабочей станции.

Если все сделано правильно мы сможем пропинговать любой из любого компьютера. Например, зайдем на компьютер PC3 и пропингуем компьютер PC0. Мы должны увидеть отчет о пинге подобный рисунку 4.7.

Однако, это не все преимущества Packet Tracer: в «Режиме симуляции» можно не только отслеживать используемые протоколы, но и видеть, на каком из семи уровней модели OSI данный протокол задействован (см.рис.4.8).

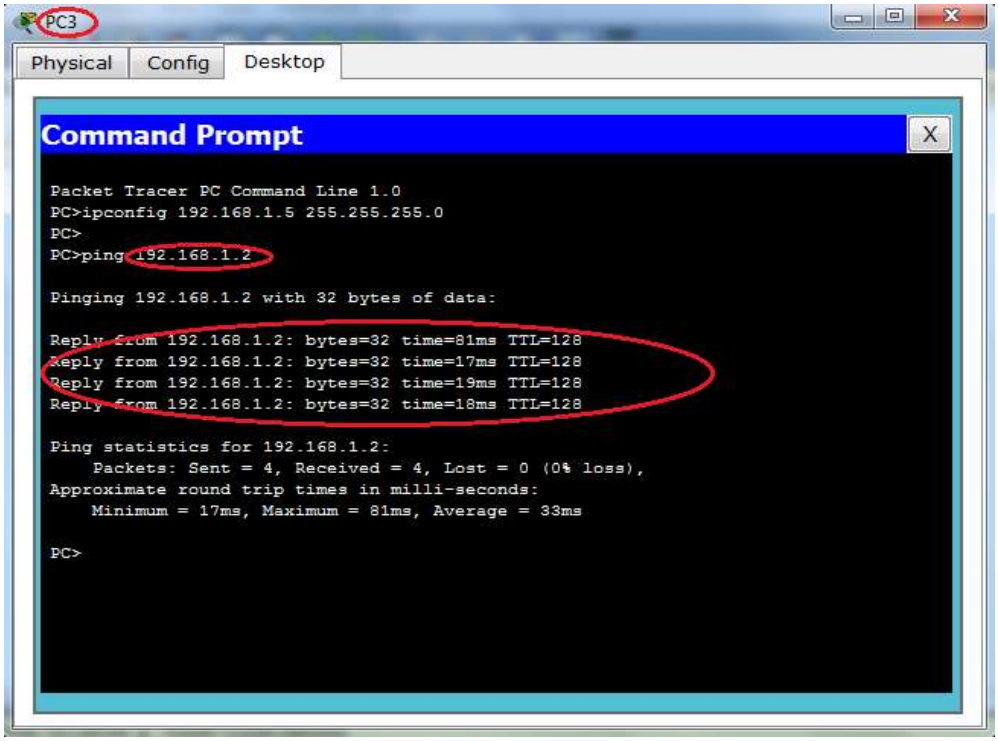


Рис.4.7. Выполнение команды ping в командной строке

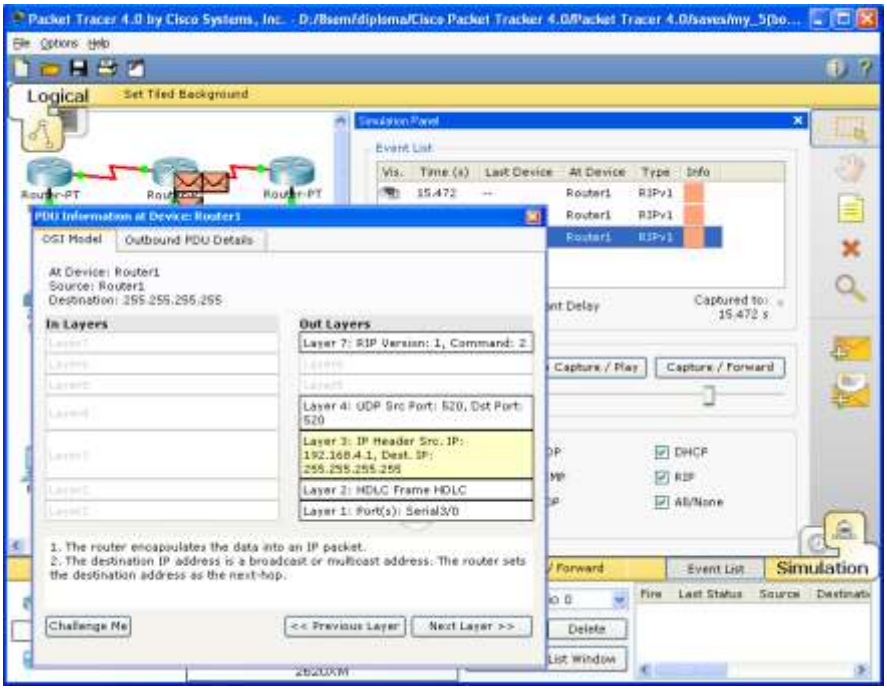


Рис.4.8 Анализ семиуровневой модели OSI в Cisco Packet Tracer 5.2.

Задание для самостоятельной работы:

1. Создайте топологию рис. 4.9.

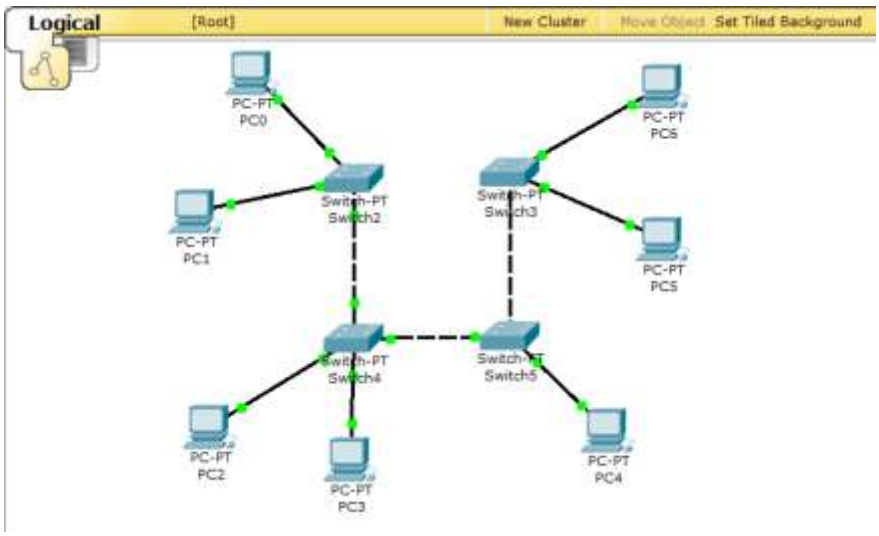


Рис 4.9. Топология сети для исследования

2. Назначьте компьютерам адреса, согласно варианту

Таблица 3.

Устройство	IP ADDRESS	SUBNET MASK
PC1	v*10. v.1.1	Маска подсети определяется в зависимости от класса сети, к которому принадлежит IP адрес
PC2	v*10. v.1.2	
PC3	v*10. v.1.3	
PC4	v*10. v.1.4	
PC5	v*10. v.1.5	
PC6	v*10. v.1.6	

Например, для варианта 7 (v=7) и компьютера PC5 имеем IP ADDRESS 70.7.1.5, маска 255.0.0.0.

Если сделано всё правильно вы сможете пропинговать любой компьютер из любого.

3. Выполните утилиту ping, согласно табл.4.

Таблица 4.

Вариант v%7	Пинг из	Пинг в	Вариант v	Пинг из	Пинг в
1	PC1	PC6	8	PC6	PC5
2	PC2	PC6	9	PC1	PC6
3	PC3	PC1	10	PC2	PC6
4	PC4	PC2	11	PC3	PC1
5	PC5	PC3	12	PC4	PC2
6	PC6	PC4	13	PC5	PC3
7	PC6	PC5	14	PC6	PC4

4. В «Режиме симуляции» отследите движение пакетов и используемые протоколы, (см.рис 4.8).

1. Переключившись в «Режим симуляции» рассмотреть и пояснить процесс обмена данными по протоколу ICMP между устройствами (выполнив команду Ping с одного компьютера на другой п.3), пояснить роль протокола ARP в этом процессе. Детальное пояснение включить в отчет.

2. Убедиться в достижимости всех объектов сети по протоколу IP.

Содержание отчёта

Отчёт готовится в электронном виде и распечатывается. Отчёт содержит:

1. Задание (Скриншот топологии согласно варианту)
2. Схема сети.
3. Ход работы:
    a. Данный раздел состоит из последовательного описания значимых выполняемых шагов (с указанием их сути) Пояснения работы команды ping и **содержимго протоколов**.
    b. копий экранов (должна быть видна набранная команда и реакция системы, если она есть).
4. Выводы.

Контрольные вопросы:

1. Что такое компьютерная сеть?
2. Назовите три преимущества компьютерной сети.
3. Опишите различия между ЛВС и ГВС?
4. Какие бывают конфигурации сетей и каковы принципы их работы, преимущества и недостатки?
5. В чем заключается функция сервера? Расскажите о технологии клиент-сервер.
6. Назовите основные сетевые топологии. Какая из них наиболее надежная и почему?
7. Назовите основные аппаратные сетевые компоненты и их назначение.
8. Какие типы сетевых устройств и соединений можно использовать в Packet Tracer?
9. Каким способом можно перейти к интерфейсу командной строки устройства.
10. Как добавить в топологию и настроить новое устройство?
11. Как сохранить конфигурацию устройства в .txt файл?

Практическая работа № 9

РАСЧЕТ ETHERNET –СЕТЕЙ, СОСТОЯЩИХ ИЗ СЕГМЕНТОВ РАЗЛИЧНЫХ ТЕХНОЛОГИЙ

Цель работы: изучить процесс обновления микропрограммного обеспечения и загрузчика.

Оборудование и программное обеспечение: методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия

Общие сведения:

Соблюдение многочисленных ограничений, установленных для различных стандартов физического уровня сетей Ethernet, гарантирует корректную работу сети (естественно, при исправном состоянии всех элементов физического уровня). Основные характеристики и ограничения технологии Ethernet приведены в таблицах 1 и 2.

Таблица 1 - Общие ограничения для всех стандартов Ethernet

Характеристика	Значение
Номинальная пропускная способность	10 Мбит/с
Максимальное число станций в сети	1024
Максимальное расстояние между узлами в сети	2500 м (в 10Base-FB - 2750 м)
Максимальное число коаксиальных сегментов в сети	5

Таблица 2 - Параметры спецификаций физического уровня для стандарта Ethernet

Параметр	10Base-5	10Base-2	10Base-T	10Base- F
Кабель	Толстый коаксиальный кабель RG-8 или RG-11	Тонкий коаксиальный кабель RG-58	Неэкранированная витая пара категорий 3,4,5	Многомодовый волоконно-оптический кабель
Максимальная длина сегмента, м	500	185	100	2000
Максимальное расстояние между узлами сети (при использовании повторителей), м	2500	925	500	2500(2740 для 10Base-FB)
Максимальное число станций в сегменте	100	30	1024	1024
Максимальное число повторителей между любыми станциями сети	4	4	4	4 (5 для 10Base-FB)

Наиболее часто приходится проверять ограничения, связанные с длиной отдельного сегмента кабеля, а также количеством повторителей и общей длиной сети.

Правила «5-4-3» (допускается соединение в линию до 5 сегментов не более чем через 4 повторителя, из этих сегментов только 3 могут использоваться для подключения узлов (Trunk segments), остальные (Link segments) используются как удлинители) для коаксиальных сетей и «4 хабов» (число повторителей (концентраторов) между любыми двумя компьютерами в сети Ethernet не может быть больше четырех) для сетей на основе витой пары и оптоволокна не только дают гарантии работоспособности сети, но и оставляют большой «запас прочности» сети. Например, если посчитать время двойного оборота в сети, состоящей из 4 повторителей 10Base-5 и 5 сегментов максимальный длины 500 м, то окажется, что оно составляет 537 битовых
интервала. А так как время передачи кадра минимальной длины (вместе с преамбулой), составляющей 72 байт, равно 575 битовым интервалам, то видно, что разработчики стандарта Ethernet оставили 38 битовых интервала в качестве запаса для обеспечения надежности. Тем не менее в документах комитета IEEE 802.3 утверждается, что и 4 дополнительных битовых интервала создают достаточный запас надежности.
Комитет IEEE 802.3 приводит исходные данные о задержках (таблицы 3 и 4), вносимых повторителями и различными средами передачи данных, для тех специалистов, которые хотят самостоятельно рассчитывать максимальное количество повторителей и максимальную общую длину сети, не довольствуясь теми значениями, которые приведены в правилах «5-4-3» и «4 хабов».

Таблица 3 - Данные для расчета значения PDV(Path Delay Value - время двойного оборота)

Тип сегмента	База левого сегмента, bt	База промежуточного сегмента, bt	База правого сегмента, bt	Задержка среды на 1 м, bt	Максимальная длина сегмента, м
10Base-5	11,8	46,5	169,5	0,0866	500
10Base-2	11,8	46,5	169,5	0,1026	185
10Base-T	15,3	42,0	165,0	0,113	100
10Base-FB	-	24,0	-	0,1	2000
10Base-FL	12,3	33,5	156,5	0,1	2000
FOIRL	7,8	29,0	152,0	0,1	1000
AUI (>2 м)	0	0	0	0,1026	2+48

Таблица 4 - Уменьшение межкадрового интервала повторителями

	Передающий сегмент, bt	Промежуточный сегмент, bt
10Base-5 или 10Base-2	16	11
10Base-FB	-	2
10Base-FL	10,5	8
10Base-T	10,5	8

Особенно такие расчеты полезны для сетей, состоящих из смешанных кабельных систем, например, коаксиала и оптоволокна, на которые правила о количестве повторителей не рассчитаны. При этом максимальная длина каждого отдельного физического сегмента должна строго соответствовать стандарту, то есть 500 м для «толстого» коаксиала, 100 м для витой пары и т. д.
Чтобы сеть Ethernet, состоящая из сегментов различной физической природы, работала корректно, необходимо выполнение четырех основных условий:

- количество станций в сети - не более 1024;
- максимальная длина каждого физического сегмента - не более величины, определенной в соответствующем стандарте физического уровня;

- время двойного оборота сигнала (Path Delay Value, PDV) между двумя самыми удаленными друг от друга станциями сети - не более 575 битовых интервала;
- сокращение межкадрового интервала (Path Variability Value, PVV) при прохождении последовательности кадров через все повторители - не больше, чем 49 битовых интервала (так как при отправке кадров конечные узлы обеспечивают начальное межкадровое расстояние в 96 битовых интервала, то после прохождения повторителя оно должно быть не меньше, чем 96 – 49 = 47 битовых интервала).

Соблюдение этих требований обеспечивает корректность работы сети даже в случаях, когда нарушаются простые правила конфигурирования, определяющие максимальное количество повторителей и общую длину сети в 2500 м.

Методика расчета времени двойного оборота и уменьшения межкадрового интервала

Для упрощения расчетов обычно используются справочные данные IEEE, содержащие значения задержекения задержек распространения сигналов в повторителях, приемопередатчиках и различных физических средах (таблица 6.3). Битовый интервал обозначен как bt.

Комитет 802.3 старался максимально упростить выполнение расчетов, поэтому данные, приведенные в таблице, включают сразу несколько этапов прохождения сигнала. Например, задержки, вносимые повторителем, состоят из задержки входного трансивера, задержки блока повторения и задержки выходного трансивера. Тем не менее в таблице все эти задержки представлены одной величиной, названной базой сегмента.

Чтобы не нужно было два раза складывать задержки, вносимые кабелем, в таблице даются удвоенные величины задержек для каждого типа кабеля.

В таблице используются также такие понятия, как левый сегмент, правый сегмент и промежуточный сегмент. Поясним эти термины на примере сети, приведенной на рисунке 6.1.

Левым сегментом называется сегмент, в котором начинается путь сигнала от выхода передатчика конечного узла. На рисунке 6.1 это сегмент 1. Затем сигнал проходит через промежуточные сегменты 2-5 и доходит до приемника наиболее удаленного узла наиболее удаленного сегмента 6, который называется правым. Именно здесь в худшем случае происходит столкновение кадров и возникает коллизия.

С каждым сегментом связана постоянная задержка, названная базой, которая зависит только от типа сегмента и от положения сегмента на пути сигнала (левый, промежуточный или правый). База правого сегмента, в котором возникает коллизия, намного превышает базу левого и промежуточных сегментов.

Кроме этого, с каждым сегментом связана задержка распространения сигнала вдоль кабеля сегмента, которая зависит от длины сегмента и вычисляется путем умножения времени распространения сигнала по одному метру кабеля (в битовых интервалах) на длину кабеля в метрах.

Расчет PDV заключается в вычислении задержек, вносимых каждым отрезком кабеля (приведенная в таблице задержка сигнала на 1 м кабеля умножается на длину сегмента), а затем суммировании этих задержек с базами левого, промежуточных и правого сегментов. Общее значение PDV не должно превышать 575.

Так как левый и правый сегменты имеют разные величины базовой задержки, то в случае различных типов сегментов на удаленных краях сети необходимо выполнить расчеты дважды: один раз принять в качестве левого сегмента сегмент одного типа, а во второй - сегмент другого типа. Результатом можно считать максимальное значение PDV. Чтобы признать конфигурацию сети корректной, нужно рассчитать также уменьшение межкадрового интервала повторителями, то есть величину PVV.

Для расчета PVV также можно воспользоваться значениями максимальных величин

уменьшения межкадрового интервала при прохождении повторителей различных физических сред, рекомендованными IEEE и приведенными в таблице 1.4.

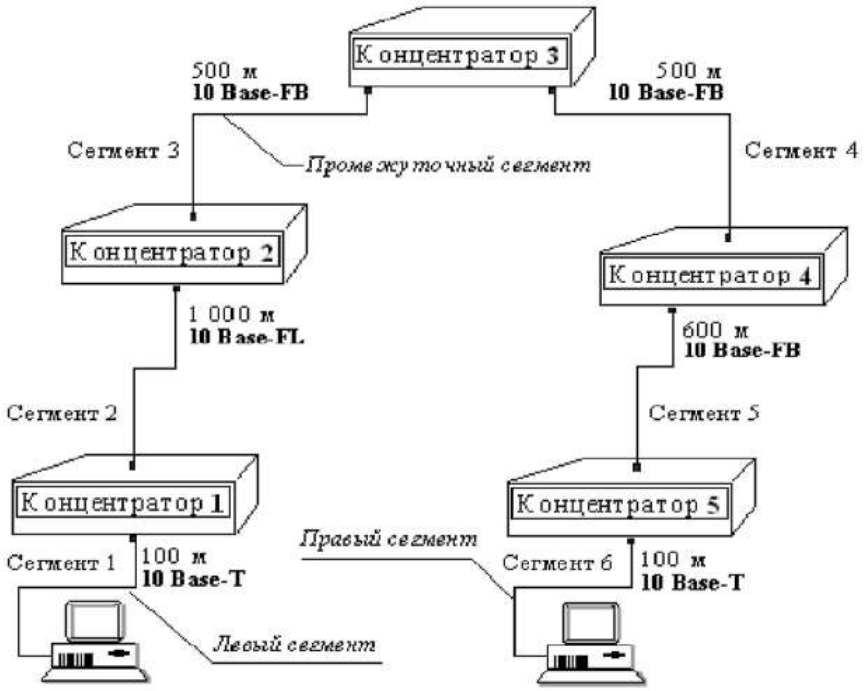


Рисунок 6.1 - Пример сети Ethernet, состоящей из сегментов различных физических стандартов

Пример расчета конфигурации сети

В примере крайние сегменты сети принадлежат к одному типу - стандарту 10Base-T, поэтому двойной расчет не требуется.

Приведенная на рисунке 6.1 сеть в соответствии с правилом «4 хабов» не является корректной - в сети между узлами сегментов 1 и 6 имеются 5 хабов, хотя не все сегменты являются сегментами 10Base-FB. Кроме того, общая длина сети равна 2800 м, что нарушает правило 2500 м. Рассчитаем значение PDV.

Левый сегмент 1:

15,3 (база) + 100-0,113 = 26,6

Промежуточный сегмент 2:

33,5 + 1000-0,1 = 133,5

Промежуточный сегмент 3:

24 + 500-0,1 = 74,0

Промежуточный сегмент 4:

24 + 500-0,1 = 74,0.

Промежуточный сегмент 5:

24 + 600-0,1 = 84,0

Правый сегмент 6:

165 + 100-0,113 = 176,3.

Сумма всех составляющих дает значение PDV, равное 568,4.

Так как значение PDV меньше максимально допустимой величины 575, то эта сеть проходит по критерию времени двойного оборота сигнала несмотря на то, что ее общая длина превышает 2500 м, а количество повторителей больше 4.

Рассчитаем значение PVV.

Левый сегмент 1 10Base-T: сокращение в 10,5 bt.

Промежуточный сегмент 2 10Base-FL: 8.

Промежуточный сегмент 3 10Base-FB: 2.

Промежуточный сегмент 4 10Base-FB: 2.

Промежуточный сегмент 5 10Base-FB: 2.

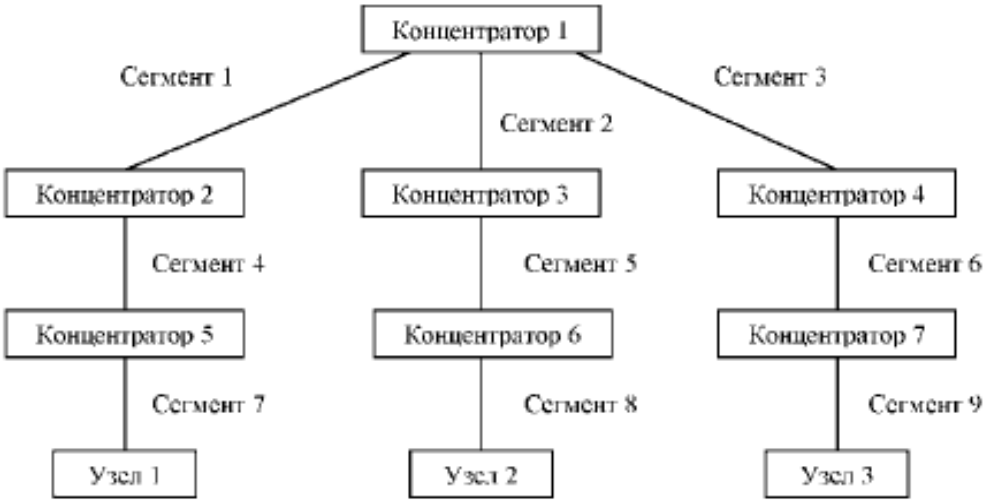
Сумма этих величин дает значение PVV, равное 24,5, что меньше предельного значения в 49 битовых интервала.

В результате сеть соответствует стандартам Ethernet по всем параметрам.

Задание

1. Ознакомиться с теоретическим материалом.
2. Произвести оценку конфигурации сети в соответствии с вариантом:
   - по физическим ограничениям: на длину сегмента, на длину сети, правило «4 хаба» («5 хабов» для 10Base-FB);
   - по времени двойного оборота сигнала в сети;
   - по уменьшению межкадрового интервала.
3. По результатам расчетов сделать вывод о корректности конфигурации сети Ethernet.
4. По результатам работы оформить отчет. Содержание отчета: исходные данные, расчеты указанных параметров, выводы.

Вариант 1



	10 Base-FB	10 Base-FL	10 Base-T	Длина, м
Сегмент 1	+			500
Сегмент 2	+			300
Сегмент 3	+			400
Сегмент 4		+		1000
Сегмент 5		+		300
Сегмент 6		+		400
Сегмент 7			+	100
Сегмент 8			+	50
Сегмент 9			+	100

Контрольные вопросы:

1. Как происходит передача информации по компьютерной сети и что такое архитектура Ethernet?
2. Что такое сетевой протокол? Расскажите о протоколе TCP/IP.
3. Каковы основные функции сетевой операционной системы? Какие сетевые ОС вы знаете? Расскажите о службах Windows NT.
4. Как произвести добавление принтера в сеть и сделать его разделяемым?
5. Какие основные этапы включает в себя администрирование сети?

Практическая работа № 10

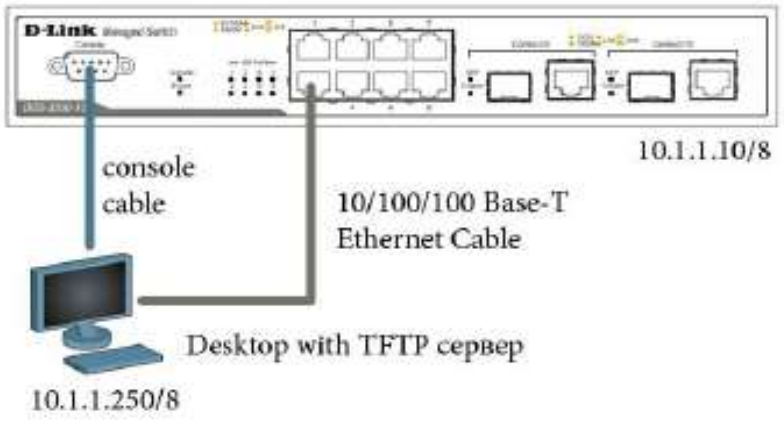
КОМАНДЫ ОБНОВЛЕНИЯ МИКРОПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КОММУТАТОРА И СОХРАНЕНИЯ/ВОССТАНОВЛЕПИЯ КОНФИГУРАЦИОННЫХ ФАЙЛОВ

Цель работы: изучить процесс обновления микропрограммного обеспечения и загрузчика.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия, рабочая станция с TFTP сервером, коммутатор DGS-3200-10, консольный кабель, Ethernet кабель.

Общие сведения:

Исходная схема:



Подготовка к режиму обновления и сохранения микропрограммного обеспечения коммутатора.

Настройте TFTP-сервер (на примере Tftpd32 byPh.Jounin)

1. В настройках необходимо установить директорию приема файлов
2. Отключить все другие сервисы кроме TFTPserver

Подготовьте файл обновления

1. Поиск необходимого файла обновления «прошивки» на сайте http://www.dlink.ru (или http://www.dlink.com)
2. Выкачивание файла и перенос в директорию указанную в TFTP-сервере.
3. Прочитайте файл сопровождения к «прошивке».

Загрузка файла микропрограммного обеспечения в память коммутатора.

НастройтеIP-адрес configipifSystemipaddress 10.1.1.10/8
Настройте TFTP-сервер
Выставить IP адрес рабочей станции 10.1.1.250/8
Запустить TFTP сервер; указать директорию с прошивкой CurrentDirectory.
Проверьте доступность TFTP-сервера ping 10.1.1.250
Проверьте текущее микропрограммное обеспечение showfirmwareinformation
Загрузите микропрограммное обеспечение на коммутатор
downloadfirmware_fromTFTP 10.1.1.250 DGS3200_Run_1_50_B038.had image_id 2
Убедитесь что программное обеспечение загружено showfirmwareinformation

Конфигурирование загрузки firmware коммутатора

Смените микропрограммное обеспечение, с которого будет загружаться коммутатор
config firmware image_id 2 boot_up
Сохраните изменения save
Перезагрузите коммутатор reboot
Обновленная прошивка вступит в силу
только после перезагрузки
Проверьте информацию прошивки showfirmwareinformation
Что вы наблюдаете

Управление изменениями конфигураций

Посмотрите текущую версию коммутатора (в RAM) showconfigcurrent_config
Посмотрите конфигурацию загрузки (из NVRAM) showconfigconfig_in_nvram 1
Выгрузите конфигурацию на TFTP-сервер uploadcfg_toTFTP 10.1.1.250
config.txt
Открыть выгруженный конфигурационный файл любым текстовым редактором,
например блокнотом и просмотреть его структуру.
Замените IP адрес 10.1.1.10/8 на 10.1.1.8/8
IP
configipif System ipaddress 10.1.1.10/8 vlan default state enable
disableautoconfig
IP
configipif System ipaddress 10.1.1.8/8 vlan default state enable
disableautoconfig
сохраните файл.
Загрузите измененную конфигурацию downloadcfg_fromTFTP 10.1.1.250
config.txt
Проверьте, изменился ли IP-адрес коммутатора showswitch
Что вы наблюдаете
Чему будет равен IP адрес после перезагрузки коммутатора?

Выгрузка log-файлов

Просмотрите log коммутатора showlog

Выгрузите log-файл на TFTP-сервер uploadlog_toTFTP 10.1.1.250 logfiles.txt
Открыть выгруженный лог файл любым текстовым редактором, например блокнотом и просмотреть его структуру.

Контрольные вопросы:

1. Подготовка к режиму обновления и сохранения микропрограммного обеспечения коммутатора.
2. Загрузка файла микропрограммного обеспечения в память коммутатора.
3. . Конфигурирование загрузки firmware коммутатора.
4. Управление изменениями конфигураций.
5. Выгрузка log-файлов.

Практическая работа № 11

АНАЛИЗ ТРАФИКА КОМПЬЮТЕРНОЙ СЕТИ С ПОМОЩЬЮ СНИФФЕРОВ

Цель работы: приобретение практических навыков в перехвате и анализе трафика сегмента компьютерной сети.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия.

Общие сведения:

Снифферы (дословный перевод - ‘вынюхиватели’) являются специализированным ПО,предназначенным для анализа потока сообщений (трафика) компьютерной сети передачи информации [4]. Известными системами подобного рода (но глобального уровня)являются ЭШЕЛОН (североамериканский проект, назначением которого является анализ содержимого линий связи Европы) и СОРМ (тотальное протоколирование трафика русскоязычной Сети). Большинство программ и сервисов (ICQ, TelNet, FTP, HTTP, POP3 и т.д.) пересылают пароль и логин пользователя открытым текстом (без всякой кодировки и шифровки), и работающий сниффер без труда позволит перехватывать такие сессии.

К простым ПО подобного класса относится, например комплект SpyNet (simik.lgg.ru/spynet312.exe); в штатную поставку Windows’NT Server и др. входит утилита Network Monitor (устанавливается добавлением сервиса Network Monitor Tools & Agent).

Обычно сетевая карта, работающая в сегменте некоммутируемой Ethernet в принципе ‘прослушивает’ весь трафик своего сегмента; однако в нормальном (без PROMISCUOUS MODE) режиме анализируются лишь первые 48 бит заголовка пакета и, если не найден собственный MAC-адрес, карта перестает читать ‘чужой’ пакет.

Функциональность сниффера достигается переводом сетевой карты в режим

PROMISCUOUS MODE, обеспечивающий перехват всех сообщений, циркулирующих в данном сегменте сети безотносительно MAC-адресов (достигается программной установкой соответствующего бита управляющего регистра карты). В случае коммутируемого Ethernet перевод карты в PROMISCUOUS MODE не позволяет прослушивать ‘чужие’ сообщения, в этом случае используется технология ‘ARP- спуфинга’ (путем соответствующей подделки ARP-сообщений данная сетевая карта ‘притворяется’ маршрутизатором с MAC-адресом, однако, данной карты), при этом трафик всех составляющих сегмента сети насильственно направится в сторону карты- обманщика.

Контрольные вопросы:

1. Что представляет из себя ПО класса снифферов и с какой целью применяется?
2. Каковы ограничения методов перехвата информации снифферами?
3. Каким образом сетевая плата конкретной ЭВМ в локальной сети распознает назначение пакетов по принципу «свой-чужой»?
4. Какие методы применяются с целью исключения возможности перехвата сообщений снифферами?

Практическая работа № 12

ОСНОВНЫЕ КОМАНДЫ КОММУТАТОРОВ. УПРАВЛЕНИЕ КОММУТАТОРАМИ

Цель работы: ознакомиться с основными командами настройки, контроля и устранения неполадок коммутаторов.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия, ПК, коммутатор DGS-3200-10, консольный кабель.

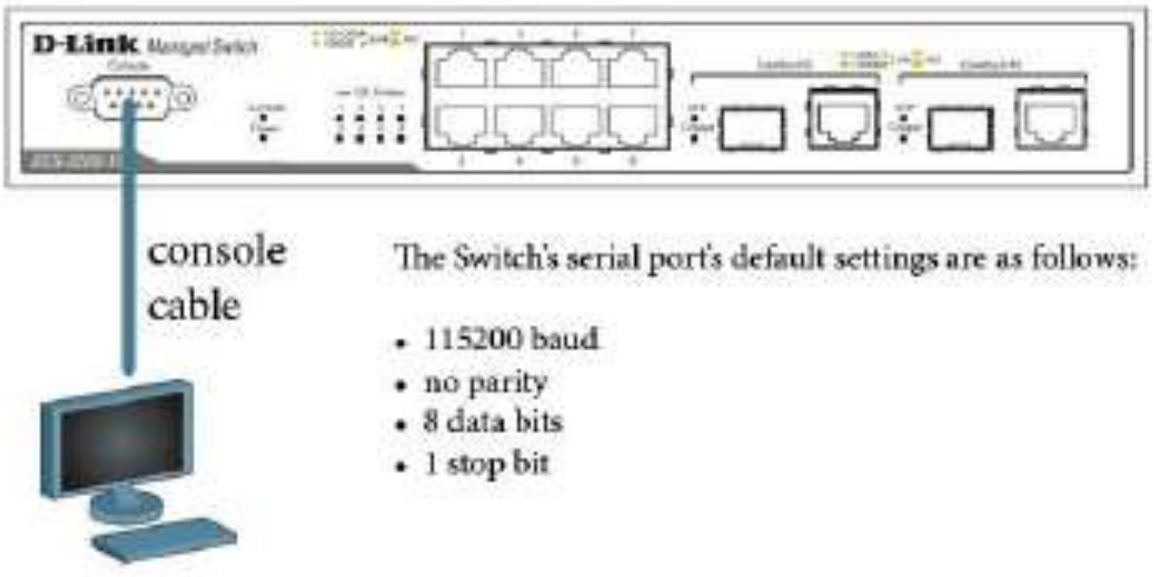
Общие сведения:

Существует три основных типа:

1. Неуправляемые коммутаторы – функции настройки и управления не поддерживают, имеют уже предустановленную функциональность. Данные коммутаторы применяются там, где характеристики необходимые в сети стандартные и не требуют дополнительных настроек. Обычно, это сети класса SOHO (SmallOfficeHomeOffice) малые предприятия и домашние сети.

2. Настраиваемые коммутаторы (Smart) – данные коммутаторы имеют ограниченные возможности управления, чаще всего через Web-консоль иногда через telnet. Применяются в сетях SOHO, бюджетных решениях ISP-сетей (InternetServiceProvider), в небольших корпоративных сетях. Отличаются небольшой стоимостью и легкостью настроек и интуитивно понятным интерфейсом.

3. Управляемые коммутаторы – коммутаторы, имеющие широкий набор функций управления и возможность получить максимально точные и необходимые настройки сети. Включающие в себя возможности управления через Web-интерфейс, через последовательный порт, с помощью сетевых консолей TELNET, SSH, протокола SNMP, имеют возможности удаленного мониторинга RMON. Область применения данных коммутаторов – ISP-сети, корпоративные сети средних и крупных предприятий и др. Интерфейс командной строки (Command-LineInterface, CLI) может быть использован для настройки и управления коммутаторами через последовательный порт и telnet.



1.1. Вызов помощи по командам

Внимание! При написании команд в CLI важно учитывать регистр. Для того чтобы ознакомиться с правильностью написания команд, последовательностью выполнения операции можно обращаться к встроенной помощи по командам!

Напишите в консоли ?

Напишите в консоли dir

Напишите в консоли config

Напишите в консоли show

1.2. Изменение IP-адреса коммутатора

Проверить параметры настройки IP-интерфейса showipif

Чему равен IP адрес по умолчанию (вписать)

Измените IP-адрес configipifSystemipaddress10.1.1.10/8

Настройте IP-адрес шлюза по умолчанию createiproutedefault 10.1.1.254

Замечание. IP-адрес шлюз по умолчанию назначается, если управление коммутатором осуществляется из других IP-подсетей.

Проверьте настройки showswitch

(IP адрес, Маска, Шлюз)

1.3. Управление учетными записями пользователей

Заведите учетную запись администратора createaccountadmindlink

Укажите пароль и подтверждение пароля администратора: dlink

Enter a case-sensitive new password: dlink

Enter the new password again for confirmation: dlink

Для выхода из режима с текущими правами введите команду logout

Осуществить вход по новой созданной учетной записи администратора

Username: dlin

Password: dlink

DES-3526:4#

Заведите учетную запись пользователя createaccountuserswuser

Укажите пароль и подтверждение пароляпользователя: dlink1

Enter a case-sensitive new password: dlink1

Enter the new password again for confirmation: dlink1

Проверьте настройки учетных записей пользователей showaccount

Измените пароль пользователя configaccountswuser

После ввода команды укажите старый

пароль пользователя и 2 раза новый пароль.

Enter a old password:****

Enter a case-sensitive new password:****

Enter the new password again for confirmation:****

Удалите учетную запись deleteaccountswuser

Проверьте удаление учетной записи пользователя showaccount

1.4. Настройка параметров идентификации коммутатора

Настройте имя коммутатора configsnmpsystem_nameTEST

Настройте месторасположение (локализацию)

configsnmpsystem_locationTEST_PRACTICE

Настройте ответственный контакт configsnmpsystem_contactLABORANT

Проверьте внесенные параметры showswitch

Внимание: Длина параметров идентификации коммутаторов от 0 до 255 символов.
0 символов подразумевает, что информация отсутствует

1.5. Настройкапараметровбаннеровприветствия (Login banner (greeting message) and Command Prompt)

Для лучшей идентификации активного оборудования пользователями или создания уникальных логотипов оборудования возможно изменения баннера загрузки, который появляется в момент загрузки оборудования. Также возможно изменения указателя CommandPrompt в командной строке CLI.

Изменитеуказатель Command Prompt configcommand_prompt TEST_SWITCH
Установите указатель по умолчанию configcommand_promptdefault
Посмотрите текущий баннер приветствия showgreeting_message
Войдите в режим конфигурирования баннера configgreeting_message
Команды конфигурирования в остнастке
<FunctionKey> <ControlKey>
Ctrl+C Quit without save left/right/
Ctrl+W Save and quit up/down Move cursor
Ctrl+D Delete line
Ctrl+X Erase all setting
Ctrl+L Reload original setting
Добавьтестрочкувприветствие SWITCH_TEST tel +7(499) 000-00-00
СохранитьивыйтиCtrl+W
Проверьтебаннер show greeting_message
Восстановите настройки баннера по умолчанию configgreeting_message default
Проверьте баннер show greeting_message

1.6. Настройка времени на коммутаторе

Проверьте время showtime
Введите команду configtime 16dec2010 15:45:30
Дату и время выставить текущую
УстановитечасовойпоясМосква (GMT +3:00) configtime_zone operator + hour 3
min 0
Проверьте время showtime
Внимание! При перезагрузке коммутатора возможен сброс настроек текущего времени на коммутаторе, это обусловлено тем, что время храниться на некоторых моделях в RAM памяти коммутатора, т.о. в случае если в сети существуют серверы службы времени (NTP сервера) или открыт доступ к серверам времени расположенным в интернете, желательно настроить синхронизацию с этими серверами.
Включите работу протокола SNTP на коммутаторе enablesntp
Занесите список серверов SNTP и интервал обращений к серверам в сек.
configsntp primary 10.1.1.200 secondary 10.1.1.201 poll-interval 3600
Проверьте текущее время showtime
Проверьте descriptions портов show ports description

Контрольные вопросы:

1. Вызов помощи по командам.
2. Изменение IP-адреса коммутатора.

3. Управление учетными записями пользователей
4. Настройка параметров идентификации коммутатора
5. Настройка времени на коммутаторе

Практическая работа № 13-14

ПОСТРОЕНИЕ ЛВС. СТРУКТУРИРОВАННАЯ КАБЕЛЬНАЯ СИСТЕМА

Цель работы: изучить назначение и способы организации СКС.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия.

Общие сведения:

СКС – основа компьютерной локальной сети (ЛВС)

Для работы организации требуется локальная сеть, объединяющая компьютеры, телефоны, периферийное оборудование. Без компьютерной сети можно обойтись. Только неудобно обмениваться файлами при помощи дискет, выстраиваться в очередь возле принтера, а доступ в интернет реализовывать через один компьютер. Решением служит технология, обозначаемая сокращенно СКС.

Структурированная кабельная система это универсальная телекоммуникационная инфраструктура здания или комплекса зданий, обеспечивающая передачу сигналов всех типов, включая речевые, информационные, видео. СКС может быть установлена прежде, чем станут известны требования пользователей, скорость передачи данных, тип сетевых протоколов. Рекомендуемые стандартами рамки СКС составляют 50 – 50 000 пользователей на площади до 1 000 000 м2.

СКС создает основу компьютерной сети, интегрированной с телефонной сетью. Совокупность телекоммуникационного оборудования здания / комплекса зданий, соединенного с помощью структурированной кабельной системы, называют локальной сетью.

СКС или компьютерная плюс телефонная сеть

Структурированные кабельные системы обеспечивают длительный срок службы, сочетая удобство эксплуатации, качество передачи данных, надежность. Внедрение СКС создает основу повышения эффективности организации, снижения эксплуатационных расходов, улучшения взаимодействия внутри компании, обеспечения качества обслуживания клиентов.

Структурированная кабельная система строится таким образом, чтобы каждый интерфейс (точка подключения) обеспечивал доступ ко всем ресурсам сети. При этом на рабочем месте достаточно двух линий. Одна линия является компьютерной, вторая – телефонной. Линии взаимозаменяемы. Кабели соединяют телекоммуникационные разъемы рабочих мест с портами распределительных пунктов.

Распределительные пункты объединяют магистральными линиями по топологии «иерархическая звезда».

СКС является интегрированной системой. Сравним СКС с устаревшей моделью "компьютерная плюс телефонная сеть". Ряд преимуществ является очевидным.

- интегрированная локальная сеть позволяет передавать разнотипные сигналы;
- СКС обеспечивает работу нескольких поколений компьютерных сетей;
- интерфейсы СКС позволяют подключать любое оборудование локальных сетей и речевых приложений;
- СКС реализует большой диапазон скорости передачи данных от 100 Кбит/сек речевых приложений до 10 Гбит/сек информационных приложений;

- администрирование СКС сокращает трудозатраты обслуживания локальной сети благодаря простоте эксплуатации;
- компьютерная сеть допускает одновременное использование разнотипных сетевых протоколов;
- стандартизация плюс конкуренция рынка СКС обеспечивают снижение цен комплектующих;
- локальная сеть позволяет реализовать свободу перемещения пользователей без изменения персональных данных (адресов, телефонных номеров, паролей, прав доступа, классов обслуживания);
- администрирование СКС обеспечивает прозрачность компьютерной и телефонной сети – все интерфейсы СКС промаркированы и документированы. Работа организация не зависит от сотрудника- монополиста соединений телефонной сети.

Надежная и долговечная структурированная кабельная система является фундаментом локальной сети.

Однако всякое достоинство имеет обратную сторону. Стандарты СКС рекомендуют избыточность количественных параметров системы, что влечет существенные единовременные затраты. Зато можно забыть о кошмаре перманентного ремонта действующего офиса для наращивания компьютерной сети под текущие потребности.

Стандарты СКС

Стандарты определяют структуру СКС, рабочие параметры конструктивных элементов, принципы проектирования, правила монтажа, методику измерения, правила администрирования, требования телекоммуникационного заземления.

Администрирование СКС включает маркировку портов, кабелей, панелей, шкафов, других элементов, а также систему записей, дополняемую ссылками. Вместе с продуманной организацией кабелей, заложенной на этапе создания кабельной системы, система администрирования позволяет поддерживать хорошую организацию локальной сети. Стандарты СКС 2007 года считают наличие администрирования одним из условий соответствия смонтированной системы требованиям стандартов.

СКС определяются международными, европейскими и национальными стандартами. Стандарты СКС адресованы строителям-профессионалам. В России СКС чаще создают специализированные фирмы. Россия является членом Международной организации стандартизации (ISO), поэтому руководствуется международными стандартами. Данная информация отражает требования международного стандарта ISO/IEC 11801.

Подсистемы СКС

Стандарт ISO/IEC 11801 подразделяет структурированную кабельную систему на три подсистемы:

- магистральную подсистему комплекса зданий;
- магистральную подсистему здания;
- горизонтальную подсистему.

Магистральная подсистема СКС и телефонная сеть

Магистральная подсистема комплекса зданий соединяет кабельные системы зданий.Магистральная подсистема здания соединяет распределительные пункты этажей. Магистральная подсистема включает информационную и речевую подсистемы СКС. Основная среда передачи информационной подсистемы – оптоволокно (одномодовое или многомодовое), дополняемое симметричными четырехпарными кабелями. Если длина магистральной линии не превы-

шает 90 метров, применяют симметричные кабели категории 5 и выше. При большей длине для информационных
приложений, то есть компьютерной сети, требуется прокладывать оптоволоконный кабель.
Речевые приложения магистрали здания работают по многопарным кабелям. Речевые приложения, создающие телефонную сеть, относятся к низшим классам СКС. Это позволяет увеличивать длину линий магистральной подсистемы, создаваемых многопарными кабелями, до двух-трех километров.

Горизонтальная подсистема СКС и компьютерная сеть

Горизонтальная подсистема СКС включает распределительные панели, коммутационные кабели распределительных пунктов этажа, горизонтальные кабели, точки консолидации, телекоммуникационные разъемы. Горизонтальная подсистема обеспечивает локальную сеть для абонентов, предоставляет доступ к магистральным ресурсам. Среда передачи горизонтальной подсистемы – симметричные кабели не ниже категории 5. Стандарты СКС 2007 года предусматривают для центров обработки данных выбор СКС не ниже категории 6. Для информационных технологий (компьютерная плюс телефонная сеть) частных домов новые стандарты рекомендуют использовать категорию 6 / 7. Среда передачи вещательных коммуникационных технологий (сокращенно ВКТ: телевидение, радио) частных домов / квартир – симметричные защищенные кабели с полосой частот 1 ГГц, плюс коаксиальные кабели до 3 ГГц. Допускается также применение оптоволокна.
В горизонтальной подсистеме СКС преобладает компьютерная сеть. Отсюда вытекает ограничение максимальной длины канала – 100 метров независимо от типа среды. Чтобы продлить срок службы без модификаций, горизонтальная подсистема СКС должна обеспечить избыточность, резерв параметров.

Рабочая область в структуре горизонтальной подсистемы СКС

Рабочая область СКС – помещения (часть помещений), где пользователи работают с терминальным (телекоммуникационным, информационным, речевым) оборудованием.
Рабочая область не относится к горизонтальной подсистеме СКС. Функциональным элементом горизонтальной подсистемы является телекоммуникационный разъем – ТР.
Рабочие места оснащаются розетками, включающими два или более телекоммуникационных разъема. Подключение оборудования рабочей области выполняют абонентскими кабелями. Абонентские / сетевые кабели находятся за рамками СКС, однако они позволяют создавать каналы, параметры которых определяются стандартами СКС. К СКС относят коммутационные кабели / перемычки, используемые для соединений между портами панелей / контактами кроссов.
Более 90% кабелей СКС приходится на горизонтальную подсистему. Кабели горизонтальной подсистемы максимально интегрированы в инфраструктуру здания. Любые изменения в горизонтальной подсистеме влияют на работу организации. Поэтому так важна избыточность горизонтальной подсистемы, обеспечивающая беспроблемную длительную эксплуатацию локальной сети.
Существует два метода прокладки кабелей — скрытый и открытый. Для скрытой прокладки используют конструкцию стен, полов, потолков. Однако, это не всегда возможно. Наиболее распространенный вариант кабель каналов – пластиковые короба.
Варианты открытой прокладки кабельных жгутов включают лотки, короба, миниколонны. Скрытая прокладка кабелей предусматривает установку встроенных розеток, монтаж напольных лючков.

Распределительные пункты СКС – узлы локальной сети

Распределительные пункты СКС представляют собой окончания горизонтальных и магистральных линий, которые для удобства использования фиксируют на панелях или кроссах. Для установки панелей, кроссов, сетевого оборудования служат напольные / настенные шкафы, телекоммуника-

ционные стойки. Распределительный пункт может занимать часть шкафа, несколько шкафов. Помещения распределительных пунктов называют телекоммуникационными помещениями, дословно – телекоммуникационными чуланами (Telecommunicationclosets). На каждом этаже здания рекомендуется устанавливать один РП этажа. Если офисная площадь этажа превышает 1000 квадратных метров, предусматривают дополнительный РП, соединяемый магистральными каналами.
Распределительные пункты СКС создают узлы локальной сети где компактно размещается сетевое и серверное оборудование.
Напольные шкафы позволяют размещать окончания сотен линий, оборудование, блоки УАТС. Телекоммуникационные стойки обеспечивают вместимость шкафов, но имеют меньшую стоимость. Их используют когда не требуется дополнительной защиты оборудования локальной сети или особых условий эксплуатации. Настенные шкафы рекомендуется выбирать при небольшом числе линий, отсутствии телекоммуникационного помещения. Оборудование шкафов охлаждают вентиляторами.
Удобство эксплуатации локальной сети зависит от качества организации, наличия маркировки СКС. Стандартная цветовая маркировка позволяет различать назначение портов панелей. Цвет говорит о принадлежности порта к магистральной подсистеме комплекса, магистральной подсистеме здания, горизонтальной подсистеме, подсистемам, не относящимся к СКС.
Цветом выделяют интерфейсы внешних подсистем, обозначают порты компьютерных и телефонных сетей. На фото линии магистральной информационной, горизонтальной, а также сигнальной подсистем маркированы согласно требованиям стандарта TIA/EIA-606-A. Первая цифра маркировки обозначает номер панели, вторая — номер порта панели. При этом соответствие номера портов розеток и панелей
такое же, как номера соединяющих их кабелей.

Система телекоммуникационного заземления

Телекоммуникационное заземление должно быть установлено во всех СКС независимо от наличия экранированных линий. Такое требование определено стандартом J-STD-607-A 2002 года «Совместный стандарт. Требования по заземлению телекоммуникационных систем коммерческих зданий».
Основное назначение заземления – безопасность персонала, защита магистралей, а также оборудования от воздействия грозовых разрядов, обеспечение балансировки приемо-передатчиков локальной сети.
Внутренние шины заземления телекоммуникационного оборудования (мультиплексоры, оптоэлектронные устройства), УАТС должны подключаться к системетелекоммуникационного заземления.
Телекоммуникационные шины заземления (ТШЗ) устанавливают в каждом распределительном пункте возле шкафов / стоек. Шины распределительных пунктов соединяют магистралями заземления с главной телекоммуникационной шиной заземления (ГТШЗ), устанавливаемой рядом с электрическим терминалом заземления. Современные стандарты рекомендуют увеличивать площадь сечения проводника магистрали заземления при увеличении длины магистрали. Максимальное рекомендуемое сечение может составлять 3/0 AWG или 90 кв.мм. Ответвления магистрали выполняются изотермической сваркой или неразъемным соединением.
Часто приходится сталкиваться с отсутствием или ненадлежащим исполнением систем заземления в старых постройках. Проектирование системы телекоммуникационного заземления не требует устранения недостатков электрического заземления. Когда эквипотенциальность заземления не обеспечена, реализуется принцип «эффективного экранирования».

Система электропитания

В большинстве случаев для работы компьютерной сети требуется обеспечить электропитание устройств, подключаемых к телекоммуникационным разъемам. На каждом рабочем месте устанавливают силовые розетки. Одни розетки служат для подключения компьютеров и оргтехники, другие – бытовых электроприборов. Такое разделение систем позволяет организовать централизованное гарантированное электропитание.

Известно, что прокладка силовых кабелей параллельно информационным ухудшает качество передачи данных по слаботочным линиям, что может вызвать сбои локальных сетей. Для уменьшения этого влияния требуется выдержать минимально допустимые расстояния параллельной прокладки, зависящие от напряжения, мощности нагрузки. Монтаж силовых и слаботочных сетей одним подрядчиком позволяет решить проблему электромагнитной совместимости, уменьшить инвестиционные затраты.

Варианты установки розеток

Силовые и телекоммуникационные розетки могут быть установлены в коробах, накладных розетках, стенах, телекоммуникационных колоннах, напольных лючках.

На фотографиях изображены варианты размещения телекоммуникационных разъемов (ТР) с блоками силовых розеток. Самый распространенный вариант создания кабель каналов – пластиковые короба. Для фиксации коробов используют стены, офисную мебель, даже потолки. Короба высотой более 80 мм удобны для размещения розеток. Узкие короба дополняют настеннымиподрозетниками.

Группы розеток могут быть отмечены маркировкой или цветом вставок. Например, красные вставки для питания компьютерной сети, белые – подключение бытовых электроприборов.

Телекоммуникационные колонны, напольные стойки, напольные лючки применяются реже. Причина — более высокая стоимость таких решений.

Самый дешевый вариант — встроенные розетки. Он также является наиболее эстетичным. Реализация такого способа монтажа розеток оптимальна при строительстве или ремонте офиса. Альтернативный недорогой вариант — установка настенных подрозетников, прокладка мини-коробов.

Тестирование и гарантии

Мнение о том, что тестирование СКС — это формальная процедура, весьма распространено. Многие заказчики считают, что измерение параметров линий это гарантийная процедура. Это верно, но только наполовину. Во-первых, тестирование позволяет обнаружить скрытые дефекты, которые могут быть незамеченными. Во-вторых, это единственная возможность избежать проблем работы приложений компьютерной сети.

Вопреки распространенному мнению о полном соответствии стандартов СКС требованиям сетевых протоколов это заблуждение. Параметры среды передачи ниже требований приложений. Стандарты СКС классов D (100 МГц), E (250 МГц) и F (600 МГц) предусматривают нулевое – отрицательно отношение затухания / суммарных наводок на верхней границе частотного диапазона. Для рабочих пар приложений класса D, реализуемых в компьютерных сетях, отношение сигнал / шум во всем диапазоне частот должно быть не менее 10-19 дБ, то есть на один – два порядка лучше, чем предусматривают стандарты СКС. Более того, некоторые приложения класса D работают в полосе частот более 100 МГц, определяемых категорией 5e. Диапазон частот 1000BASE-T GigabitEthernet составляет 125 МГц, ATM 155 – 155 МГц.

Таким образом, СКС может соответствовать стандартам, но не обеспечивать работу ряда приложений локальной сети по параметру коэффициента битовых ошибок (BER – BitErrorRate). При этом уменьшается скорость передачи данных вплоть до "зависаний" компьютерной сети.
Качество передачи сигналов по каналам СКС обеспечивается благодаря резерву параметров. Чтобы проверить, достаточен ли резерв, проводится тестирование соответствия сетевым протоколам. Например, при использовании кабельного анализатора Fluke (пример отчета), подтверждается соответствие базовой линии / канала одиннадцати сетевым протоколам. Это означает возможность использования также любых приложений низших классов.

Контрольные вопросы:

1. Оборудование СКС.
2. Подсистемы СКС.
3. Стандарты СКС.

Практическая работа № 15-16-17

АДРЕСАЦИЯ В IP- СЕТЯХ. ПОДСЕТИ И МАСКИ

Цель работы: Изучить способы адресации в IP сетях.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия.

Общие сведения:

Адресация в IP-сетях

Типы адресов: физический (MAC-адрес), сетевой (IP-адрес) и символьный (DNS-имя)

Каждый компьютер в сети TCP/IP имеет адреса трех уровней:

- Локальный адрес узла, определяемый технологией, с помощью которой построена отдельная сеть, в которую входит данный узел. Для узлов, входящих в локальные сети, это MAC-адрес сетевого адаптера или порта маршрутизатора, например, 11-A0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизовано. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: старшие 3 байта — идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем.
- IP-адрес, состоящий из 4 байт, например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Network Information Center, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами. Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла — гибкое, и граница между этими полями может устанавливаться весьма произвольно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.
- Символьный идентификатор-имя, например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес, называемый также DNS-именем, используется на прикладном уровне, например, в протоколах FTP или telnet.

Три основных класса IP-адресов

IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме, и разделенных точками, например:

128.10.2.30 — традиционная десятичная форма представления адреса,

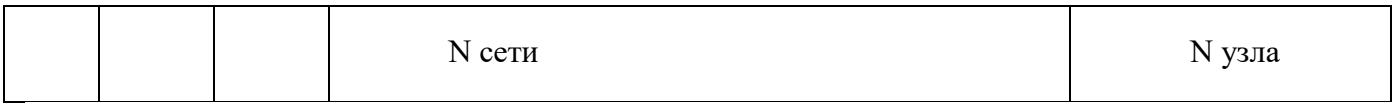
10000000 00001010 00000010 00011110 — двоичная форма представления этого же адреса.

Далее показана структура IP-адреса в зависимости от класса сети.

Класс А

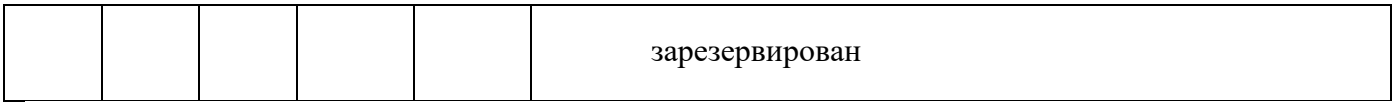
Класс B

Класс C



Класс D

Класс E



Адрес состоит из двух логических частей — номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса:

- Если адрес начинается с 0, то сеть относят к классу A, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса A имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей, о чем будет сказано ниже.) В сетях класса A количество узлов должно быть больше 2^{16}, но не превышать 2^{24}.
- Если первые два бита адреса равны 10, то сеть относится к классу B и является сетью средних размеров с числом узлов 2^{8} — 2^{16}. В сетях класса B под адрес сети и под адрес узла отводится по 16 бит, то есть по 2 байта.
- Если адрес начинается с последовательности 110, то это сеть класса C с числом узлов не больше 2^{8}. Под адрес сети отводится 24 бита, а под адрес узла — 8 бит.
- Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес — multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.
- Если адрес начинается с последовательности 11110, то это адрес класса E, он зарезервирован для будущих применений.

В таблице приведены диапазоны номеров сетей, соответствующих каждому классу сетей.

Класс	**Наименьший адрес**	**Наибольший адрес**
A	0.1.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0

D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Отображение символьных адресов на IP-адреса: служба DNS

DNS (Domain Name System) — это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet. Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. Спецификация DNS определяется стандартами RFC 1034 и 1035. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.

Протокол DNS является служебным протоколом прикладного уровня. Этот протокол несимметричен — в нем определены DNS-серверы и DNS-клиенты. DNS-серверы хранят часть распределенной базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Internet. Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес.

Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет — то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос, либо передать его другому DNS-серверу. Все DNS-серверы соединены иерархически, в соответствии с иерархией доменов сети Internet. Клиент опрашивает эти серверы имен, пока не найдет нужные отображения. Этот процесс ускоряется из-за того, что серверы имен постоянно кэшируют информацию, предоставляемую по запросам. Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов, для повышения надежности своей работы.

База данных DNS имеет структуру дерева, называемого доменным пространством имен, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.

Корень базы данных DNS управляется центром Internet Network Information Center. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны следовать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций используются следующие аббревиатуры:

- com — коммерческие организации (например, microsoft.com);
- edu — образовательные (например, mit.edu);
- gov — правительственные организации (например, nsf.gov);
- org — некоммерческие организации (например, fidonet.org);
- net — организации, поддерживающие сети (например, nsf.net).

Каждый домен DNS администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, а каждый из поддоменов имеет уникальное имя внутри своего домена. Имя домена может содержать до 63 символов. Каждый хост в сети Internet однозначно определяется своим *полным доменным именем (fully qualified domain name, FQDN)* ,

которое включает имена всех доменов по направлению от хоста к корню. Пример полного DNS-имени:

server.aics.acs.cctpu.edu.ru

Автоматизация процесса назначения IP-адресов узлам сети — протокол DHCP

IP-адреса могут назначаться администратором сети вручную. Это представляет для администратора утомительную процедуру. Ситуация усложняется еще тем, что многие пользователи не обладают достаточными знаниями для того, чтобы конфигурировать свои компьютеры для работы в интерсети и должны поэтому полагаться на администраторов.

Протокол *Dynamic Host Configuration Protocol (DHCP)* был разработан для того, чтобы освободить администратора от этих проблем. Основным назначением DHCP является динамическое назначение IP-адресов. Однако, кроме динамического, DHCP может поддерживать и более простые способы ручного и автоматического статического назначения адресов.

В ручной процедуре назначения адресов активное участие принимает администратор, который предоставляет DHCP-серверу информацию о соответствии IP-адресов физическим адресам или другим идентификаторам клиентов. Эти адреса сообщаются клиентам в ответ на их запросы к DHCP-серверу.

При автоматическом статическом способе DHCP-сервер присваивает IP-адрес (и, возможно, другие параметры конфигурации клиента) из пула (набора) наличных IP-адресов без вмешательства оператора. Границы пула назначаемых адресов задает администратор при конфигурировании DHCP-сервера. Между идентификатором клиента и его IP-адресом по-прежнему, как и при ручном назначении, существует постоянное соответствие. Оно устанавливается в момент первичного назначения сервером DHCP IP-адреса клиенту. При всех последующих запросах сервер возвращает тот же самый IP-адрес.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, что дает возможность впоследствии повторно использовать IP-адреса другими компьютерами. Динамическое разделение адресов позволяет строить IP-сеть, количество узлов в которой намного превышает количество имеющихся в распоряжении администратора IP-адресов.

Системные утилиты сетевой диагностики

Утилита ipconfig

Утилита ipconfig (IP configuration) предназначена для настройки протокола IP для операционной системы Windows. В данной работе эта утилита будет использоваться только для получения информации о соединении по локальной сети. Для получения этой информации выполните «Пуск» → «Выполнить» → cmd и в командной строке введите:

ipconfig /all

В разделе «Адаптер Ethernet Подключение по локальной сети» для данной работе будут необходимы поля «DHCP», «IP-адрес» и «DNS-серверы».

Утилита ping

Утилита ping (Packet Internet Groper) является одним из главных средств, используемых для отладки сетей, и служит для принудительного вызова ответа конкретной машины. Она позволяет проверять работу программ TCP/IP на удаленных машинах, адреса устройств в локальной сети, адрес и маршрут для удаленного сетевого устройства. В выполнении команды ping участвуют система маршрутизации, схемы разрешения адресов и сетевые шлюзы. Это утилита низкого уровня, которая не требует наличия серверных процессов на проверяемой машине, поэтому успешный результат при прохождении запроса вовсе не означает, что выполняются какие-либо сервисные программы высокого уровня, а говорит о том, что сеть находится в рабочем состоянии, питание проверяемой машины включено, и машина не отказала («не висит»).

В Windows утилита ping имеется в комплекте поставки и представляет собой программу, запускаемую из командной строки.

Запросы утилиты ping передаются по протоколу ICMP (Internet Control Message Protocol). Получив такой запрос, программное обеспечение, реализующее протокол IP у адресата, посылает эхо-ответ. Если проверяемая машина в момент получения запроса была загружена более приоритетной работой (например, обработкой и перенаправлением большого объема трафика), то ответ будет отправлен не сразу, а как только закончится выполнение более приоритетной задачи. Поэтому следует учесть, что задержа, рассчитанная утилитой ping, вызвана не только пропускной способностью канала передачи данных до проверяемой машины, но и загруженностью этой машины.

Эхо-запросы посылаются заданное количество раз (ключ -n). По умолчанию передается четыре запроса, после чего выводятся статистические данные.

Обратите внимание: *поскольку с утилиты ping начинается хакерская атака, некоторые серверы в целях безопасности могут не посылать эхо-ответы (например, www . microsoft . com). Не ждите напрасно, введите команду прерывания (CTRL + C).*

Формат команды: ping [-t][-a][-n][-l][-f][-i TTL][-v TOS]
[-r][][имя машины][[-j списокУзлов]|[-k списокУзлов]][-w]

Параметры утилиты ping

Ключи	Функции
-t	Отправка пакетов на указанный узел до команды прерывания
-a	Определение имени узла по IP-адресу
-n	Число отправляемых запросов
-l	Размер буфера отправки
-f	Установка флага, запрещающего фрагментацию пакета
-i TTL	Задание времени жизни пакета (поле «Time To Live»)

На практике большинство опций в формате команды можно опустить, тогда в командной строке может быть: ping имя узла (для зацикливания вывода информации о соединении используется опция –t; для вывода информации n-раз используется опция –n количество раз).

Пример :

ping –n 20 peak.mountin.net

Обмен пакетами с peak.mountin.net [207.227.119.2] по 32 байт:
Превышен интервал ожидания для запроса.
Ответ от 207.227.119.2: число байт=32 время=734мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=719мс TTL=231

Ответ от 207.227.119.2: число байт=32 время=688мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=704мс TTL=231
Превышен интервал ожидания для запроса.
Ответ от 207.227.119.2: число байт=32 время=719мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=1015мс TTL=231
Превышен интервал ожидания для запроса.
Ответ от 207.227.119.2: число байт=32 время=703мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=688мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=782мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=688мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=688мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=688мс TTL=231
Превышен интервал ожидания для запроса.
Ответ от 207.227.119.2: число байт=32 время=687мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=735мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=672мс TTL=231
Ответ от 207.227.119.2: число байт=32 время=704мс TTL=231

Статистика Ping для 207.227.119.2:
Пакетов: отправлено = 20, получено = 16, потеряно = 4 (20% потерь),
Приблизительное время передачи и приема:
наименьшее = 672мс, наибольшее = 1015мс, среднее = 580мс

Пример определения имени узла по IP-адресу
ping –a 194.67.57.26
Обмен пакетами с mail.ru [194.67.57.26] по 32 байт: …

Утилита tracert

Утилита tracert позволяет выявлять последовательность маршрутизаторов, через которые проходит IP-пакет на пути к пункту своего назначения.

Формат команды: tracert имя_машины

имя_машины может быть именем узла или IP-адресом машины. Выходная информация представляет собой список машин, начиная с первого шлюза и заканчивая пунктом назначения.

Пример:
tracert peak.mountin.net
Трассировка маршрута к peak.mountin.net [207.227.119.2]
с максимальным числом прыжков 30:

№	Пакет 1	Пакет 2	Пакет 3	DNS-имя узла и (или) его IP-адрес
1	<10 мс	<10 мс	<10 мс	SLAVE [192.168.0.1]
2	<10 мс	<10 мс	<10 мс	gw.b10.tpu.edu.ru [195.208.164.2]

№	Пакет 1	Пакет 2	Пакет 3	DNS-имя узла и (или) его IP-адрес
3	<10 мс	<10 мс	<10 мс	195.208.177.62
4	<10 мс	<10 мс	<10 мс	news.runnet.tomsk.ru [195.208.160.4]
5	<10 мс	<10 мс	16 ms	ra.cctpu.tomsk.su [195.208.161.34]
6	781 ms	563 ms	562 ms	spb-2-gw.runnet.ru [194.85.33.9]
7	547 ms	594 ms	578 ms	spb-gw.runnet.ru [194.85.36.30]
8	937 ms	563 ms	562 ms	20.201.atm0-201.ru-gw.run.net [193.232.80.105]
9	1125 ms	563 ms	547 ms	fi-gw.nordu.net [193.10.252.41]
10	906 ms	1016 ms	578 ms	s-gw.nordu.net [193.10.68.41]
11	844 ms	828 ms	610 ms	dk-gw2.nordu.net [193.10.68.38]
12	578 ms	610 ms	578 ms	sl-gw10-cop-9-0.sprintlink.net [80.77.65.25]
13	610 ms	968 ms	594 ms	sl-bb20-cop-8-0.sprintlink.net [80.77.64.37]
14	641 ms	672 ms	656 ms	sl-bb21-msq-10-0.sprintlink.net [144.232.19.29]
15	671 ms	704 ms	687 ms	sl-bb21-nyc-10-3.sprintlink.net [144.232.9.106]
16	985 ms	703 ms	765 ms	sl-bb22-nyc-14-0.sprintlink.net [144.232.7.102]
17	719 ms	734 ms	688 ms	144.232.18.206
18	891 ms	703 ms	734 ms	p1-0.nycmny1-nbr1.bbnplanet.net [4.24.8.161]
19	719 ms	985 ms	703 ms	so-6-0-0.chcgil2-br2.bbnplanet.net [4.24.4.17]
20	688 ms	687 ms	703 ms	so-7-0-0.chcgil2-br1.bbnplanet.net [4.24.5.217]
21	719 ms	703 ms	672 ms	p1-0.chcgil2-cr9.bbnplanet.net [4.24.8.110]

№	Пакет 1	Пакет 2	Пакет 3	DNS-имя узла и (или) его IP-адрес
22	687 ms	719 ms	687 ms	p2-0.nchicago2-cr2.bbnplanet.net [4.0.5.242]
23	781 ms	703 ms	672 ms	p8-0-0.nchicago2-core0.bbnplanet.net [4.0.6.2]
24	672 ms	703 ms	687 ms	fa0.wcnet.bbnplanet.net [207.112.240.102]
25	734 ms	687 ms	688 ms	core0-s1.rac.cyberlynk.net [209.100.155.22]
26	1188 ms	*	890 ms	peak.mountin.net [207.227.119.2]

Трассировка завершена.

Пакеты посылаются по три на каждый узел. Для каждого пакета на экране отображается величина интервала времени между отправкой пакета и получением ответа. Символ * означает, что ответ на данный пакет не был получен. Если узел не отвечает, то при превышении интервала ожидания ответа выдается сообщение «Превышен интервал ожидания для запроса». Интервал ожидания ответа может быть изменен с помощью опции –w команды tracert.

Команда tracert работает путем установки поля времени жизни (числа переходов) исходящего пакета таким образом, чтобы это время истекало до достижения пакетом пункта назначения. Когда время жизни истечет, текущий шлюз отправит сообщение об ошибке на машину-источник. Каждое приращение поля времени жизни позволяет пакету пройти на один маршрутизатор дальше.

Примечание:

Для вывода информации в файл используйте символ перенаправления потока вывода «>». Данный символ справедлив и для утилит ping и tracert .

Пример:

tracert 195.208.164.1 > tracert.txt

Отчет о трассировке маршрута до указанного узла будет помещен в файл tracert.txt.

Задание

Отчёт по практической работе необходимо оформить в MS Word. Файл с отчетом необходимо назвать в следующем формате: «НОМЕР_ПРАКТИЧЕСКОЙ ГРУППА ФИО», например: «1 41П Иванов А.С. «. Поместить изображение текущего окна в отчёт можно следующим способом: нажмите ALT+PrintScreen, перейдите в редактор и нажмите CTRL+V. Скопировать текст из окна командной строки можно следующим образом: выделите необходимый текст с помощью мыши и нажмите на выделенном участке правой кнопкой мыши, затем перейдите в текстовый редактор и нажмите Ctrl+V. Список адресов узлов для всех вариантов приведён в 4-ом пункте.

С помощью утилиты ipconfig определить IP адрес и физический адрес основного сетевого интерфейса компьютера, IP адрес шлюза, IP адреса DNS-серверов и используется ли DHCP.. Результаты представить **в виде таблицы** .

Проверить состояние связи с любыми двумя узлами (работоспособными) в соответствии с вариантом задания. Число отправляемых запросов должно составлять не менее 20. В качестве результата отразить для каждого из исследуемых узлов **в виде табилицы** :

a. процент потерянных пакетов;
b. среднее время приема-передачи;
c. количество маршрутизаторов (с учетом шлюза) до опрашиваемого узла;
d. IP адрес узла.
e. класс сети, к которой принадлежит данный узел;
f. имя узла, полученное по IP-адресу узла.

В отчёте необходимо пояснить, как были определены значения.

Произвести трассировку двух работоспособных узлов в соответствии с вариантом задания. Результаты запротоколировать в таблице.

№ узла	Время прохождения пакета №1	Время прохождения пакета №2	Время прохождения пакета №3	среднее вермя прохождения пакета	DNS-имя маршрутизатора	IP-адрес маршрутизатора

Если значения времени прохождения трёх пакетов отличаются более, чем на 10 мс, либо если есть потери пакетов, то для соответствующих узлов среднее время прохождения необходимо определять с помощью утилиты ping по 20 пакетам. . По результатам таблицы в отчете привести **график** изменения среднего времени прохождения пакета. В отчёте привести одну копию окна с результатами команды tracert. Для каждого опрашиваемого узла определить участок сети между двумя соседними маршрутизаторами, который характеризуется наибольшей задержкой при пересылке пакетов. Для найденных маршрутизаторов с помощью сервиса Whois определить название организации и контактные данные (тел., email). Полученную информацию необходимо указать в отчёте.

ВАРИАТЫ ЗАДАНИЙ

1	www.informika.ru www.rfbr.ru www.ras.ru
2	www.gpntb.ru www.rusmedserv.com www.nsc.ru
3	www.chemnet.ru www.rsl.ru www.philosophy.ru
4	www.rbc.ru www.membrana.ru www.mrsu.ru
5	www.viniti.ru www.sostav.ru www.ioffe.ru
6	www.fegi.ru www.elibrary.ru www.extech.ru
7	www.ripn.net www.shpl.ru sai.msu.su

8	www.scsml.rssi.ru www.sscc.ru www.nlr.ru
9	web.ru www.kamaz.ru www.rulex.ru
10	www.jinr.ru uic.nnov.ru www.ruthenia.ru
11	www.tractor.ru www.rsci.ru www.astronet.ru
12	www.keldysh.ru www.fom.ru www.inauka.ru
13	www.gramota.ru www.csa.ru www.bionet.nsc.ru
14	www.inp.nsk.su www.scientific.ru www.med2000.ru
15	www.gpi.ru iki.cosmos.ru www.spsl.nsc.ru
16	www.uiggm.nsc.ru hist.dcn-asu.ru www.cemi.rssi.ru
17	psychology.net.ru www.irex.ru www.medlinks.ru
18	www.viniti.ru www.sostav.ru www.gramota.ru
19	www.sscc.ru www.nlr.ru www.fom.ru
20	uic.nnov.ru www.ruthenia.ru www.rsl.ru

Контрольные вопросы:

1. Что такое адрес IP?
2. Что такое MAC адрес?
3. Что такое маска подсети?
4. На какие классы делятся сети IP?
5. Даны адрес узла и маска подсети. Что здесь не верно? Адрес узла в частной сети 131.107.2.100, маска подсети 255.255.255.0.
6. Дана маска подсети 255.255.0.0. К какому классу относится сеть? Каково максимальное количество узлов в сети?
7. Дана маска подсети 255.255.255.0. Число узлов в сети 255. Что здесь не верно?
8. Дан IP адрес узла в частной сети 221.101.2.150. Задайте правильную маску подсети.
9. Перечислите утилиты, которые можно использовать для поиска неисправностей в настройках TCP/IP. Каковы их возможности.
10. Утилита IPConfig. Назначение, параметры, результаты применения.

11. Утилита Ping. Назначение, параметры, результаты применения.
12. Порядок совместного применения утилит IPConfig и Ping.
13. Назначение утилиты ARP.

Практическая работа № 18

КОМАНДЫ VLAN НА ОСНОВЕ ПОРТОВ И МЕТОК 802. IQ.

Цель работы: изучить виртуальную локальную сеть (Virtual Local Area Netwrok, VLAN).

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия.

Общие сведения:

Виртуальная локальная сеть (Virtual Local Area Netwrok, VLAN) представляет собой коммутируемый сегмент сети, который логически отделен по выполняемым функциям, рабочим группам или приложениям, вне зависимости от физического расположения пользователей. Виртуальные локальные сети имеют все свойства физических локальных сетей, но вы можете группировать рабочие станции, даже если они физически расположены не в одном сегменте. Любой порт коммутатора может принадлежать к VLAN, и одноадресный, широковещательный и групповой трафик передается только рабочим станциям принадлежащим данной VLAN. Каждый VLAN рассматривается как логическая сеть, т.е. пакеты, предназначенные станциям, которые не принадлежат данной VLAN должны передаваться через маршрутизатор или мост. Таким образом, с помощью виртуальных сетей решается проблема ограничений при передаче широковещательных пакетов и вызываемых ими следствий, которые существенно снижают производительность сети, вызывают широковещательные штормы.

Сети, построенные с применением VLAN, обладают следующими преимуществами:

- Гибкость внедрения. VLAN является эффективным способом группировки сетевых устройств (рабочие станции, сервера, сетевые принтеры, МФУ) в виртуальные рабочие группы, несмотря на их размещение в сети;
- VLAN обеспечивает возможность контроля широковещательных сообщений, что увеличивает полосу пропускания доступную для пользователя;
- VLAN позволяет усилить безопасность сети, определив с помощью фильтров, настроенных на коммутаторе или маршрутизаторе политику взаимодействия пользователей из разных виртуальных сетей (в простейшем случае сетевые устройства из одного VLAN в другой VLAN не имеют доступа на канальном уровне, что позволяет бороться с различными типами сетевых атак, например ARP-spoofing).

Существует несколько способов (типов) организации VLAN:

- VLAN на базе портов (Port-based) – каждый порт коммутатора назначается в определенную VLAN и любое сетевое устройство подключенное в данный порт, будет находиться в назначенной виртуальной сети;
- VLAN на основе MAC-адресов (MAC-based) – членство в VLAN’е основывается на MAC-адресе рабочей станции. В этом случае на коммутаторе необходимо создать привязку MAC-адресов всех устройств к VLAN;
- VLAN на основе протокола (Protocol-based) – данные 3-4 уровня в заголовке пакета используются чтобы определить членство в VLAN’е;
- VLAN на основе меток (IEEE 802.1q) – поле о принадлежности к VLAN, интегрируется в структуру кадра, что позволяет передавать данную информацию по сети. Преимуществом

является гибкость настройки, использование не только на одном коммутаторе, но и в пределах всей коммутируемой сети, возможность использовать оборудование разных производителей при организации сети. Данный тип организации VLAN используется чаще остальных методов.

Существуют два подхода назначения порта в определѐнный VLAN:

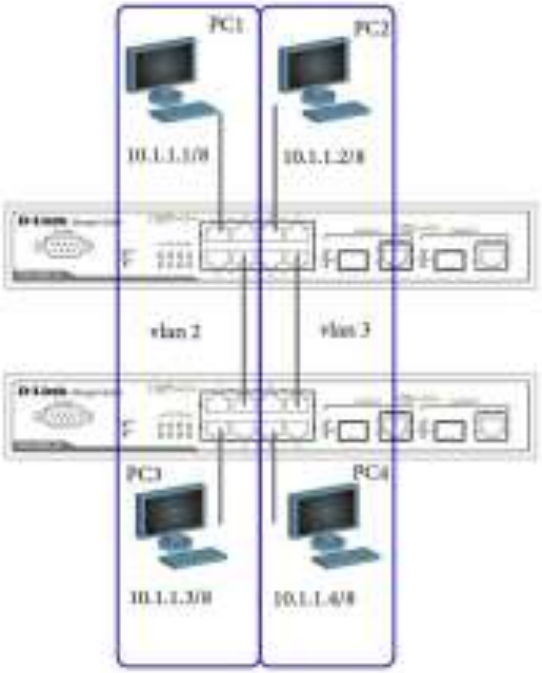
- Статическое назначение – когда принадлежность порта VLAN задаѐтся администратором в процессе настройки;
- Динамическое назначение – когда принадлежность порта VLAN определяется в ходе работы коммутатора с помощью процедур, описанных в специальных стандартах, таких, например, как 802.1x. При использовании 802.1x для того чтобы получить доступ к порту коммутатора, пользователь проходит аутентификацию на RADIUS-сервере. По результатам аутентификации порт коммутатора размещается в тот или иной VLAN.

Введем основные определения IEEE 802.1q:

- Tag (Тег) – дополнительное поле данных 4 байта, содержащее информацию о VLAN (vlan id/12bit, поле приоритета/3bit, поле обозначения типа сети/1bit), добавляется в кадр;
- Tagging (Вставка тега в кадр) – процесс добавления информации (тега) о принадлежности к VLAN в заголовок кадра;
- Untagging (Удаление тега из кадра) – процесс извлечения информации IEEE 802.1q из заголовка кадра;
- Ingress port (Входной порт) – порт коммутатора, на который поступают кадры, и принимается решение о принадлежности к VLAN;
- Egress port (Выходной порт) – порт коммутатора, с которого кадры передаются на другие сетевые устройства (коммутаторы, рабочие станции) и на нем соответственно принимается решение о маркировке кадра.

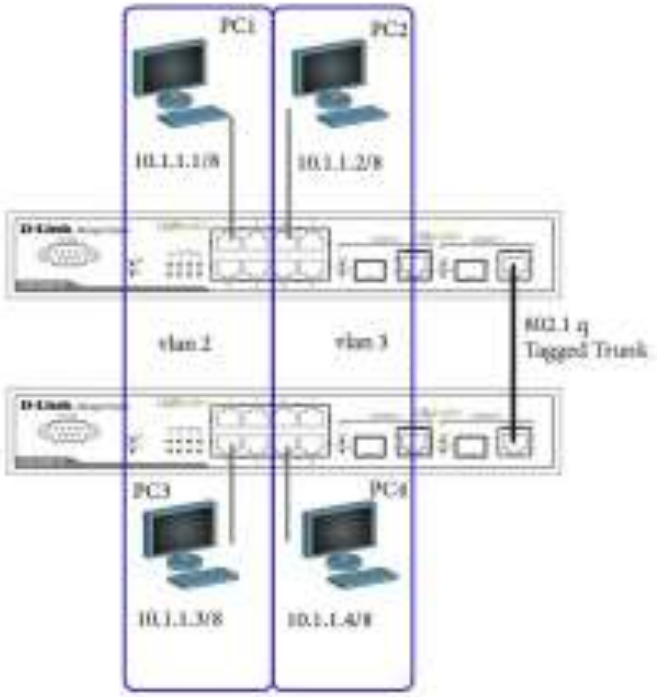
Любой порт коммутатора может быть настроен как «tagged» или «untagged». Функция «untagged» позволяет работать с такими сетевыми устройствами VLAN, которые не понимают меток в заголовках кадров Ethernet. Функция «tagged» позволяет настраивать VLAN между несколькими коммутаторами, передавать информацию о нескольких VLAN через данные порты коммутаторов, подключать сетевые устройства, понимающие IEEE 802.1q (например, сервера с сетевыми интерфейсами с поддержкой 802.1q), обеспечивать возможность создания сложных сетевых инфраструктур.

Настройка VLAN, основанной на портах.



Удалите порты из VLAN по умолчанию для использования в других VLAN
config vlan default delete 1-10
Создайте VLAN v2 и v3, назначьте нетэгированные порты соответствующим VLAN
create vlan v2 tag 2
config vlan v2 add untagged 1-4
create vlan v3 tag 3
config vlan v3 add untagged 5-8
Проверьте настройки VLAN
show vlan
Повторите процедуру настройки для второго коммутатора
Проверьте доступность узлов командой ping
- от PC1 к PC3 _____
- от PC2 к PC4 _____
- от PC1 к PC2 & PC4 _____
- от PC2 к PC1 & PC3 _____

Настройка VLAN на основе меток 802.1q



Перед выполнением данной процедуры необходимо сбросить настройки коммутатора к заводским командой reset config
Удалите порты из VLAN по умолчанию для использования в других VLAN
config vlan default delete 1-10
Создайте VLAN v2 и v3, назначьте нетэгированные порты соответствующим VLAN
create vlan v2 tag 2
config vlan v2 add untagged 1-4
config vlan v2 add tagged 10
create vlan v3 tag 3
config vlan v3 add untagged 5-8
config vlan v3 add tagged 10
Проверьте настройки VLAN
show vlan
Повторите процедуру настройки для второго коммутатора
Проверьте доступность узлов командой ping
- от PC1 к PC3 _____
- от PC2 к PC4 _____
- от PC1 к PC2 & PC4 _____
- от PC2 к PC1 & PC3 _____

Оптимизация конфигурирования коммутаторов с большим количеством VLAN

Перед выполнением данной процедуры необходимо сбросить настройки коммутатора к заводским командой reset config
Удалите порты из VLAN по умолчанию для использования в других VLAN
config vlan default delete 1-10

Создайте двадцать VLAN с тегами с 2 по 21 create vlan vlanid 2-21
Примечание: При создании VLAN имена присваиваются по шаблону (VLAN x , где x – тег создаваемого
VLAN)
Добавьте теггированные порты в несколько VLAN, включите функции объявления
config vlan vlanid 2-21 add tagged 1-10 advertisement enable
Проверьте настройки VLAN show vlan
Измените имя VLAN и добавьте untagged порты:
config vlan vlanid 11 name SALE add untagged 1-8
Удалите порты из нескольких VLAN
config vlan vlanid 2-21 delete 1-7
Проверьте настройки VLAN show vlan
Удалите несколько VLAN delete vlan vlanid 2-21
Проверьте корректность выполнения команды show vlan

Контрольные вопросы:

1. Преимущества сетей, построенных с применением VLAN.
2. Способы организации VLAN.
3. Настройка VLAN
4. Настройка VLAN на основе меток 802.1q

Практическая работа № 19-20

ИЗУЧЕНИЕ ПРИНЦИПА РАБОТЫ МАРШРУТИЗАТОРОВ

Цель работы: изучить виды маршрутизаторов, их классификацию.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия.

Ход работы:

1. Изучить виды маршрутизаторов:

1.1 Многопротокольные маршрутизаторы концептуально напоминают мосты с той существенной разницей, что они работают на сетевом уровне. Как и любой маршрутизатор, они берут пакет с одной линии и передают его на другую, но при этом линии принадлежат к разным сетям и используют разные протоколы (например, IP и IPX). Кроме того, сетевые устройства типа моста/маршрутизатора (brouter или bridge/router) работают в нормальном режиме как многопротокольные маршрутизаторы, а при получении пакета с неизвестным сетевым протоколом обрабатывают его как мост. Другие устройства со сходным названием "маршрутизирующий мост" (routing bridge) принадлежат к устройствам второго уровня и упоминаются здесь лишь из-за причастия routing. Они работают как мосты, но при этом поддерживают некоторые функции третьего уровня для оптимизации передачи данных.

1.2 Маршрутизаторы с интеграцией услуг гарантируют приоритетному трафику, в частности трафику реального времени, своевременную доставку. Они поддерживают протокол RSVP для резервирования таких ресурсов, как пропускная способность и буферы в очереди.

1.3 Коммутаторы третьего уровня, по сути, также являются маршрутизаторами, причем пакетные коммутаторы (Packet-by-Packet Switch) - на самом деле обычные, только быстрые маршрутизаторы.

2. Изучить типы маршрутизаторов:

2.1 Внутренний маршрутизатор (internal router) — маршрутизатор все интерфейсы, которого принадлежат одной зоне. У таких маршрутизаторов только одна база данных состояния каналов.

2.2 Пограничный маршрутизатор (area border router, ABR) — соединяет одну или больше зон с магистральной зоной и выполняет функции шлюза для межзонального трафика. У пограничного маршрутизатора всегда хотя бы один интерфейс принадлежит магистральной зоне. Для каждой присоединенной зоны маршрутизатор поддерживает отдельную базу данных состояния каналов.

2.3 Магистральный маршрутизатор (backbone router) — маршрутизатор, у которого всегда хотя бы один интерфейс принадлежит магистральной зоне. Внутренний маршрутизатор интерфейсы, которого принадлежат нулевой зоне, также является магистральным.

2.4 Пограничный маршрутизатор автономной системы (AS boundary router, ASBR) — обменивается информацией с маршрутизаторами принадлежащими другим автономным системам. Пограничный маршрутизатор автономной системы может находиться в любом месте автономной системы и быть внутренним, пограничным или магистральным маршрутизатором.

3. Классификация маршрутизаторов по областям применения

По областям применения маршрутизаторы делятся на несколько классов.

3.1 Магистральные маршрутизаторы (backbone routers) предназначены для построения центральной сети корпорации. Центральная сеть может состоять из большого количества локальных сетей, разбросанных по разным зданиям и использующих самые разнообразные сетевые технологии, типы компьютеров и операционных систем. Магистральные маршрутизаторы - это наиболее мощные устройства, способные обрабатывать несколько сотен тысяч или даже несколько миллионов пакетов в секунду, имеющие большое количество интерфейсов локальных и глобальных сетей. Поддерживаются не только среднескоростные интерфейсы глобальных сетей, такие как T1/E1, но и высокоскоростные, например, ATM или SDH со скоростями 155 Мбит/с или 622 Мбит/с. Чаще всего магистральный маршрутизатор конструктивно выполнен по модульной схеме на основе шасси с большим количеством слотов - до 12-14. Большое внимание уделяется в магистральных моделях надежности и отказоустойчивости маршрутизатора, которая достигается за счет системы терморегуляции, избыточных источников питания, заменяемых «на ходу» (hot swap) модулей, а также симметричного муль-типроцессирования. Примерами магистральных
маршрутизаторов могут служить маршрутизаторы Backbone Concentrator Node (BCN) компании Nortel Networks (ранее Bay Networks), Cisco 7500, Cisco 12000.

3.2 Маршрутизаторы региональных отделений соединяют региональные отделения
между собой и с центральной сетью. Сеть регионального отделения, так же как и центральная сеть, может состоять из нескольких локальных сетей. Такой маршрутизатор обычно представляет собой некоторую упрощенную версию магистрального маршрутизатора. Если он выполнен на основе шасси, то количество слотов его шасси меньше: 4-5. Возможен также конструктив с фиксированным количеством портов. Поддерживаемые интерфейсы локальных и глобальных сетей менее скоростные. Примерами маршрутизаторов региональных отделений могут служить маршрутизаторы BLN, ASN компании Nortel Networks, Cisco 3600, Cisco 2500, NetBuilder II компании 3Com. Это наиболее обширный класс выпускаемых маршрутизаторов, характеристики которых могут приближаться к характеристикам магистральных маршрутизаторов, а могут и опускаться до характеристик маршрутизаторов удаленных офисов.

3.3 Маршрутизаторы удаленных офисов соединяют, как правило, единственную локальную сеть удаленного офиса с центральной сетью или сетью регионального отделения по глобальной связи. В максимальном варианте такие маршрутизаторы могут поддерживать и два интерфейса локальных сетей. Как правило, интерфейс локальной сети - это Ethernet 10 Мбит/с, а интерфейс глобальной сети - выделенная линия со скоростью 64 Кбит/с, 1,544 или 2 Мбит/с. Маршрутизатор удаленного офиса может поддерживать работу по коммутируемой телефонной линии в качестве резервной связи для выделенного канала. Существует очень большое количество типов маршрутизаторов удаленных офисов. Это объясняется как массовостью потенциальных потребителей, так и специализацией такого типа устройств, проявляющейся в поддержке одного конкретного типа глобальной связи. Например, существуют маршрутизаторы, работающие только по сети ISDN, существуют модели только для аналоговых выделенных линий и т. п. Типичными представителями этого класса являются маршрутизаторы Nautika компании Nortel Networks, Cisco 1600, Office Connect компании 3Com, семейство Pipeline компании Ascend.

3.4 Маршрутизаторы локальных сетей (коммутаторы 3-го уровня) предназначены
для разделения крупных локальных сетей на подсети. Основное требование, предъявляемое к ним, - высокая скорость маршрутизации, так как в такой конфигурации отсутствуют низкоскоростные порты, такие как модемные порты 33,6 Кбит/с или цифровые порты 64 Кбит/с. Все порты имеют

скорость по крайней мере 10 Мбит/с, а многие работают на скорости 100 Мбит/с. Примерами коммутаторов 3-го уровня служат коммутаторы CoreBuilder 3500 компании 3Com, Accelar 1200 компании Nortel Networks, Waveswitch 9000 компании Plaintree, Turboiron Switching Router компании Foudry Networks.

3.5 В зависимости от области применения маршрутизаторы обладают различными основными и дополнительными техническими характеристиками.

Контрольные вопросы:

1. Маршрутизатор – понятие, классы.
2. Назначение магистрального маршрутизатора.
3. Перечислить виды маршрутизаторов и дать характеристику каждому.

Практическая работа № 21-22

ИЗУЧЕНИЕ СИСТЕМЫ УПРАВЛЕНИЯ СЕТЕВЫМ ОБОРУДОВАНИЕМ. ПРОТОКОЛ SNMP.

Цель работы: изучить задачи протокола SNMP.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия.

Общие сведения:

Основная задача при управлении компьютерными сетями – автоматизировать процесс конфигурации и мониторинга параметров сети. На сегодня существует множество моделей и систем сетевого управления. Эта статья должна помочь читателю разобраться во всем этом разнообразии.
Обычно, система сетевого управления представляет собой прикладную программу высокого уровня, которая использует один из стандартных протоколов сетевого управления.(SimpleNetworkManagementProtocol(SNMP) или ommon ManagementInformationProtocol (CMIP)). CMIP применяется в телекоммуникационных сетях, где необходимы все доступные возможности управления сетями, в то время как SNMP используется в локальных и корпоративных сетях, где достаточно минимума данных.
Информационная структура большинства компаний представляет собой сложную
разнородную сеть, которая состоит из разнообразного программного и аппаратного обеспечения многих производителей, а интеллектуальная система управления сетевым оборудованием способна значительно упростить процесс управления телекоммуникационным оборудованием.
Основными задачами системы управления являются:

1. обеспечение высокой производительности сети;
2. обеспечение удобной среды для управления сетевыми ресурсами;
3. сбор информации о состоянии всех сетевых устройств;
4. анализ и хранение информации о состоянии всех сетевых устройств;
5. прогнозирование возможных сбоев в работе сети.

ПРОТОКОЛЫ УПРАВЛЕНИЯ СЕТЯМИ

Системы управления сетями используют один из стандартных протоколов (SNMPили CMIP).
Система, основанная на протоколе SNMP, включает в себя:

1.протокол взаимодействия агента и менеджера;

2.язык описания моделей MIB и сообщений SNMP — язык абстрактной синтаксической нотации ASN.1

3.ограниченное количество моделей MIB (MIB-I, MIB-II, RMON, …)

Изначально, протокол SNMP и база SNMPMIB разрабатывались как временное решение для управления маршрутизаторами Интернет. Но решение оказалось настолько простым, эффективным и гибким, что и по сей день, оно находит повсеместное применение при управлении сетевым оборудованием.
С помощью протокола SNMP можно оценить производительность сетевых устройств, количество свободных ресурсов, загруженность и получить множество других полезных характеристик, необ-

ходимых для управления сетевыми устройствами. SNMP – протокол типа “запрос-ответ” т.е на каждый запрос от менеджера должен быть передан ответ от агента.

Протокол SNMP обладает достаточно небольшим набором команд:

1.Команда ‘Get-request’ применяется менеджером для получения от агента значения объекта по имени;

2.Команда ‘GetNext-request’ применяется менеджером для получения значения следующего объекта при последовательном обходе MIB;

3.При помощи команды ‘Get-response’ агент SNMP передает менеджеру результаты вышеперечисленных команд;

4.Команда ‘Set’ устанавливает значения объекта;

5.Команда ‘Trap’ сообщает менеджеру о возникновении какой-либо нестандартной ситуации;

6.В SNMPv.2 добавлена команда ‘GetBulk’, при помощи которой менеджер может получить несколько значений переменных за один запрос.

Сама структура MIB имеет стандартизированную структуру, которой придерживаются все фирмы-производители сетевого оборудования. Для специфических параметров сетевого оборудования используются специальные частные (private) поддеревья.

В протоколе SNMP присутствует агент, который обрабатывает данные, полученные из MIB, и передает их менеджеру, на управляющей станции сети. В результате управляющие станции обладают всей информацией, которая им необходима из MIB. главное достоинство протокола SNMP заключается в его простоте и в том, что он поддерживается почти всеми производителями сетевого оборудования.

Из-за своей простоты, протокол SNMP обладает еще и некоторыми недостатками:

1.при опросе происходит загрузка сети сервисной информацией, что ухудшает пропускную способность сети в целом;

2.данные практически не шифруются при передаче;

3.Так как вкачестве транспортного протокола используется протокол низкого уровня (UDP), нет возможности подтвердить доставку информации.

В следующей таблице представлены наиболее важные характеристики самых распространенных платформ управления:

	HP OpenView Network Node Manager	IBM Tivoli NetView	Sun Solstice Domain Manager
Определение имени хоста по его адресу через сервер DNS	+	+	+
Возможность модификации присвоенного имени хоста	+	+	+
Распознавание сетевых топологий	Любые сети, работающие по TCP/IP	Распознавание по интерфейсам устройств	Ethernet, Token Ring, FDDI, распределенные сети
Поддержка баз данных	MicrosoftSQLServer, Oracle, интегрированные	DB2, Informix, Oracle, SQL, Sybase	Informix, Oracle, Sybase
Формат отчетов	Формат HTML,электронная почта	Формат HTML	Консоль
Поддерживаемые веб серверы	MicrosoftIIS,Apache	WebSphere® Application Server, BEA WebLogic Application	

Контрольные вопросы:

1. Достоинства и недостатки SNMP.
2. Основные задачи системы управления.
3. Набор команд протокола SNMP.

Практическая работа № 23

ПРОТОКОЛ МАРШРУТИЗАЦИИ RIP.

Цель работы: изучить назначение протоколов маршрутизации.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия.

Общие сведения:

Интернет – это комбинация сетей, соединяемых с помощью маршрутизаторов.
Когда дейтаграмма идет от источника к пункту назначения, она, вероятнее всего, проходит много маршрутизаторов, пока достигает маршрутизатора, закрепленного за сетью пункта назначения. Маршрутизатор получает пакет от сети и передает его другой сети. Маршрутизатор обычно закрепляется за несколькими сетями. Когда он получает пакет, он должен решить две задачи:

1. к какой сети он должен его передать;
2. по какому пути.

Последнее решение основано на выборе оптимального пути. Какой доступный путь является оптимальным путем? Это обычно определяется метрикой. Метрика – это
условная стоимость передачи по сети. Полное измерение конкретного маршрута равно сумме метрик сетей, которые включают в себя маршрут. Маршрутизатор выбирает маршрут с наименьшей метрикой. Метрика назначается для интерфейса сети в зависимости от типа протокола. Некоторые простые протоколы, подобно протоколу маршрутной информации (RIP – Routing Information Protocol), рассматривают все сети как одинаковые. Тогда стоимость прохождения через каждую сеть — одна и та же, и для определения метрики подсчитываются участки. Так, если пакет, чтобы достигнуть конечного пункта, проходит через 10 сетей, полная стоимость составляет 10 участков.
Другие протоколы, такие как "первоочередное открытие наикратчайших путей" (OSPF — Open Shortest Path First), позволяют администратору назначить стоимость для передачи через сеть, основанную на типе требуемого обслуживания. Маршрут через сеть может иметь различную стоимость (метрику). Например, если для типа сервиса желательна максимальная производительность, спутниковый канал имеет меньшую метрику, чем оптическая линия. С другой стороны, если типу сервера желательна минимальная задержка, оптическая линия имеет меньшую метрику, чем спутниковый канал. OSPF позволяет каждому маршрутизатору иметь таблицу последовательностей маршрутов, основанную на требуемом типе сервиса.
Другие протоколы определяют метрику различно. В протоколе пограничной маршрутизации (BGP — Border Gateway Protocol) критерий — это политика, которую может устанавливать администратор. Политика — это принцип, по которому определяется путь.
В любой метрике маршрутизатор должен иметь таблицы маршрутизации, чтобы консультироваться при дальнейшей передаче пакета. Таблица маршрутизации задает оптимальный путь для пакета. Таблица может быть либо статическая, либо динамическая. Статическая таблица — одна из тех, которые часто не меняются. Динамическая таблица — одна из тех, которая обновляется автоматически, когда имеются изменения где-либо в Интернете.
Сегодня Интернет нуждается в динамических таблицах. Таблицы нужно обновлять по мере появления изменений в Интернете. Например, их нужно обновить, когда маршрут вышел из строя, или они должны быть обновлены всякий раз, когда создается лучший маршрут.

Протоколы маршрутизации созданы для отображения требований таблиц динамической маршрутизации. Протокол маршрутизации— комбинация правил и процедур, которые позволяют в Интернете маршрутизаторам информировать друг друга об изменениях. Протоколы маршрутизации также включают процедуры для комбинирования информации, полученной от других маршрутизаторов.

Внутренняя и внешняя маршрутизация

Сегодня Интернет — громадная сеть, так что один протокол маршрутизации не может обрабатывать задачу обновления таблиц всех маршрутизаторов. По этой
причине Интернет разделяется на автономные системы. Автономная система (Autonomous System – AS) — группа сетей и маршрутизаторов под управлением одного администратора. Маршрутизация внутри автономной системы отнесена к внутренней маршрутизации. Маршрутизация между автономными системами отнесена к внешней маршрутизации. Каждая автономная система может выбрать протокол внутренней маршрутизации для того, чтобы обрабатывать маршрутизацию внутри автономной системы.

Однако для обработки маршрутизации между автономными системами выбирается только один-протокол маршрутизации.

Разработано несколько внутренних и внешних протоколов. В этой лекции мы коснемся только наиболее популярных из них — внутренних протоколов RIP и OSPF и одного внешнего протокола BGP. RIP и OSPF используются для обновления таблиц маршрутизации внутри автономной системы. Протокол BGP применяется в обновлении таблиц маршрутизации для маршрутизаторов, которые объединяют вместе автономные системы.

Протокол маршрутной информации (RIP)

Протокол маршрутной информации (RIP – Routing Information Protocol) — внутренний протокол маршрутизации, используется внутри автономной системы. Это очень простой протокол, основанный на применении дистанционного вектора маршрутизации. В этом разделе сначала рассмотрим принцип дистанционного вектора маршрутизации, так как он применяется в RIP, азатем обсудим сам протокол RIP.

Вектор расстояния маршрутизации

Используя вектор расстояния маршрутизации, каждый маршрутизатор периодически делится своей информацией о входах в Интернет со своими соседями. Ниже приводятся три основных принципа этого процесса, для того чтобы понять, как работает алгоритм.

1. Распределение информации о входе в автономную систему. Каждый маршрутизатор распределяет информацию о входе соседним автономным системам. Вначале эта информация может быть не подробной. Однако объем и качество информации не играют роли. Маршрутизатор посылает, во всяком случае, все что имеет.
2. Распределение только соседям. Каждый маршрутизатор посылает свою информацию только к соседям. Он посылает информацию, которую получает через все интерфейсы.
3. Распределение через регулярные интервалы. Каждый маршрутизатор посылает свою информацию соседней автономной системе через фиксированные интервалы, например, каждые 30 с.

Таблицы маршрутизации

Каждый маршрутизатор хранит таблицы маршрутизации, имеющие один вход для каждой сети назначения, которую маршрутизатор зарегистрировал. Вход содержит:

- адрес сети пункта назначения,
- кратчайший путь для того, чтобы достичь пункта назначения, отсчитываемый в участках,
  - следующий участок (следующий маршрутизатор), к которому должен быть доставлен пакет по пути к своему конечному пункту назначения,
  - счетчик участков – это число сетей, которые пакет пересечет для достижения своего конечного пункта назначения.

Таблица может содержать другую информацию, такую как маску подсети (или префикс) или время, когда этот вход был обновлен.

Номер входа в таблицу участков	Пункт назначения	Счет участков	Следующий участок	Другая информация
0	163.5.0.0	7	172.6.23.4	
1	197.5.13.0	5	176.3.6.17	
2	189.45.0.0	4	200.5.1.6	
3	115.0.0.0	6	131.4.7.19	

Контрольные вопросы:

1. Назначение протокола RIP
2. Как составляется таблица маршрутизации.

Практическая работа № 24

ПРОТОКОЛ МАРШРУТИЗАЦИИ OSPF. ПОСТРОЕНИЕ МАРШРУТНЫХ ТАБЛИЦ

Цель работы: изучить назначение и принцип работы протокола OSPF.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия.

Общие сведения:

Протокол OSPF (Open Shortest Pass First, RFC-1245-48, RFC-1583-1587, алгоритмы предложены Дикстрой) является альтернативой RIP в качестве внутреннего протокола маршрутизации. OSPF представляет собой протокол состояния маршрута (в качестве метрики используется - коэффициент качества обслуживания). Каждый маршрутизатор обладает полной информацией о состоянии всех интерфейсов всех маршрутизаторов (переключателей) автономной системы. Протокол OSPF реализован в демоне маршрутизации gated, который поддерживает также RIP и внешний протокол маршрутизации BGP.

Автономная система может быть разделена на несколько областей, куда могут входить как отдельные ЭВМ, так и целые сети. В этом случае внутренние маршрутизаторы области могут и не иметь информации о топологии остальной части AS. Сеть обычно имеет выделенный (designated) маршрутизатор, который является источником маршрутной информации для остальных маршрутизаторов AS. Каждый маршрутизатор самостоятельно решает задачу оптимизации маршрутов. Если к месту назначения ведут два или более эквивалентных маршрута, информационный поток будет поделен между ними поровну. Переходные процессы в OSPF завершаются быстрее, чем в RIP. В процессе выбора оптимального маршрута анализируется ориентированный граф сети. Приведена схема узлов (A-J) со значениями метрики для каждого из отрезков пути. Анализ графа начинается с узла A (Старт). Пути с наименьшим суммарным значением метрики считаются наилучшими. Именно они оказываются выбранными в результате рассмотрения графа ("кратчайшие пути").

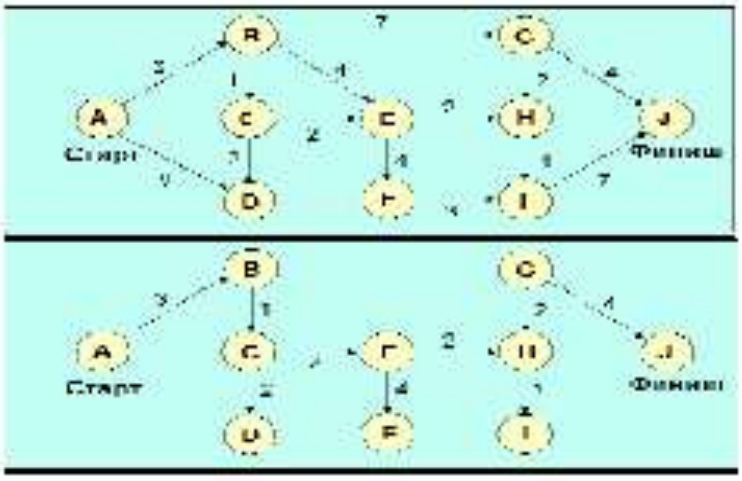


Иллюстрация работы алгоритма Дикстры

Определяющими являются три характеристики: задержка, пропускная способность и надежность. Для транспортных целей OSPF использует IP непосредственно, т.е. не привлекает протоколы UDP или TCP. OSPF имеет свой код (89) в протокольном поле IP-заголовка. Код TOS (type of service) в IP-пакетах, содержащих OSPF-сообщения, равен нулю, значение TOS здесь задается в самих пакетах OSPF. Маршрутизация в этом протоколе определяется IP- адресом и типом сервиса. Так как протокол не требует инкапсуляции пакетов, сильно облегчается управление сетями с большим количеством бриджей и сложной топологией (исключается циркуляция пакетов, сокращается транзитный трафик). Автономная система может быть поделена на отдельные области, каждая из которых становится объектом маршрутизации, а внутренняя структура снаружи не видна (узлы на рис. 4.2.11.2.1 могут Представлят собой как отдельные ЭВМ или маршрутизаторы, так и целые сети). Этот прием позволяет значительно сократить необходимый объем маршрутной базы данных. В OSPF используется термин опорной сети (backbone) для коммуникаций между выделенными областями. Протокол работает лишь в пределах автономной системы. В пределах выделенной области может работать свой протокол маршрутизации.

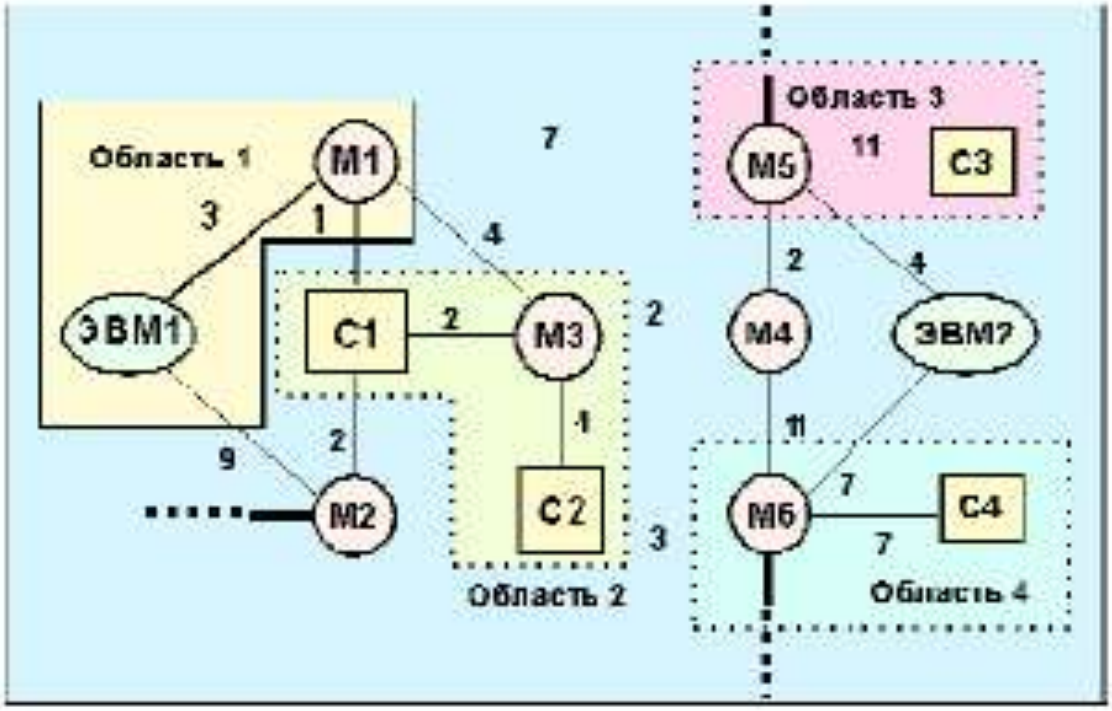


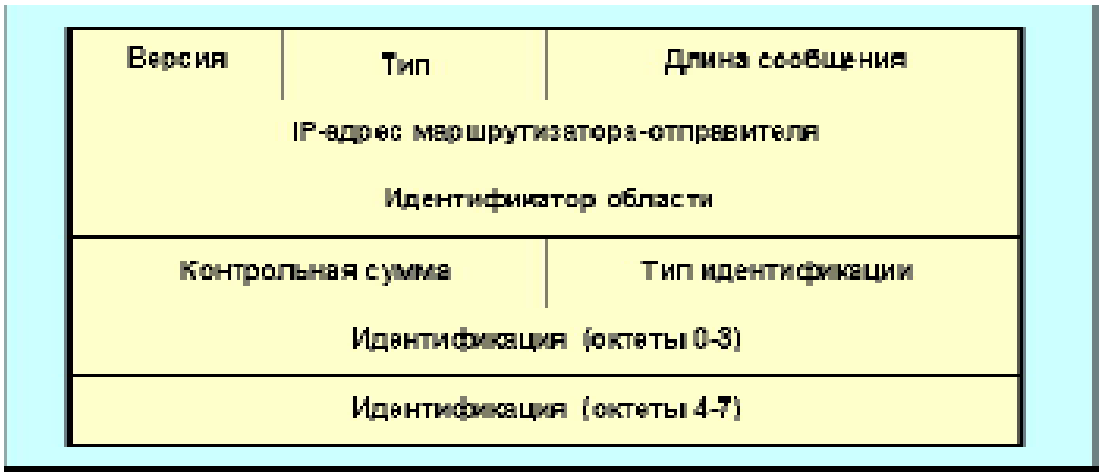
Рис. 4.2.11.2.2 Пример выделения областей при ospf маршру маршрутизаторы; с - сети).

На рисунке приведен пример выделения областей маршрутизации при ospf-маршрутизации в пределах автономной системы. Маршрутизаторы М4 и М2 выполняют функция опорной сети для других областей. В выделенных областях может быть любое число маршрутизаторов. Более толстыми линиями выделены связи с другими автономными системами. При передаче OSPF-пакетов фрагментация не желательна, но не запрещается. Для передачи статусной информации OSPF использует широковещательные сообщения Hello. Для повышения безопасности предусмотрена авторизация процедур. OSPF-протокол требует резервирования двух мультикастинг-адресов:

224.0.0.5 предназначен для обращения ко всем маршрутизаторам, поддерживающим этот протокол.

224.0.0.6 служит для обращения к специально выделенному маршрутизатору.

Любое сообщение ospf начинается с 24-октетного заголовка:



Сообщения об изменениях маршрутов могут быть вызваны следующими причинами:

1. Возраст маршрута достиг предельного значения (lsrefreshtime).

2. Изменилось состояние интерфейса.
3. Произошли изменения в маршрутизаторе сети.
4. Произошло изменение состояния одного из соседних маршрутизаторов.
5. Изменилось состояние одного из внутренних маршрутов (появление нового, исчезновение старого и т.д.)
6. Изменение состояния межзонного маршрута.
7. Появление нового маршрутизатора, подключенного к сети.
8. Вариация виртуального маршрута одним из маршрутизаторов.
9. Возникли изменения одного из внешних маршрутов.
10. Маршрутизатор перестал быть пограничным для данной as (например, перезагрузился).

Каждое сообщение о состоянии канала начинается с заголовка - "объявление состояния канала" (LS- link state).

Маршрутная таблица OSPF содержит в себе:

- IP-адрес места назначения и маску;
- тип места назначения (сеть, граничный маршрутизатор и т.д.);
- тип функции (возможен набор маршрутизаторов для каждой из функций TOS);
- область (описывает область, связь с которой ведет к цели, возможно несколько записей данного типа, если области действия граничных маршрутизаторов перекрываются);
- тип пути (характеризует путь как внутренний, межобластной или внешний, ведущий к AS);
- цена маршрута до цели;
- очередной маршрутизатор, куда следует послать дейтограмму;
- объявляющий маршрутизатор (используется для межобластных обменов и для связей автономных систем друг с другом).

Преимущества OSPF:

Для каждого адреса может быть несколько маршрутных таблиц, по одной на каждый вид IP- операции (TOS).

Каждому интерфейсу присваивается безразмерная цена, учитывающая пропускную способность, время транспортировки сообщения. Для каждой IP-операции может быть присвоена своя цена (коэффициент качества).

При существовании эквивалентных маршрутов OSFP распределяет поток равномерно по этим маршрутам.

Поддерживается адресация субсетей (разные маски для разных маршрутов).

При связи точка-точка не требуется IP-адрес для каждого из концов. (Экономия адресов!)

Применение мультикастинга вместо широковещательных сообщений снижает загрузку не вовлеченных сегментов.

Недостатки:

Трудно получить информацию о предпочтительности каналов для узлов, поддерживающих другие протоколы, или со статической маршрутизацией.

OSPF является лишь внутренним протоколом.

Контрольные вопросы:

1. Алгоритм Дейкстра.
2. Причины сообщений об изменениях маршрутов.

Практическая работа № 25

ИЗУЧЕНИЕ БАЗОВЫХ ЭЛЕМЕНТОВ ТЕХНОЛОГИЙ WWW

Цель работы: изучить базовые элементы технологий WWW.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия.

Программное обеспечение для трассировки маршрута — это утилита, содержащая списки сетей, по которым должны пройти данные от отправляющего оконечного устройства пользователя до удалённой сети назначения.

Как правило, для запуска этого сетевого средства в командную строку необходимо ввести следующее:

tracert <destination network name or end device address>

(для операционных систем семейства Microsoft Windows)

или

traceroute <destination network name or end device address>

(для Unix и подобных систем)

Утилиты трассировки маршрута позволяют определять пути или маршруты, а также вычислять время задержки в IP-сети. Для выполнения этой функции существует несколько средств.

Инструмент traceroute (или tracert) часто используется для поиска и устранения неполадок в сети. Она отображает список пройденных маршрутизаторов и позволяет определить, какой путь использовался для достижения определённого пункта назначения в одной сети или перехода между несколькими сетями. Каждый маршрутизатор — это точка соединения двух сетей, через которую пересылаются пакеты данных. Количество маршрутизаторов называется количеством «переходов», совершённых данными на пути от источника до места назначения.

Отображаемый список поможет определить, какие проблемы с потоком данных возникают при попытке доступа к какому-либо сервису, например веб-сайту. Также список может пригодиться при выполнении таких задач, как загрузка данных. Если один и тот же файл доступен на нескольких веб-сайтах (зеркалах), можно проверить маршрут для каждого зеркала и выбрать наиболее быстрый вариант.

Две трассировки маршрута, выполненные между одними и теми же узлами источника и адресата, но в разное время, могут дать разные результаты. Это может быть связано с «полносвязным» характером взаимно подключённых сетей, состоящих из возможностей Интернета и протоколов Интернета выбирать различные кабельные каналы для отправки пакетов.

Средства трассировки маршрута с использованием командной строки обычно заложены в операционную систему оконечного устройства.

Другие инструменты, такие как VisualRoute™, являются проприетарными программами и позволяют получать более подробную информацию. VisualRoute формирует графическое отображение маршрута, используя доступную информацию в сети.

Для выполнения данной практической работы необходима программа VisualRoute. Если на вашем компьютере программа VisualRoute не установлена, загрузите её по следующей ссылке:

http://www.visualroute.com/download.html

Если с загрузкой или установкой программы VisualRoute возникнут проблемы, обратитесь за помощью к инструктору. Убедитесь, что выполняется загрузка Lite Edition.

VisualRoute Lite Edition	Windows XP\2003\Vista\7	4.0Mb	Download
	Mac OS X (dmg) 10.3+, universal binary	2.0Mb	Download

Сценарий

Используя интернет-подключение и три различных утилиты трассировки маршрута, вы должны будете отследить путь прохождения пакетов данных через Интернет к сетям назначения. Для этого вам потребуется компьютер, подключение к Интернету и доступ к командной строке. Сначала вы воспользуетесь утилитой «tracert», встроенной в ОС Windows, затем веб-средством для трассировки маршрута (http://www.subnetonline.com/pages/network-tools/online-traceroute.php) и, наконец, программой VisualRoute.

Необходимые ресурсы 1 ПК (Windows 7, Vista или XP с выходом в Интернет)

Часть 1: Проверка подключения к сети посредством эхо-запроса с помощью команды ping

Шаг 1: Определите, доступен ли удалённый сервер.

Для трассировки маршрута к удалённой сети используемый ПК должен быть подключён к Интернету.

a. Сначала мы воспользуемся эхо-запросом с помощью команды ping. Эхо-запрос с помощью команды ping — это средство для проверки доступности узла. Пакеты информации пересылаются удалённому узлу с требованием ответа. Локальный ПК определяет, получен ли ответ для каждого пакета, и рассчитывает, какое время заняла пересылка этих пакетов по сети. Название эхо-запрос пришло из области активной гидролокации, где оно обозначало звуковой сигнал, отправляемый под воду и отражающийся от дна или других кораблей.

b. Нажмите кнопку **Пуск** на экране компьютера, введите команду **cmd** в поле **Найти программы и файлы** и нажмите клавишу ВВОД.

c. В командной строке введите **ping www.cisco.com**.

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

d. В первой строке полученных данных отображается полное доменное имя (FQDN) e144.dscb.akamaiedge.net. Затем следует IP-адрес 23.1.48.170. Веб-узлы компании Cisco, содержащие одну и ту же информацию, размещаются на различных серверах (так называемых зеркалах)

по всему миру. Это значит, что имя FQDN и IP-адрес будут отличаться в зависимости от вашего местонахождения.

e. Возьмём приведённую ниже часть полученных результатов.

```
Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

Из неё видно, что были отправлены четыре эхо-запроса с помощью команды ping, на каждый из которых был получен ответ. Ответ поступил на все эхо-запросы с помощью команды ping, значит, потери пакетов нет (0 % потерь). В среднем для передачи пакетов по сети требуется 54 мс (миллисекунды). Миллисекунда — это 1/1000 секунды. От потери пакетов или медленного сетевого подключения в первую очередь страдает качество потокового видео и онлайн-игр. Чтобы определить скорость интернет-подключения более точно, можно отправить не 4 эхо-запроса с помощью команды ping, предусмотренных по умолчанию, а 100. Для этого используется указанная ниже команда.

```
C:\>ping -n 100 www.cisco.com
```

Результат будет выглядеть следующим образом.

```
Ping statistics for 23.45.0.170:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 53ms, Average = 49ms
```

f. Теперь отправьте эхо-запрос с помощью команды ping на веб-сайты регионального интернет-регистратора (RIR), расположенные в различных частях мира.

Африка: C:\> **ping www.afrinic.net**

```
C:\>ping www.afrinic.net

Pinging www.afrinic.net [196.216.2.136] with 32 bytes of data:
Reply from 196.216.2.136: bytes=32 time=314ms TTL=111
Reply from 196.216.2.136: bytes=32 time=312ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111

Ping statistics for 196.216.2.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 312ms, Maximum = 314ms, Average = 313ms
```

Австралия: C:\> **ping www.apnic.net**

```
C:\>ping www.apnic.net

Pinging www.apnic.net [202.12.29.194] with 32 bytes of data:
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=287ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49

Ping statistics for 202.12.29.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 286ms, Maximum = 287ms, Average = 286ms
```

Европа: C:\> **ping www.ripe.net**

```
C:\>ping www.ripe.net

Pinging www.ripe.net [193.0.6.139] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 193.0.6.139:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Южная Америка: C:\> **ping lacnic.net**

```
C:\>ping www.lacnic.net

Pinging www.lacnic.net [200.3.14.147] with 32 bytes of data:
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=157ms TTL=51

Ping statistics for 200.3.14.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 157ms, Maximum = 158ms, Average = 157ms
```

Все эти эхо-запросы с помощью команды ping были отправлены с компьютера, расположенного в США. Что происходит со средним временем эхо-запроса (в миллисекундах), когда данные передаются в пределах одного континента (Северной Америки), по сравнению с ситуацией, когда данные из Северной Америки пересылаются на другие континенты?

Что интересного можно сказать об эхо-запросах с помощью команды ping, отправленных на европейский веб-сайт?

Часть 2: Отслеживание маршрута к удалённому серверу с помощью утилиты «traceroute»

Шаг 1: Определите, какой маршрут из всего интернет-трафика направлен к удалённому серверу.

Проверив достижимость с помощью утилиты «ping», стоит более внимательно рассмотреть каждый сегмент сети, через который проходят данные. Для этого воспользуемся утилитой **tracert**.

a. В командной строке введите **tracert** www.cisco.com.

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

b. Сохраните результаты, полученные после ввода команды «tracert», в текстовый файл, выполнив указанные ниже действия. 1) Нажмите правой кнопкой мыши на строку заголовка окна командной строки и выберите параметры **Изменить** > **Выделить всё**.

2) Ещё раз нажмите правой кнопкой мыши на строку заголовка окна командной строки и выберите параметры **Изменить** > **Копировать**.

3) Откройте **Блокнот Windows**. Для этого нажмите кнопку **Пуск** и выберите **Все программы** > **Стандартные** > **Блокнот**.

4) Чтобы вставить данные в Блокнот, выберите в меню **Правка** команду **Вставить**.

5) В меню **Файл** выберите команду **Сохранить как** и сохраните файл Блокнота на рабочий стол с названием **tracert1.txt**.

c. Запустите утилиту **tracert** для каждого веб-сайта назначения и сохраните полученные результаты в последовательно пронумерованные файлы.

C:\> **tracert www.afrinic.net** C:\> **tracert www.lacnic.net**

d. Интерпретируйте данные, полученные с помощью утилиты **tracert**.

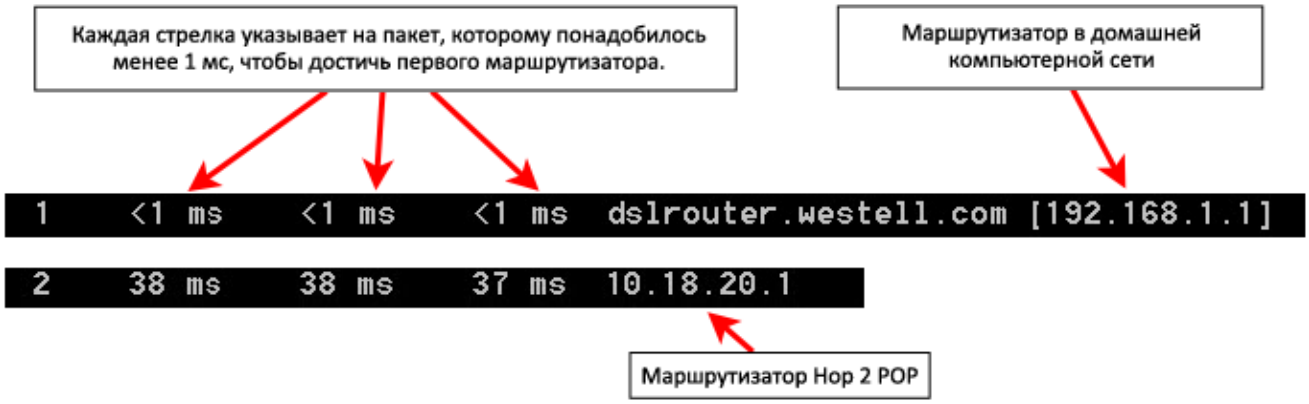
В зависимости от зоны охвата вашего интернет-провайдера и расположения узлов источника и назначения отслеженные маршруты могут пересекать множество переходов и сетей. Каждый переход — это один маршрутизатор. Маршрутизатор представляет собой особый компьютер, который используется для перенаправления трафика через Интернет. Представьте, что вы отправились в поездку по автодорогам нескольких стран. Во время своего путешествия вы постоянно попадаете на развилки, где нужно выбирать одно из нескольких направлений. Теперь представьте себе, что на каждой такой развилке имеется устройство, которое указывает правильный путь к конечной цели вашего путешествия. То же самое делает маршрутизатор для пакетов в сети.

Поскольку компьютеры используют язык цифр, а не слов, маршрутизаторам присваиваются уникальные IP-адреса (номера в формате x.x.x.x). Утилита **tracert** показывает, по какому пути проходит пакет данных до конечного пункта назначения. Кроме того, с помощью утилиты **tracert** можно определить, с какой скоростью проходит трафик через каждый сегмент сети. Каждому

маршрутизатору на пути прохождения данных отправляются три пакета, время ответа на которые измеряется в миллисекундах. Используя данную информацию, проанализируйте результаты, полученные с помощью утилиты **tracert** при отправке пакетов к www.cisco.com. Ниже представлен весь маршрут трассировки.

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

Детализируем.



В приведённом выше примере пакеты, отправленные утилитой «tracert», пересылаются из ПК источника на основной шлюз локального маршрутизатора (переход 1: 192.168.1.1), а затем на маршрутизатор в точке подключения (POP) к интернет-провайдеру (переход 2: 10.18.20.1). У каждого провайдера есть множество маршрутизаторов POP. Они отмечают границы сети интернет-провайдера и служат точками подключения к Интернету для клиентов. Пакеты передаются по сети компании Verizon, пересекают два перехода и попадают в маршрутизатор, принадлежащий alter.net. Это может означать, что пакеты достигли другого интернет-провайдера. Этот момент очень важен, поскольку при пересылке пакетов от одного к другому провайдеру возможны потери, а также важно помнить, что не все интернет-провайдеры способны обеспечить одинаковую скорость передачи данных. Как определить, является ли alter.net тем же самым или другим интернет-провайдером?

е. Существует интернет-сервис whois, с помощью которого можно узнать владельца доменного имени. Сервис whois доступен по адресу http://whois.domaintools.com/. Согласно информации, полученной с помощью whois, домен alter.net также принадлежит компании Verizon.

```
Registrant:
        Verizon Business Global LLC
        Verizon Business Global LLC
        One Verizon Way
         Basking Ridge NJ 07920
        US
         domainlegalcontact@verizon.com +1.7033513164 Fax: +1.7033513669

    Domain Name: alter.net
```

Таким образом, интернет-трафик начинается на домашнем ПК и проходит через домашний маршрутизатор (переход 1). Затем он подключается к интернет-провайдеру и передаётся по его сети (переходы 2–7), пока не достигнет удалённого сервера (переход 8). Это довольно нетипичный пример, в котором от начала до конца задействован только один провайдер. Как видно из следующих примеров, чаще всего в пересылке данных участвуют два и более интернет-провайдеров.

f. Теперь рассмотрим пример с пересылкой интернет-трафика через несколько интернет-провайдеров. Ниже представлены результаты применения утилиты «tracert» к узлу www.afrinic.net.

```
C:\>tracert www.afrinic.net

Tracing route to www.afrinic.net [196.216.2.136]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    39 ms    38 ms    37 ms  10.18.20.1
  3    40 ms    38 ms    39 ms  G4-0-0-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.197.182]
  4    44 ms    43 ms    43 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    42 ms  0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
  6    43 ms    71 ms    43 ms  0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
  7    47 ms    47 ms    47 ms  te-7-3-0.edge2.NewYork2.level3.net [4.68.111.137
]
  8    43 ms    55 ms    43 ms  vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
  9    52 ms    51 ms    51 ms  ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]

 10   130 ms   132 ms   132 ms  ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
 11   139 ms   145 ms   140 ms  ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.13
7]
 12   148 ms   140 ms   152 ms  ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14
]
 13   144 ms   144 ms   146 ms  ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29
]
 14   151 ms   150 ms   150 ms  ae-23-23.ebr2.London1.Level3.net [4.69.148.193]

 15   150 ms   150 ms   150 ms  ae-58-223.csw2.London1.Level3.net [4.69.153.138]

 16   156 ms   156 ms   156 ms  ae-227-3603.edge3.London1.Level3.net [4.69.166.1
54]
 17   157 ms   159 ms   160 ms  195.50.124.34
 18   353 ms   340 ms   341 ms  168.209.201.74
 19   333 ms   333 ms   332 ms  csw4-pkl-gi1-1.ip.isnet.net [196.26.0.101]
 20   331 ms   331 ms   331 ms  196.37.155.180
 21   318 ms   316 ms   318 ms  fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
 22   332 ms   334 ms   332 ms  196.216.2.136

Trace complete.
```

Что происходит в переходе 7?

Является ли level3.net тем же самым интернет-провайдером, что и в переходах 2–6?

Чтобы ответить на этот вопрос, воспользуйтесь сервисом whois.

Как меняется время, необходимое для пересылки пакета данных между Вашингтоном и Парижем в переходе 10 по сравнению с предыдущими переходами 1–9?

Что происходит в переходе 18? С помощью сервиса whois выполните поиск по адресу 168.209.201.74. Кто является владельцем этой сети?

g. Введите команду **tracert www.lacnic.net**.

```
C:\>tracert www.lacnic.net

Tracing route to www.lacnic.net [200.3.14.147]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    38 ms    38 ms    39 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    42 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    82 ms    47 ms    47 ms  0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
  6    46 ms    47 ms    56 ms  204.255.168.194
  7   157 ms   158 ms   157 ms  ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
  8   156 ms   157 ms   157 ms  xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]

  9   161 ms   161 ms   161 ms  xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]

 10   158 ms   157 ms   157 ms  ae0-0.ar3.nu.registro.br [200.160.0.249]
 11   176 ms   176 ms   170 ms  gw02.lacnic.registro.br [200.160.0.213]
 12   158 ms   158 ms   158 ms  200.3.12.36
 13   157 ms   158 ms   157 ms  200.3.14.147

Trace complete.
```

Что происходит в переходе 7?

Часть 3: Отслеживание маршрута к удалённому серверу с помощью программных и веб-средств

Шаг 1: Воспользуйтесь веб-средством для трассировки маршрута.

a. С помощью сайта http://www.subnetonline.com/pages/network-tools/online-tracepath.php отследите маршрут к следующим веб-сайтам:

www.cisco.com www.afrinic.net Скопируйте данные и сохраните их в файл Блокнота.

Как меняется трассировка маршрута при переходе на www.cisco.com из командной строки (см. часть 1), а не через веб-сайт? (Полученные результаты могут изменяться в зависимости от местонахождения и того, с каким интернет-провайдером работает ваше учебное заведение.)

Сравните результаты трассировки маршрута в Африку из части 1 с результатами трассировки того же маршрута через веб-интерфейс. Какую разницу вы заметили? В некоторых результатах трассировки маршрута можно увидеть сокращение «asymm». Есть идеи, что оно может означать? В чём его смысл? Шаг 2: Работа с программой VisualRoute Lite Edition

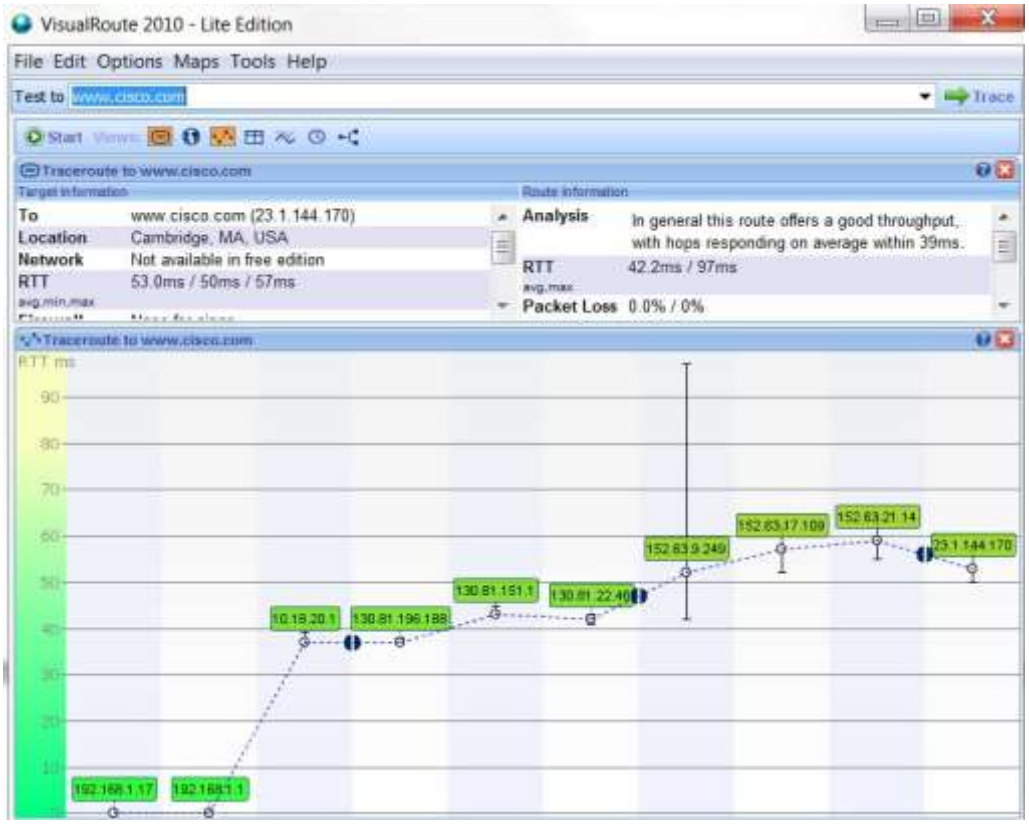
VisualRoute — это проприетарная программа, позволяющая отобразить результаты трассировки маршрута наглядно.

a. Если программа VisualRoute Lite Edition на вашем компьютере не установлена, загрузите ее по следующей ссылке:

http://www.visualroute.com/download.html Если с загрузкой или установкой программы VisualRoute возникнут проблемы, обратитесь за помощью к инструктору. Убедитесь, что выполняется загрузка Lite Edition.

b. С помощью программы VisualRoute 2010 Lite Edition отследите маршруты к www.cisco.com.

c. Сохраните полученные IP-адреса в файле Блокнота.



Часть 4: Сравнение результатов трассировки

Сравните результаты трассировки маршрута к www.cisco.com, полученные в частях 2 и 3.

Шаг 1: Перечислите адреса на маршруте к www.cisco.com, полученные с помощью утилиты «tracert».

Шаг 2: Перечислите адреса на маршруте к www.cisco.com, полученные с помощью веб-сервиса subnetonline.com.

Шаг 3: Перечислите адреса на маршруте к www.cisco.com, полученные с помощью программы VisualRoute Lite Edition.

Все ли инструменты для трассировки использовали одни и те же маршруты к www.cisco.com?

Контрольные вопросы:

1. Проверка подключения к сети с помощью эхо-запроса с помощью команды ping?
2. Отслеживание маршрута к удалённому серверу с помощью утилиты Windows «traceroute».
3. Отслеживание маршрута к удалённому серверу с помощью программных и веб-средств.

Практическая работа № 26

НАСТРОЙКА БРАУЗЕРОВ

Цель работы: изучить особенности настройки различных сетевых служб, облегчающих администрирование ЛВС, а так же возможности управления доступом к внешним сетевым ресурсам на примере программного комплекса Winroute.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия.

Общие сведения:

Каждый компьютер, подключенный к Интернет, идентифицируется уникальным числовым IP-адресом. Для установки соединения между двумя компьютерами через Интернет, первый должен знать IP-адрес второго. Поскольку IP–адреса неудобны для запоминания, была создана Служба доменных Имен (Domain Name Service — DNS). DNS представляет собой базу данных доменных имен, которые легко запомнить. Таким образом пользователю не нужно помнить IP–адрес сервера, доступ к которому он хочет получить. Достаточно ввести соответствующее имя (напр.,) и DNS найдет актуальный IP–адрес.

WinRoute снабжен DNS-модулем, способным перенаправлять запросы DNS на нужный DNS-сервер в Интернете. Последовательно повторяющиеся запросы обрабатываются с использованием кэшированных данных, так что отпадает необходимость ожидать прибытия ответа из Интернет. DNS-сервер в WinRoute также способен обрабатывать запросы DNS в соответствии с определяемым пользователем файлом HOSTS.

При настройке TCP/IP на клиентской машине, которая будет использовать WinRoute как DNS-сервер, необходимо ввести адрес машины, на которой запущен WinRoute как адрес DNS-сервера.

DNS настраивается с использованием меню: Settings => DNS Server.

Диалоговое окно настройки показано на рисунке 11.1

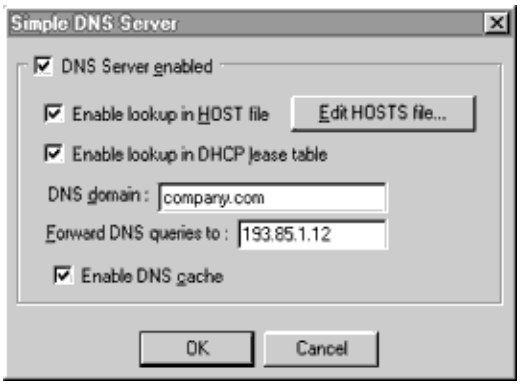


Рис. 11.1 Диалоговое окно настройки

- "DNS Server enabled" Управляет включением/выключением DNS-сервера
- "Enable lookup in HOSTS file" Если эта опция включена, DNS-сервер будет использовать данные из файла HOSTS при обработке запросов.
- "Edit HOSTS file..." Эта кнопка запускает внешний редактор, в котором вы можете отредактировать файл HOSTS.

- "Enable lookup in DHCP lease table" Эта опция позволяет DNS-серверу обрабатывать запросы, используя поле Host name в данных, использованых DHCP-сервером. Может быть использована только в том случае, если вы используете DHCP-сервер, входящий в состав WinRoute. См. Руководство по DHCP-серверу.
- "DNS domain" Введите имя вашего домена (например, ""). При обработке запросов DNS, имя домена добавляется к имени хоста, полученному из файла HOSTS или таблицы обмена DHCP.
- "Forward DNS queries to" Введите числовой IP-адрес DNS-сервера, на который вы хотите перенаправлять запросы DNS. Выберите адрес DNS-сервера вашего провайдера или сервера, к которому у вас есть быстрый доступ.
- "Enable DNS cache" Позовляет хранить ответы на запросы DNS во внутреннем кэше. При этом повторяющиеся запросы обрабатываются, использую содержимое кэша, без ожидания ответа от DNS-сервера, находящегося за пределами вашей ЛВС.

Имейте в виду, что в кэше хранятся только ответы типа "Name => IP address". Ответы хранятся до истечения срока, определяемого DNS-сервером для каждого ответа.

Прокси-сервер

Прокси-кэш

Сервисные функции WWW интернет-прокси: Прокси-сервер собирает данные из интернета и передает их по запросам браузерам в локальной сети. Эти данные также хранятся в разделяемом (общедоступном) кэше. Если эта же информация запрашивается снова, она берется из кэша. Поскольку кэш находится внутри ЛВС, передача данных происходит с соответствующей скоростью, гораздо быстрее, чем из Интернет.

В основном, кэш увеличивает скорость доступа в Интернет путем локального предоставления данных, с уже посещенных сайтов, позволяя таким образом получать данные из Интернета только из мест, еще не посещенных. Результатом является улучшение производительности без изменения коммуникационных ресурсов.

Управление доступом

Прокси-сервер может использоваться для управления доступом к ресурсам Интернет. Например, вы можете ограничить доступ определенному(ым) пользователю(ям) к определенным Web-сайтам.

Запреты могут быть применены к отдельным пользователям, группам пользователей или отдельным URL'ам.

Настройка прокси-сервера

General Properties (Основные свойства)

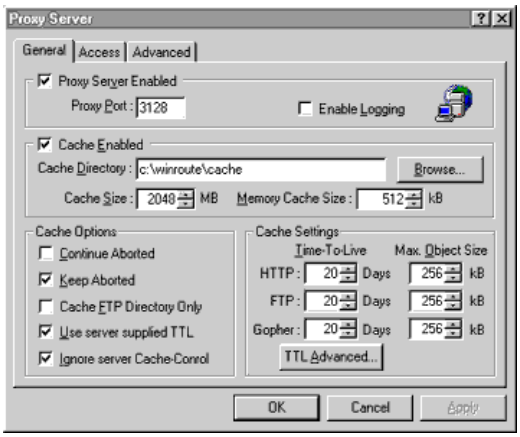


Рис. 11.2

Port (Порт) Номер порта, используемого браузером для сообщения с прокси, по умолчанию - 3128. Предпочтительно использование значения по умолчанию.

Enable Logging (Разрешить лог) Разрешить лог URL'ов страниц, посещенных браузерами через прокси.

Cache Enabled (Кэш включен) Включить кеширование. Если эта функция выключена, данные берутся только из Интернета.

Cache Directory (Подкаталого кэша) Путь к подкаталогу прокси-кэша.

Cache Size (Размер кэша) Максимальный размер кэша в мегабайтах. Когда кэш превосходит этот лимит, происходит урезание наполнения кэша до 85% от лимита. Наиболее "старые" в кэше данные удаляются.

Continue Aborted (Продолжать закачку) Когда пользователь нажимает "стоп" или переходит к другой странице, не закончив загрузку текущей, прокси-сервер продолжает закачку данных с этой страницы. Если впоследствии пользователь вернется к этой странице, она будет предоставлена ему из кэша. Включение этой функции ускоряет открытие страниц.

Keep Aborted (Хранить прерванные запросы) Разрешает хранение объектов, закачка которых была прервана (страницы, рисунки и т.п.) Предположим закачивается страница, 50% выполнено, связь прерывается — эти 50% записываются в кэш, так что при повторном обращении ресурс будет предоставлен без закачки.

Разрешить кэширование только каталогов FTP

Если кэшировать файлы, которые поступают по FTP, быстро расходуется дисковое пространство. Вполне достаточно кэшировать структуру каталогов FTP-сервера.

Это значение определяет, сколько дней объекты будут храниться в вашем кэше. Если запрашивается объект, время хранения которого истекло, он закачивается из Интернет.

Время жизни (дополнительно)

Вы можете установить время жизни объекта, исходя из его URL. Определения URL могут включать умолчания (*).

Примеры: *www*, ftp://*.zip

Максимальный размер объекта

Все объекты, размер которых превосходит это значение, не будут записываться в кэш.

Доступ

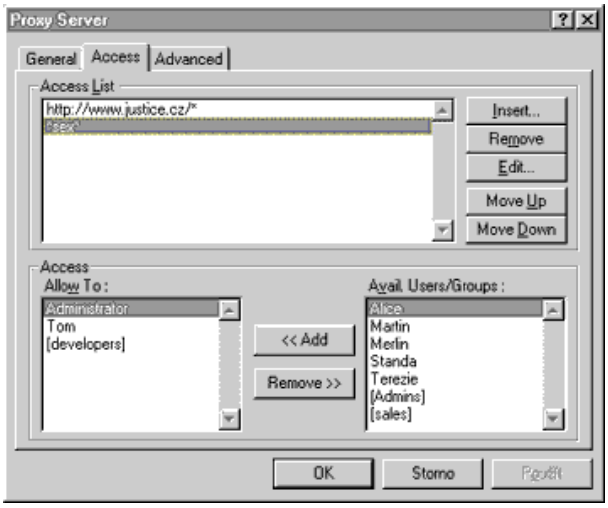


Рис. 11.3

Закладка "Доступ" описывается в пункте Access Control (Управление доступом)

Сложные настройки

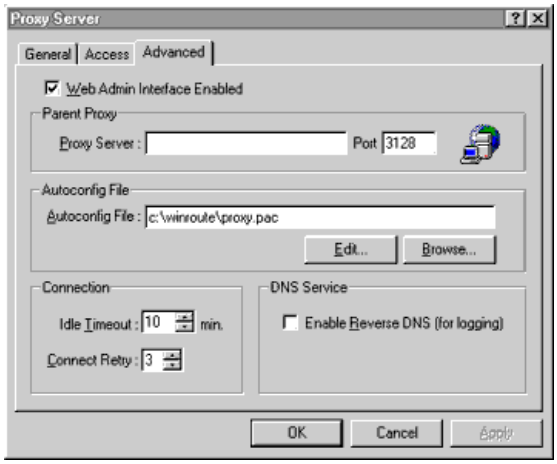


Рис.11.4

Parent Proxy (Старший прокси) DNS-имя или IP-адрес и номер порта "старшего" прокси-сервера (например, находящегося у провайдера). Если это значение установлено, все запросы будут перенаправляться на него.

Autoconfig File (Файл автоматической настройки) Расположение файла автоконфигурации прокси-сервера. Этот файл может использоваться для настройки параметров прокси в браузерах на клиентских машинах. Эта особенность поддерживается Netscape Navigator'ом и старшими версиями MSIE. В файле указаны имя и номер порта WinRoute-сервера.

В браузере вы должны в панели адреса ввести: http://<host>:3129/autoconfig, где <host> — имя WinRoute-сервера.

Idle Timeout (Время бездействия) TCP-соединение будет разорвано, если не будет проявлено активности в течении этого времени.

Connect Retry (Попыток восстановить соединение) Определяет количество попыток установить соединение.

Enable Reverse DNS (Разрешить обратное представление DNS) Разрешает обратное представление DNS для входа в некоторые системы.

Настройка прокси-клиентов

Для использования прокси-сервера, вы должны установить в браузерах клиентских машин его IP-адрес и номер порта.

Ниже типичные примеры настроек для популярных браузеров:

Netscape Navigator 2.0, 3.0

1. Выберите пункты меню: Options->Network Configuration->Proxies
2. Выберите ручную настройку параметров прокси (Manual Proxy Configuration)
3. Нажминте кнопку [View] (просмотр)
4. Введите IP-адрес и порт WinRoute-сервера для полей HTTP, FTP и GOPHER. Номер порта по умолчанию 3128.

Netscape Communicator

1. Выберите пункты меню: Edit -> Preferences -> Advanced -> Proxies
2. Выберите ручную настройку параметров прокси (Manual Proxy Configuration)
3. Нажминте кнопку [View] (просмотр)
4. Введите IP-адрес и порт WinRoute-сервера для полей HTTP, FTP и GOPHER. Номер порта по умолчанию 3128.

MS Internet Explorer 3.0

1. Выберите пункты меню: View->Options->Connections
2. Для версии Windows 95, нажмите кнопку Proxy

3. Отметьте check box для Use the same proxy for all protocols (Использовать один прокси для всех протоколов).

4. Введите IP-адрес и порт WinRoute-сервера в соответствующих полях.

Управление доступом

Управление доступом позволяет вам ограничивать права доступа пользователей WWW-сервера.

Список свойств доступа

В списке доступа указываются URL, запрещенные для определенных пользователей и групп. Форматы записи: протокол://хост/путь — непостоянные элементы строк могут заменяться звездочками. У каждого запрещенного URL есть ассоциированный с ним список пользователей и групп, имеющих доступ к этому URL. Для получения доступа они должны вводить имя и пароль по опдсказке браузера. Примечание: запрещенные URL'ы всегда открыты для доступа членам группы Администраторов.

Запрет доступа к web-интерфейсу WinRoute

Также запрет может быть применен к доступу к web-интерфейсу администратора WinRoute. Для этого добавьте следующую строку в Список Доступа (Access List): http://WinRoute/admin/* в точности как указано здесь. WinRoute распознает свое собственное имя, так что нет нобходимости вводить актуальное имя хоста. Перед запретом доступа к web-интерфейсу WinRoute, убедитесь, что вы являетесь членом группы Администраторов, иначе вы заблокируете себе доступ к нему. Однако, вы всегда можете получить доступ к настройкам WinRoute используя графическое приложение WinRoute.

Замечание о браузерах:

- Некоторые браузеры не поддерживают функцию аутентификации, необходимую для доступа к запрещенным страницам. Эти браузеры не смогут получить доступ к закрытым URL'ам; это, однако, не относится к остальным URL'ам. Аутентификация прокси поддерживается Netscape Navigator 3.0, MSIE 3.0 и всеми более поздними версиями.
- Пожалуйста имейте в виду, что аутентификация пользователя будет запрашиваться однократно для каждой сессии браузера. Впоследствии браузер будет автоматически предоставлять прокси-серверу имя и пароль пользователя по требованию. Это известно как кэшинг аутентификации. Чтобы очистить кэш аутентификации, пользователь должен прервать сессию браузера.

Управление доступом (примеры)

1. Мы хотим закрыть пользователям группы [users] к следующим доменам. Однако пользователь boss должен иметь доступ повсюду. Установите Список Доступа (Access List) как показано в таблице.

Access List	**users/groups**
*	boss
./	[users]
./	[users]

2. Чтобы полностью закрыть доступ к домену **:**

Access List	**users/groups**
*./	

Почтовый сервер

Почтовый сервер WinRouite может быть использован в качестве почтового шлюза между ЛВС и Интернет. Он собирает сообщения, посланные пользователями ЛВС и входящую из Интер-

нет почту. Затем исходящая почта отправляется по адресам в Интернете, а входящая распределяется по почтовым ящикам пользователей ЛВС.

Если ЛВС подключена к Интернет через dial-up, есть возможность составлять расписания отсылки и приема почты Интернет.

Пользователи ЛВС могут использовать любой почтовый клиент, поддерживающий работу с протоколами SMTP/POP3 (MS Internet Mail, Netscape Mail client, MS Exchange, Eudora, Pegasus mail, и т.п.) для подключения к почтовому серверу WinRoute.

Почтовый сервер настраивается в диалоговом окне "Mail Server", вызываемом из меню "Settings, Mail Server".

Получение почты из Интернет

Существует несколько путей, которыми почтовый сервер WinRoute может получать почту из Интернет:

1. Получение почты с удаленного почтового ящика POP3

Почтовый сервер WinRoute позволяет получать почту из индивидуального почтового ящика POP3, расположенного у вашего провайдера или где-то еще в Интернете. Полученная почта распределяется по почтовым ящикам пользователей.

Управление удаленными почтовыми ящиками POP3 производится в закладке "Remote POP3".

Примечание: чтобы почтовый сервер WinRoute немедленно доставлял почту, посланную пользователем с локальной машины на удаленный почтовый ящик, представленный в Remote POP3 accounts, вам нужно добавить соответствующую запись в закладке "Alias". В качестве "Alias" необходимо ввести адрес электронной почты удаленного почтового ящика POP3 и в поле "Deliver To" указать того же пользователя, что и в соответствующей записи POP3. Смотрите примеры для конкрентных настроек.

2. Получение почты из почтового ящика домена

Некоторые провайдеры позволяют хранить почту для всего домена в одном (удаленном) почтовом ящике POP3. Например, если домен вашей компании , то вся электронная почта, адресованная на этот домен (@) будет храниться в одиночном почтовом ящике вашего провайдера.

Почтовый сервер WinRoute позоволяет сортировать и распределять почту после загрузки из удаленного ящика POP3 по почтовым ящикам пользователей ЛВС в соответствии с полем To: (Кому:) заголовка письма.

Чтобы WinRoute производил сортировку на удаленном ящике, вы должны выбрать опцию <Sorting Rules> в поле "Deliver To". Затем нажмите кнопку "Sorting Rules" и установите правила сортировки. В закладке "General" выберите "I have Internet domain" и в поле "Local Domain(s)" введите ваш домен (например,). Опция "Use ETRN command" должна быть не установлена.

3. Доменная почтовая служба SMTP

Если ваша ЛВС имеет постоянное подключение к Интернет, было бы хорошо получать получать почту для вашего домена напрямую через протокол SMTP. Такая возможность есть и на коммутируемых линиях, но в этом случае вам нужен постоянный IP-адрес и соединение должно устанавливаться через определенные промежутки времени. Запись MX (Mail eXchange - почтовый обмен) для вашего домена должна указывать на IP-адресс, с которого работает почтовый сервер WinRoute. Если вы используете NAT, вы должны создать порт (mapped port) для протокола SMTP.

В закладке "General" выберите "I have Internet domain" и в поле "Local Domain(s)" введите ваш домен (например,). Если ваша ЛВС подключена к Интернет через коммутируемую линию и удаленный сервер SMTP поддерживает команду ETRN, нужно установить опцию "Use ETRN command".

Отсылка почты в Интернет

Вся почта Интернет (исходящая) отсылается через сервер Relay SMTP.

"Relay SMTP server" может быть установлен в закладке "General".

Настройка почтовых клиентов

Каждому пользователя почтового сервера WinRoute нужно создать собственную учетную запись. Учетные записи пользователей создаются в диалоговом окне "Accounts", меню "Settings>>Accounts".

Для каждого клиента применяется соответствующая процедура настройки. Для настройки клиента необходимо указать IP-адрес хоста, на котором находятся серверы SMTP и POP3. В нашем случае это IP-адрес машины, на которой кстановлен WinRoute. Имя пользователя и пароль POP3 должны соответствовать таковым для WinRoute.

Составление расписания обмена почтой

Обмен почтой Интернет (отсылка и получение) управляется модулем расписания работы (далее — Scheduler), меню Settings. Scheduler обеспечивает два типа действий:

1. Отсылка/Получение почты

2. Отсылка почты

Для каждого действия можно выбрать одно из следующих условий:

"Valid on" Дни недели, в которые может выполняться действие.

"Every — At" Периодические промежутки времени или определенное время, в которых будет выполняться действие.

"When dialed only" Действие будет выполняться, только если установлено модемное соединение.

"Allow to dial" Запрос установки модемного соединения.

Примечание: вы можете вручную запустить обмен почтой через Web-интерфейс. Откройте в браузере страницу Manual, кликните на кнопке [Send and Receive].

Алиасы

Используется для создания алиасов пользователей и переназначения/пересылки электронной почты.

Алиасы используются в следующих ситуациях:

- почта получена из Интернет через SNTP (от пользовательского почтового клиента или из Интернет)
- перед загрузкой в почтовый ящик почты с удаленного ящика POP3

Алиасы устанавливаются в закладке "Aliases".

Почтовый сервер (Примеры)

Получение почты с удаленного почтового ящика POP3

Каждый пользователь имеет эккаунт у провайдера. Для исходящей почты используется почтовый сервер провайдера .

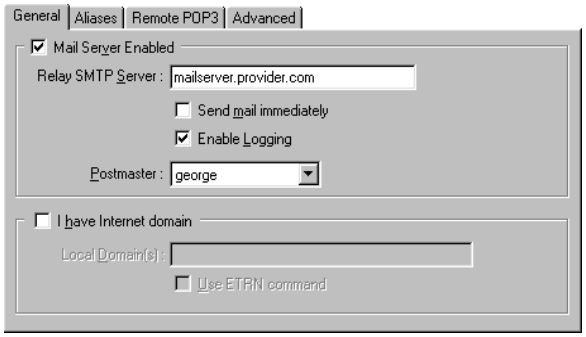


Рис. 11.5

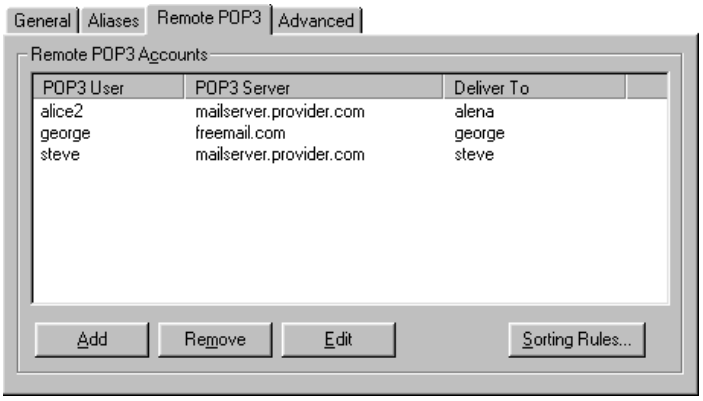


Рис. 11.6

В этом случае в поле Aliases нужно ввести e-mail пользователя (см. ниже). Это полезно, если пользователи в ЛВС обмениваются почтой. Без соответствующих настроек алиасов, почтовый сервер WinRoute не сможет распознать, что почта локальная, и отправит ее через Интернет для получения с удаленного ящика POP3.

Рис. 11.7

Получение почты из почтового ящика домена

Рассмотрим случай с компанией, в которой 5 работников. У каждого есть учетная запись в WinRoute. Записи следующие: alice, george, jane, martin и tom.

Компания имеет домен и провайдер всю почту для этого домена хранит в ящике company на свем почтовом сервере . Для исходящей почты используется тот же сервер.

Компания хочет использовать адреса info@ и sales@. Почту, посланную на info@ должен получать george; почту, посланную на sales@ должны получать пользователи в группе sales.

В закладке "General" выберите "I have Internet domain" и в поле "Local Domain(s)" введите .

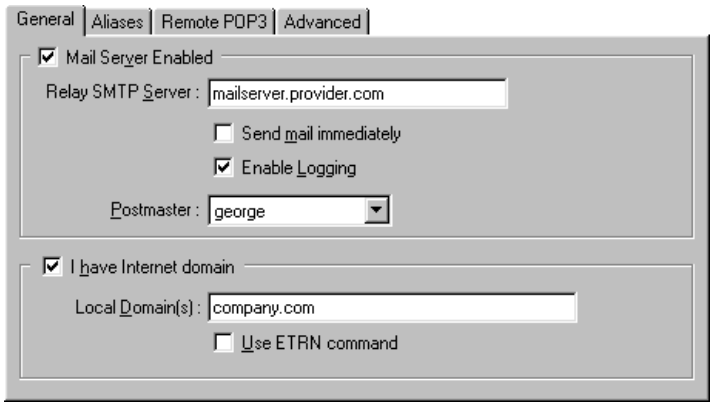


Рис. 11.8

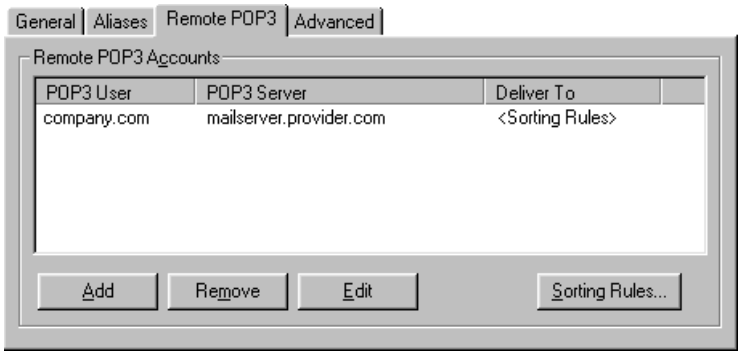


Рис. 11.9

Рис. 11.10

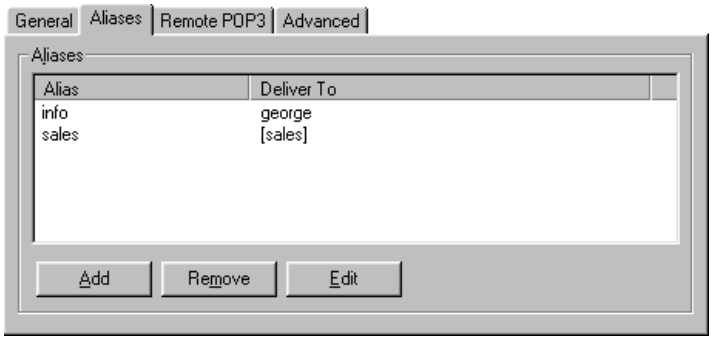


Рис. 11.11

Доменная почтовая служба SMTP

Случай с той же компанией: 5 пользователей, у каждого есть учетная запись WinRoute. Записи следующие: alice, george, jane, martin и tom.

Компания имеет домен , получение почты производится с использованием протокола SMTP. В случае модемного соединения необходим фиксированный IP-адрес. Запись MX (почтового обмена) для домена должна указывать на этот IP-адрес. Адрес почтового сервера провайдера .

Компания хочет использовать адреса info@ и sales@. Почту, посланную на info@ должен получать george; почту, посланную на sales@ должны получать пользователи в группе sales.

В случае использования в ЛВС NAT (Network Address Translation), необходимо назначить порт для протокола SMTP. (меню Settings -> Advanced -> Mapped ports).

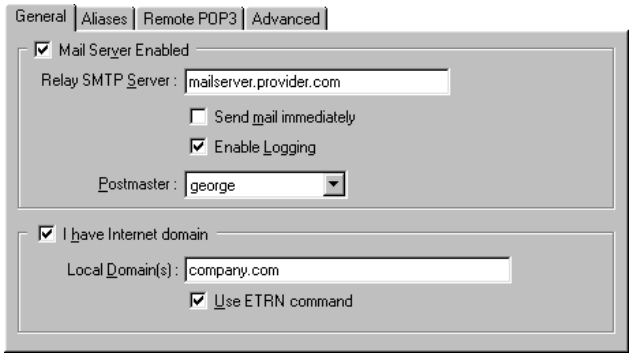


Рис. 11.12

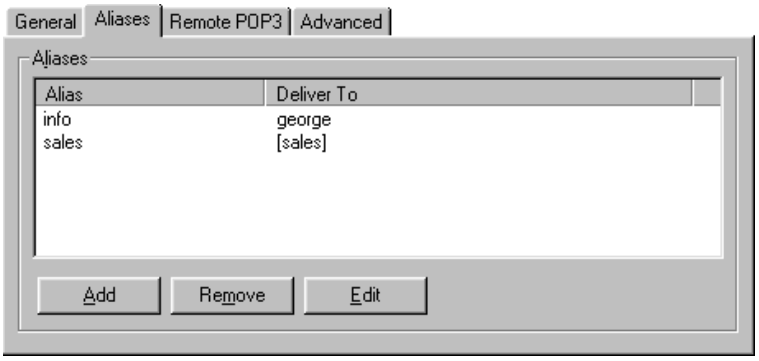


Рис. 11.13

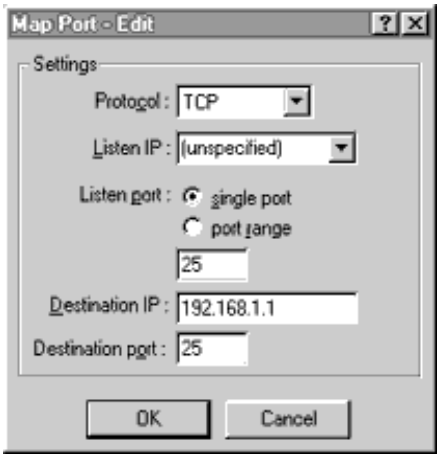


Рис. 11.14

WinRoute работает на компьютере с адресом 192.168.1.1

-сервер

TCP/IPдолжен быть правильно настроен у каждого компьютера в сети. Это означает, что на каждом компьютере должны быть настроены IP-адрес, сетевая маска, адрес сетевого шлюза, адрес DNS-сервера и т.д. Если специалисту необходимо настроить вручную большое количество компьютеров в сети, тяжело избежать ошибок, например использования одного адреса дважды, что может вызывать коллизии и зачастую нарушать работу сети в целом.

Для облегчения задачи был создан Протокол динамического конфигурирования хоста (Dynamic Host Configuration Protocol, DHCP), используемый для динамической настройки протокола TCP/ip на клиентских машинах. Во время загрузки компьютера с DHCP-клиентом, посылается запрос. При его получении DHCP-сервером он выбирает параметры настройки TCP/IP для клиента, такие как IP-адрес, сетевая маска, шлюз, адрес DNS-сервера, имя домена клиента и т.п. Используя эти параметры, сервер формирует ответ и отсылает его клиенту. Конфигурация, назначенная клинету сервером, действует ограниченное время (так называемое "время аренды"). Сервер всегда назначает IP-адрес, не совпадающий с другими адресами, использованными DHCP-сервером другим клиентам.

С включенным DHCP-сервером появляется возможность использовать опцию "Obtain IP address from DHCP server" ("Получать IP-адрес с DHCP- сервера") и DHCP-сервер берет на себя ответственность за правильную настройку TCP/IP на клиентских компьютерах.Это может помочь в значительной мере снизить стоимость поддержки и управления сетью.

В сосатве WinRoute имеется полнофункциональный DHCP-сервер, позволяющий динамически назначать параметры TCP/IP клиентам DHCP. Если вы хотите использовать DHCP-сервер, вы должны настроить его соответствующим образом (см. ниже) и включить опцию "Obtain IP

address from DHCP server" в настройках TCP/IP на клиентских машинах. Если некоторые компьютеры в вашей сети будут работать без использования DHCP, необходимо позаботиться о том, чтобы параметры, использованные при их настройке, не совпадали с оными, используемыми в настройках DHCP.

Настройка DHCP-сервера

Вы можете настроить DHCP-сервер, используя диалоговое окно, вызываемое командой меню

Settings => DHCP server

- "DHCP server enabled" Включает WinRoute's DHCP-сервер. При выключении настройки не теряются, просто останавливается работа DHCP-сервера.

Диалоговое окно содержит две основные области: Scopes и Options.

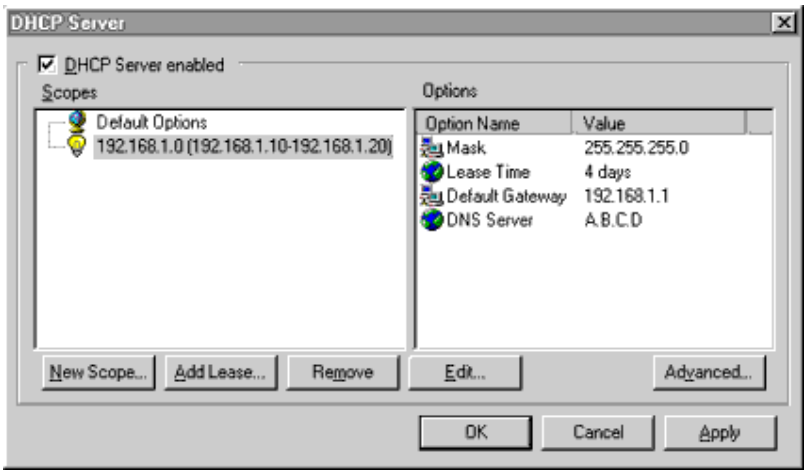


Рис. 11.15

В "Scopes" показаны интервалы IP-адресов, используемых для назначения клиентам. Показываются первый и последний адреса интервала.

Для каждого интервала могут настраиваться дополнительные параметры, показанные в разделе "Options".

Раздел Scopes всегда содержит "Default Options" — список параметров, назначаемых клиенту по умолчанию. Чтобы определить, является ли параметр глобальным или нет (указывается в "Default Options"), показывается следующая иконка:

– для интервала определен параметры

– параметр назначен по умлочанию

Нижняя часть диалогового окна содержит следующие кнопки:

- "New Scope..." При нажатии этой кнопки вызывается диалог, определяющий параметры нового интервала.
- "Edit..." Используется для редактирования параметров существующего интервала.
- "Remove" Удалить интервал.

Диалоговое окно настройки параметров интервала:

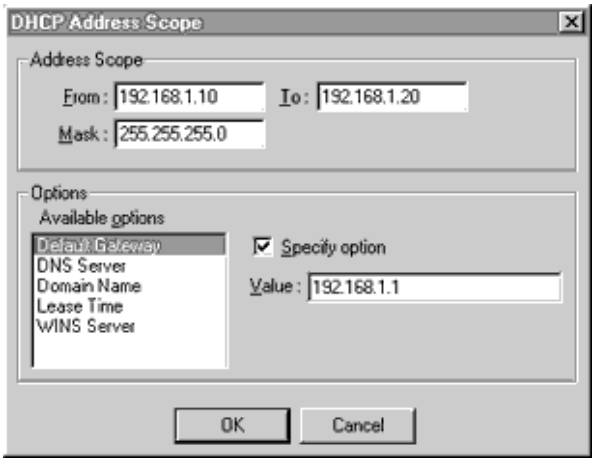


Рис. 11.16

"Address Scope" Введите диапазон IP-адресов, назначаемых клиентом (поля "From" ("От") и "To" ("До")) с указанем сетевой маски (поле "Mask"). IP-адреса задаваемого диапазона должны принадлежать назначенным подсети.

"Options" Показывает список остальных конфигурационных параметров, назначаемых станциям в пределах заданного диапазона. Если параметр не задан (не стоит галочка в боксе "Specify option"), будет использоваться значение по умолчанию. Могут быть использованы следующие параметры:

- "Default Gateway" Адрес шлюза по умолчанию. Шлюз обслуживает коммуникацию со станциями в других подсетях.
- "DNS Server" IP-адрес DNS-сервера.
- "Domain Name" Вы можете ввести здесь имя вашего домена (если у вас есть зарегистрированный домен).
- "Lease Time" Определяет время, в течении которого клиент может использовать конфигурационные данные. По его истечении клиент должен запросить новые параметры TCP/IP у сервера DHCP.
- "WINS Server" Адрес сервера WINS, используемого для распространения информации об общих ресурсах сети Microsoft.

Для каждого интервала вы можете зарезервировать определенные IP-адреса для некоторых компьютеров,\ используя кнопку "Add Lease...".

Резервирование обеспечивает постоянное получение соответствующим компьютером определенного IP-адреса (полезно, если на этом компьютере запущена какая-либо служба, например принт–сервер).

Диалог резервирования адреса:

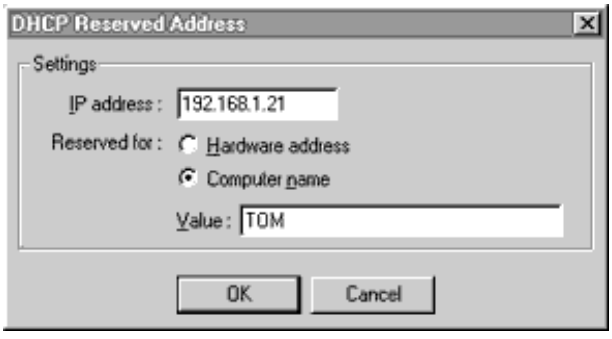


Рис. 11.17

- "IP address" IP-адрес для резервирования.

- "Reserved for" Вы можете определить, каким образом будет производиться идентификация компьютера, для которого был зарезервирован адрес:

  1. "Hardware address" Компьютер идентифицируется адресом (идентификатором) сетевой карты. Адрес должен быть введен в поле "Value" в виде шести байтов, разделенных дефисами (пример: 00-60-08-5f-75-b9)

  2. "Computer name" Компьютер идентифицируется своим именем в сети MS Windows.

- Кнопка "Advanced..." Используется для настройки DHCP-сервера таким образом, чтобы он отвечал на запросы, посланные по протоколу BOOTP (старый протокол настройки TCP/IP). Вы должны включить эту опцию, если у вас в сети есть компьютеры, использующие BOOTP.

Список адресов, назначенных определенным клиентам DHCP-сервером может быть получен щелчком правой кнопкой мышки в основном окне лога WinRoute и выбором Show => Leased IPs из меню. Альтернативный путь вызова этого меню - нажатие CTRL+SHIFT+L.

Настройка в мультисегментной сети

Чтобы использовать сервер DHCP в сети с несколькими сегментами, вам нужно настроить шлюзы в вашей сети так, чтобы они пересылали запросы DHCP на сегмент, к которому подключен DHCP-сервер. Примеры настроек для некоторых типов роутеров показаны ниже:

- Windows NT. Если вы используете в качестве роутера (шлюза) сервер Windows NT, необходимо установить на нем службу "DHCP Relay Agent" Затем, в настройках TCP/IP на сервере, переключитесь на закладку DHCP Relay и введите IP-адрес сервера DHCP, на который будут перенаправляться запросы DHCP (то есть, вы должны ввести IP-адрес компьютера, на котором работает WinRoute).
- Novell Netware. Если вы используете в качестве роутера (шлюза) сервер NetWare, необходимо загрузить на нем модуль BOOTPFWD.NLM. Модуль возьмет на себя пересылку запросов DHCP и BOOTP. Команда выглядит так: load bootpfwd.nlm <DHCP server address>

Повторим, что IP-адресом DHCP-сервера является IP-адрес компьютера, на котором работает WinRoute.

Настройка DHCP-сервера (пример)

Следующий рисунок показывает пример настройки сервера DHCP:

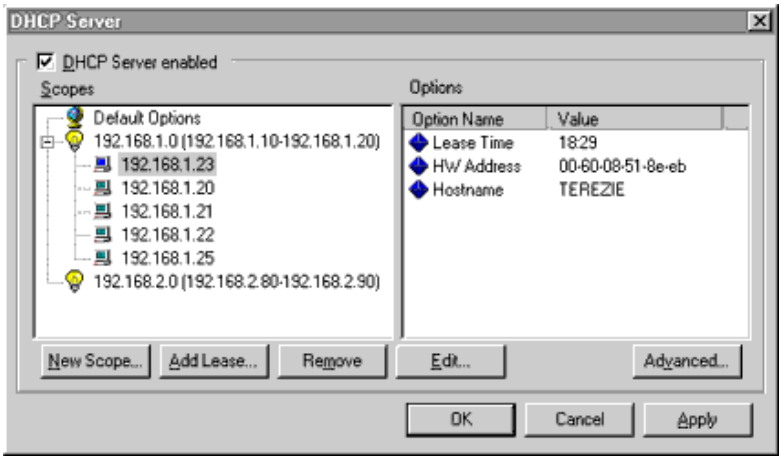


Рис. 11.18

В примере определены два диапазона. Первый запрещен для 192.168.1.0, второй для 192.168.2.0. В первом диапазоне адреса от 192.168.1.10 до 192.168.1.20, во втором со 192.168.2.80 до 192.168.2.90.

Также видно, что в диапазоне для 192.168.1.0 следующие адреса назначены клиентам: 192.168.1.23, 192.168.1.20, 192.168.1.21, 192.168.1.22 и 192.168.1.25. Для 192.168.2.0 не было назначений адресов из диапазона.

В области "Scopes", выбран адрес 192.168.1.23 и показана информация о нем. Например, показано время, в течении которого будут действовать назначенные компьютеру параметры настроек. Также видно, что "железячный" (MAC) адрес компьютера 00-60-08-51-8e-eb и его имя "TEREZIE"

Порядок выполнения работы

1. Удалить все правила фильтрации входящего и исходящего трафика.

2. Установить правило, разрешающее прохождение IP–пакетов с журналированием. Проверить прохождение пакетов в журнале Sequrity Log данной машины при посылке эхо-пакетов с любой станции локальной сети (ping <host>, где host — IP–адрес данной машины)

3. Настроить DNS–модуль Winroute в качестве DNS–сервера для локальной подсети

3.1. Используя диалог DNS Forwarding разрешить перенаправление и указать внешний DNS–сервер (см. раздел «DNS-сервер» данного пособия, адрес внешнего DNS–сервера — 192.168.8.254)

3.2. Проверить работоспособность DNS–сервера Winroute, настроив другие машины этой подсети на DNS–сервер Winroute (Пуск/Настройка/Панель управления/Сеть, закладка Конфигурация, запись ”TCP/IP->SURECOM…”, закладка “Конфигурация DNS”, включить DNS, Порядок просмотра серверов DNS, Добавить запись вида ip_address, где ip_address — IP–адрес машины с настроенным сервером DNS Winroute, удалив старые записи; перезагрузить компьютер). Проверить после перезагрузки сетевые настройки (запустить winipcfg) — должен быть корректно указан DNS–сервер. Убедится в прохождении UDP–пакетов, порт 53 (nameserver) — для определения адреса хоста при попытке получить адрес, например в случае задания команды “ping ” в журнале Sequrity Log

3.3. Включить использование HOSTS–файла для разрешения имен

3.4. Изменить содержимое HOSTS–файла — добавить несколько записей вида:

xxx.xxx.xxx.xxx host

где:

xxx.xxx.xxx.xxx — IP–адрес

host — имя станции

Например: 192.168.8.16 myhost

3.5. Проверить с помощью команды ”ping myhost” или ”ping –a 192.168.8.16” с соседней станции (настроенной на DNS–сервер Winroute) работу DNS–сервера Winroute.

При настроенном HOSTS-файле на соседней машине, являющейся DNS-сервером для, команда типа **ping myhost** выполняется на этом DNS-сервере, но не выполняется на других машинах сети. Так и должно быть?

4. Выполнить настройку Proxy–сервера Winroute

4.1. Используя диалог Proxy Server Settings настроить Proxy–сервер Winroute (см. раздел «Прокси-сервер» данного пособия, имя внешнего Proxy–сервера — proxy.mipk kspu.kharkov.ua)

4.2. Проверить работоспособность Proxy–сервера Winroute, настроив другие машины этой подсети на Proxy–сервер Winroute (Internet Explorer, пункт меню Сервис/Свойства обозревателя, закладка Подключение/Настройка локальной сети/Использовать прокси–сервер/адрес_машины_с_включенным_Winroute, порт — который был использован при настройке Winroute, 3128 по умолчанию). Проверить прохождение TCP–пакетов на порт 3128 в журнале Sequrity Log

4.3. Ограничить доступ для некоторых пользователей, предварительно добавив с помощью диалога User Accounts, к различным внешним серверам (см. раздел «Доступ» данного пособия)

4.4. Выполнить п.4.2. предварительно проверив корректность настроек Proxy в броузерах на других машинах сети (обратить внимание на закладку “Дополнительно”). При корректной настройке фильтрация запросов будет происходить последовательно — Winroute Proxy, внешний Proxy–сервер, о чем можно судить по автоматически генерируемым предупреждениям, отображаемым броузером.

При попытке загрузить страницу по http-протоколу на машине-клиенте, в строке состояния браузера действительно отображается запрос к Proxy, настроенном на соседней машине в сети, но страница в браузере все равно не отображается, несмотря на то что в настройках прокси набираемый адрес добавлен в список разрешенных.

5. Выполнить настройку Mail–сервера Winroute для использования в качестве почтового сервера локальной сети. Проверить его работоспособность в различных режимах (см. раздел «Почтовый сервер» данного пособия)

5.1. Указать внешний SMTP server

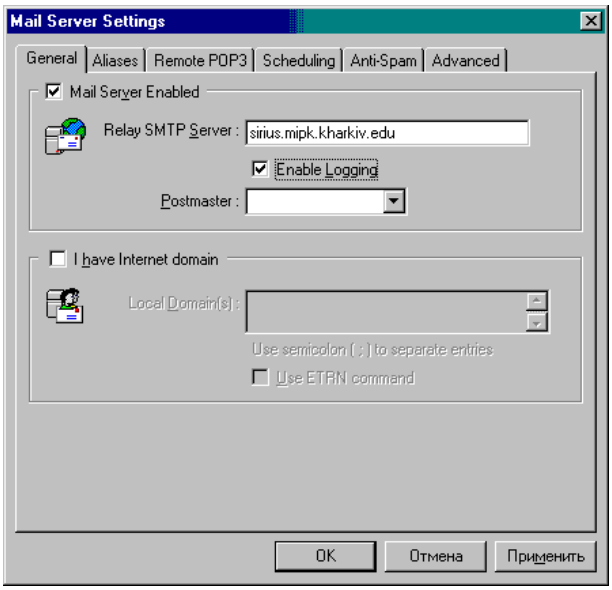


Рис. 11.19

5.2. Добавить алиасы

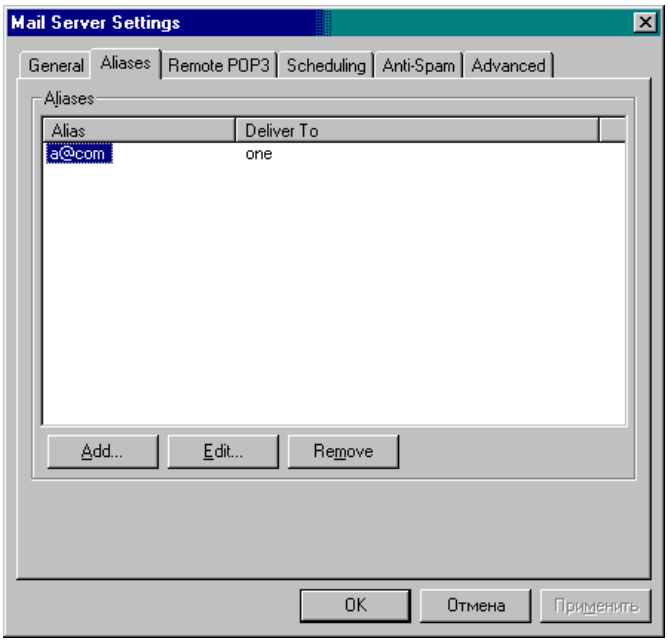


Рис. 11.20

5.3. Настроить удаленный POP3 сервер

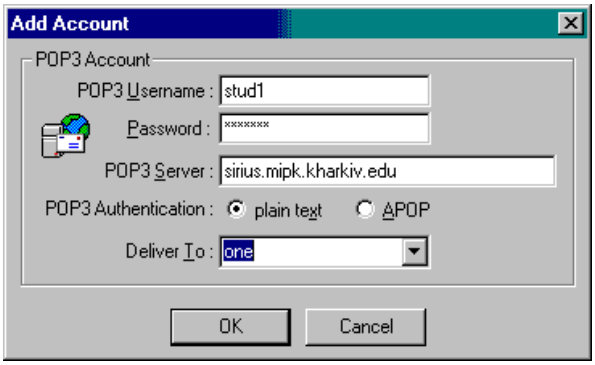


Рис. 11.21

5.4. Выполнить настройку почтовых агентов (Outlook Express) других машин локальной сети с указанием в качестве POP3 и SMTP серверов адреса машины Mail сервера Winroute

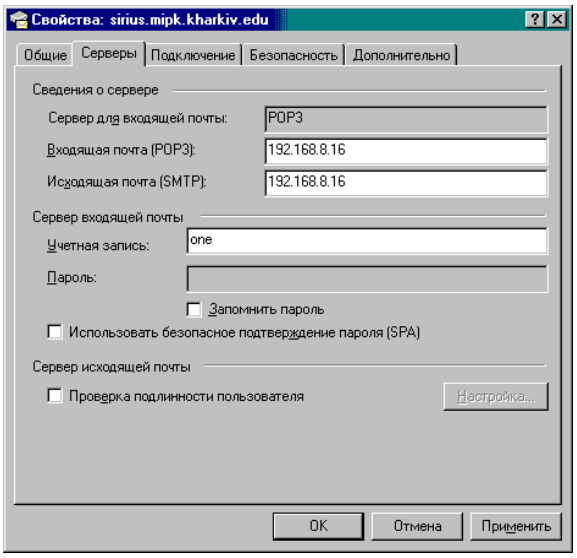


Рис. 11.22

5.5. Для тестирования почтового агента и сервера использовать адреса:

stud1@sirius.mipk.kharkiv.edu — stud12@sirius.mipk.kharkiv.edu, пароль: pas4you

Настраиваем почтовый сервер и Outlook на машине-клиенте точно по методичке, но Outlook все равно даже не может произвести соединение с настроенным на соседней машине POP-сервером. Предположили, что это из-за закрытого на машинах 110-го порта. Ставим 39-й порт (единственный открытый), но результат тот же. Почему?

6. Выполнить настройку DHCP–сервера Winroute локальной сети. Проверить его работоспособность в различных режимах (см. раздел «Настройка DHCP-сервера» данного пособия)

6.1. Включить DHCP–сервера Winroute: Settings/DHCP Server/DHCP Server Enabled

6.2. Добавить диапазон адрессов, например:

New Scope,

From: 192.168.8.50, To: 192.168.8.70, Mask: 255.255.255.0

Options:

Default Gateway, Specify value: 192.168.8.254

DNS Server, Specify value: 192.168.8.254

6.3. Зарезервировать IP–адрес за определенной станцией локальной сети, наример:

Add Lease,

IP address: 192.168.8.40

Reserved for,

Computer name,

Value: ewm30702

6.4. Выполнить настройку служб TCP/IP других станций локальной сети: диалог Настройка/Панель Управления/Сеть/”TCP/IP->Surecom…”, закладка «IP адрес», переключатель «Получить IP адрес автоматически». Запретить прохождение входящих и исходящих IP–пакетов на адрес 192.168.8.254 (иначе DHCP–сервер Winroute будет игнорироваться, а в качестве DHCP–сервера будет использоваться станция 192.168.8.254 под управлением MS Windows NT). Перезагрузить машину.

6.5. Проверить работоспособность DHCP–сервера Winroute, убедившись в корректности настройки служб TCP/IP других станций локальной сети при получении параметров от DHCP–сервера Winroute. Для этого, после перезагрузки станций, с помощью утилиты winipcfg, дать команду “Обновить все”, и, при появлении сообщений об ошибках, еще раз перезагрузить машину. Проверить следующие значения: “Сервер DHCP” (должен совпадать с IP–адресом DHCP–сервера Winroute), “IP–адрес” (должен быть выделен из диапазона, укзанного при настройке DHCP–сервера Winroute), “Основной шлюз” (должен соответствовать параметру, указанному при настройке DHCP–сервера Winroute), “Сервер DNS” (должен соответствовать параметру, указанному при настройке DHCP–сервера Winroute).

6.5.1. Вернуть настройки TCP/IP–служб станций локальной сети в исходное состояние:

IP–адрес: см. наклейку на системном блоке

Шлюз: 192.168.8.254

Маска: 255.255.255.0

Сервер DNS: 192.168.8.254

6.5.2. Удалить все фильтры прохождения пакетов в Winroute.

6.5.3. Перезагрузить машину.

Контрольные вопросы:

1. Особенности настройки различных сетевых служб.
2. Особенности программного комплекса Winrout.
3. Возможности управления доступом к внешним сетевым ресурсам

Практическая работа № 27

ЭЛЕМЕНТЫ УПРАВЛЕНИЯ СЕТЬЮ. ОБЩИЙ ДОСТУП К РЕСУРСАМ

Цель работы: Научиться управлять сетью, организовывать общий доступ к сети.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия.

Ход работы: Центр управления сетями и общим доступом и сетевое размещение:

Чтобы открыть окно Центр управления сетями и общим доступом нажмите на кнопку Пуск, откройте Панель управления, из списка компонентов панели управления выберите категорию Сеть и Интернет, а затем перейдите по ссылке Центр управления сетями и общим доступом (рис. 12.1).

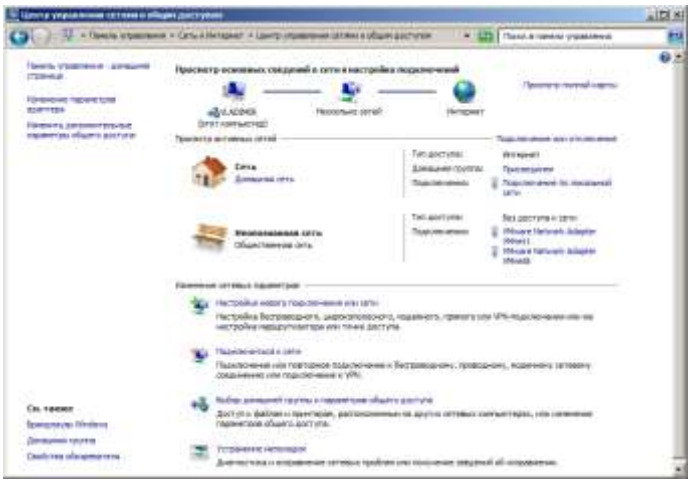


Рис. 12.1. Окно Центр управления сетями и общим доступом

Если в данном окне, нажать на значок **Домашняя сеть**, то вы сможете изменить параметр «сетевое размещение» (рис. 12.2).

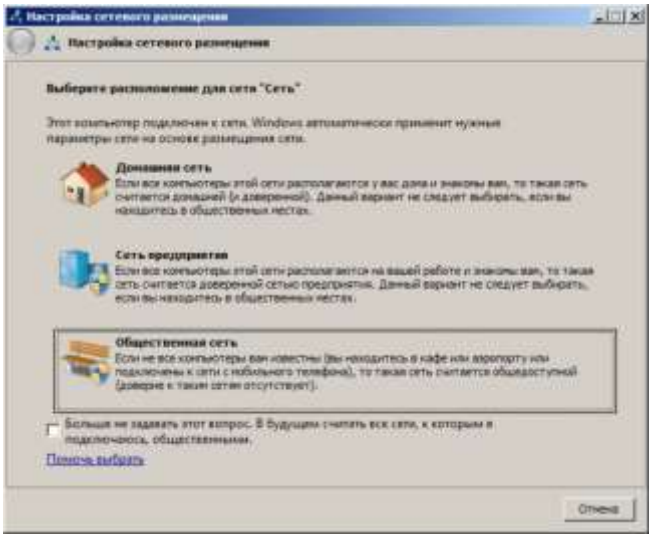


Рис. 12.2. Окно Настройка сетевого размещения

Существует четыре типа сетевого размещения:

- **Домашняя сеть** — для использования компьютера в домашних условиях (где пользователи хорошо знают друг друга). Сетевое обнаружение включено.

- **Сеть предприятия** — для сети небольшого офиса. Сетевое обнаружение включено.
- **Общественная сеть** — для использования компьютера в общественных местах (кафе, клуб, вокзал, аэропорт). Сетевое обнаружение отключено.
- Вариант **Доменная сеть** выбирается, если компьютер присоединён к домену Active Directory. Конфигурация брандмауэра, сетевого обнаружения и сетевой карты определяется групповой политикой безопасности.

Карта сети и просмотр сетевых подключений

В окне **Центр управления сетями и общим доступом** нажмите на гиперссылку **Просмотр полной карты** (рис. 3). Карта сети – это графическое представление вашей сети. В нашем примере стационарный ПК VLADIMIR через роутер WNR612v2 подключен к Интернет. Так же к Интернет через Wi-Fi подключен ноутбук MARIA.

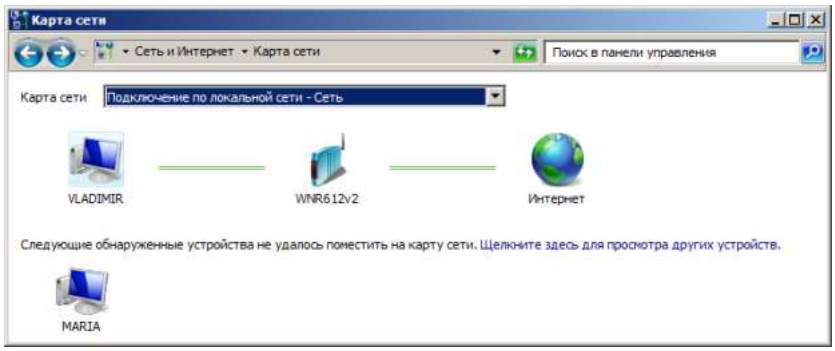


Рис. 12.3. Карта сети

В окне Центр управления сетями и общим доступом нажмите на гиперссылку Изменение параметров адаптера или нажмите на кнопку Пуск для открытия меню, в поле поиска введите Просмотр сетевых подключений (рис. 12.4).

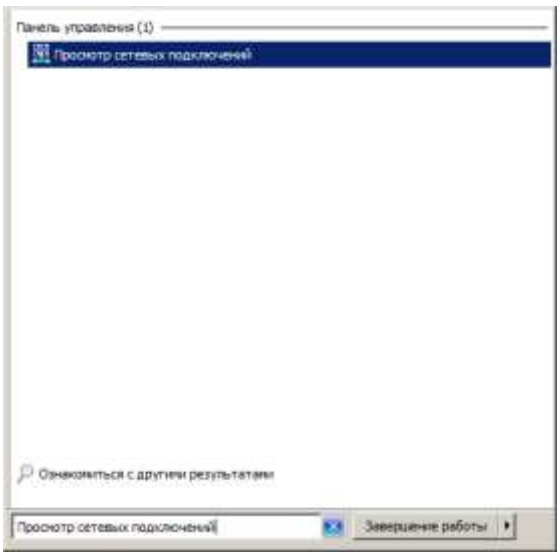


Рис. 12.4. Поиск сетевых подключений

После установки драйвера сетевого адаптера, операционная система Windows 7 пытается автоматически сконфигурировать сетевые подключения на локальном компьютере. В качестве примера, на рис. 12.5 показаны сетевые подключения двух виртуальных компьютеров, стационарного (физического) ПК и Bluetooth устройства.

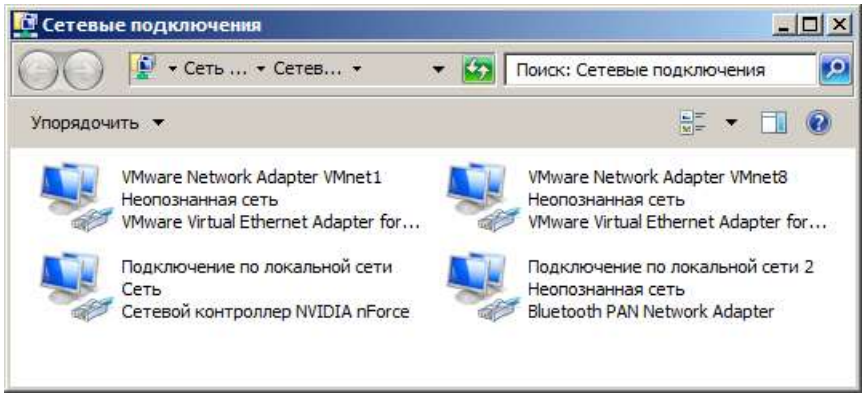


Рис. 12.5. Окно Сетевые подключения

Сведения о сетевом подключении

Нажмите на кнопку **Пуск** и в поле поиска введите **Просмотр сетевых подключений.**

Нажмите правой кнопкой мыши на интересующем вас сетевом подключении и из контекстного меню выберите команду **Состояние-Сведения**. В данном окне мы можете увидеть IP и MAC адреса ПК, маску подсети и ряд другой информации о вашем сетевом соединении (рис.12.6).

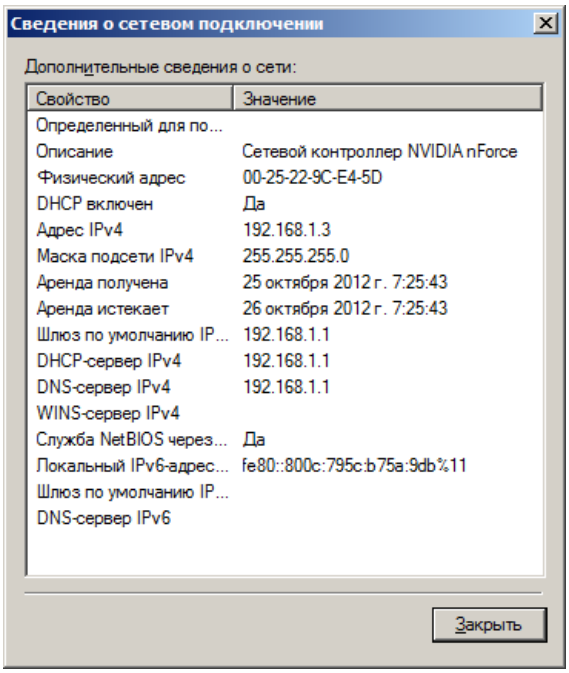


Рис. 12.6. Сведения о сетевом подключении

Сетевые профили и сетевое обнаружение

Выполните команду **Пуск — Панель управления-Сеть и Интернет- Центр управления сетями и общим доступом—Изменить дополнительные параметры общего доступа** (рис. 12.7). При помощи окна **Дополнительные параметры общего доступа**, вы можете указать разные настройки общего доступа для любого из трех сетевых профилей ПК (**Домашний** или **Рабочий**, а также **Общий** профиль).

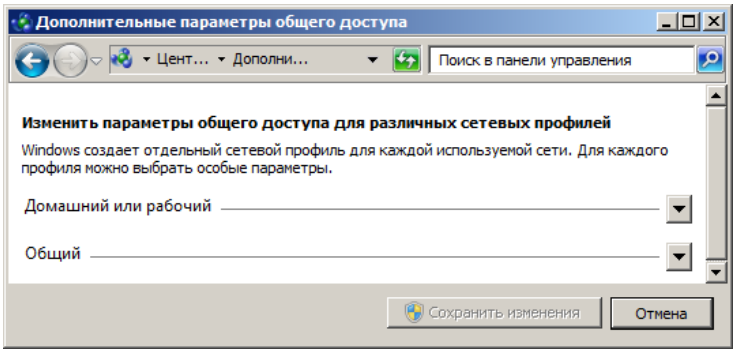


Рис. 12.7. Окно Дополнительные параметры общего доступа

Разверните ваш сетевой профиль (рис. 12.8)

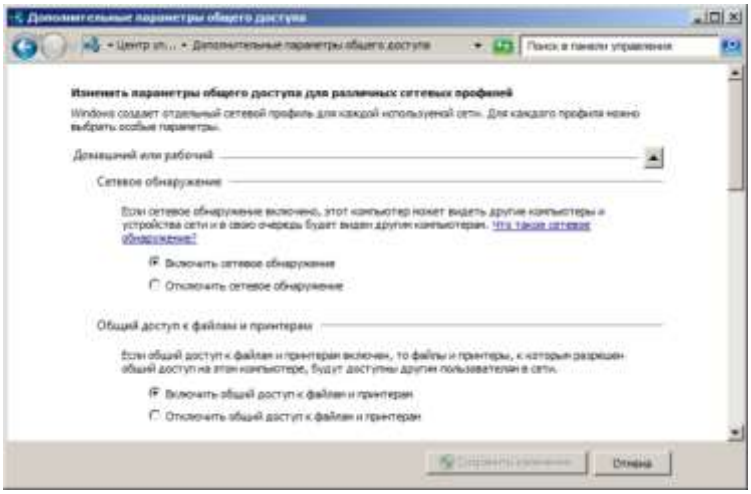


Рис. 12.8. В окне показана часть сетевого профиля Домашний или рабочий

Здесь по умолчанию активирован переключатель Сетевое обнаружение, который определяет, могут ли другие компьютеры в сети обнаруживать компьютер пользователя, и может ли он их видеть.

Подключение общего доступа к папкам

Командой **Панель управления-Сеть и Интернет-Центр управления сетями и общим доступом-Дополнительные параметры общего доступа** разверните ваш сетевой профиль и включите переключатель**Включить общий доступ к файлам и принтерам** (рис. 12.9). Нажмите на кнопку **Сохранить изменения**.

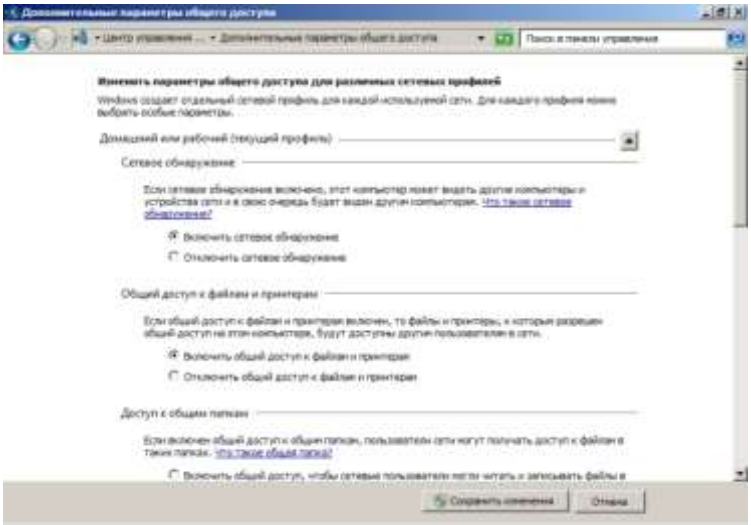


Рис. 12.9. Активируем переключатель Включить общий доступ к файлам и принтерам

Совет

Общий доступ к любому из файлов или к какой-либо папке можно организовать, переместив их в папку **Общие**. Найти ее можно, если в строку поиска вставить **%USERS%\Public (%Пользователи%\Общие** (рис. 12.10).

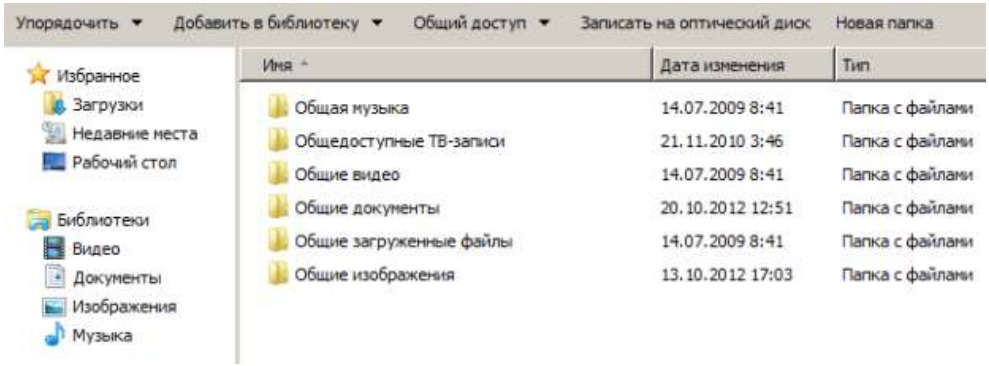


Рис. 12.10. Содержание папки Общие

Итак, создайте папку, для которой будет предоставлен общий доступ, например, на рабочем столе папку **PC_1 Общая** (рис. 12.11).

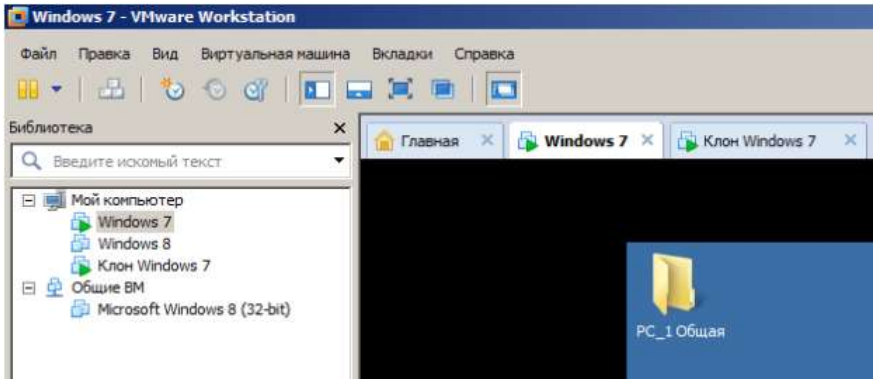


Рис. 12.11. Создаем папку для общего доступа к ней по виртуальной сети

Откройте **Проводник** Windows, выделите эту папку, нажмите на ней правой кнопкой мыши и из контекстного меню выберите команду **Свойства-Доступ**, затем нажмите на кнопку **Общий доступ** для предоставления разрешений пользователя и группам (рис. 12.12).

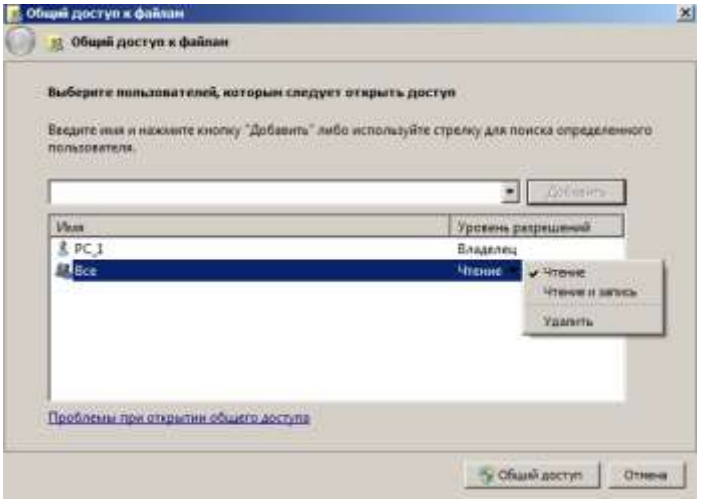


Рис. 12.12. Окно Общий доступ к файлам

По умолчанию администратор ПК, т.е. **Владелец** папки, имеет к ней полный доступ. Он может добавить любого пользователя папки и назначить ему права на эту папку (**Чтение** или **Чтение и запись**). В заключение нажмите на кнопку **Общий доступ** (рис. 12.13). Это, так называемый, простой доступ к папке.

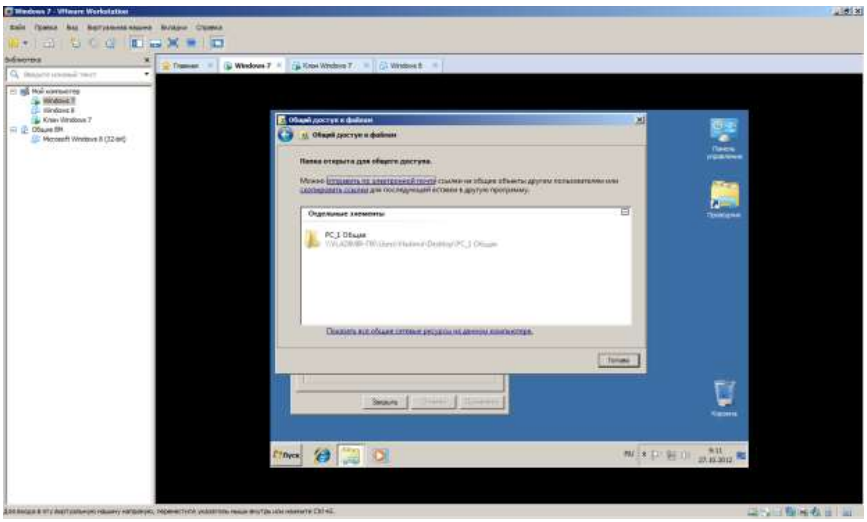


Рис. 12.13. Завершение предоставления общего доступа к папке

Для предоставления расширенного доступа к той же папке в окне свойств папки, нажмите на кнопку **Расширенная настройка** (рис. 12.14 и рис. 12.15).

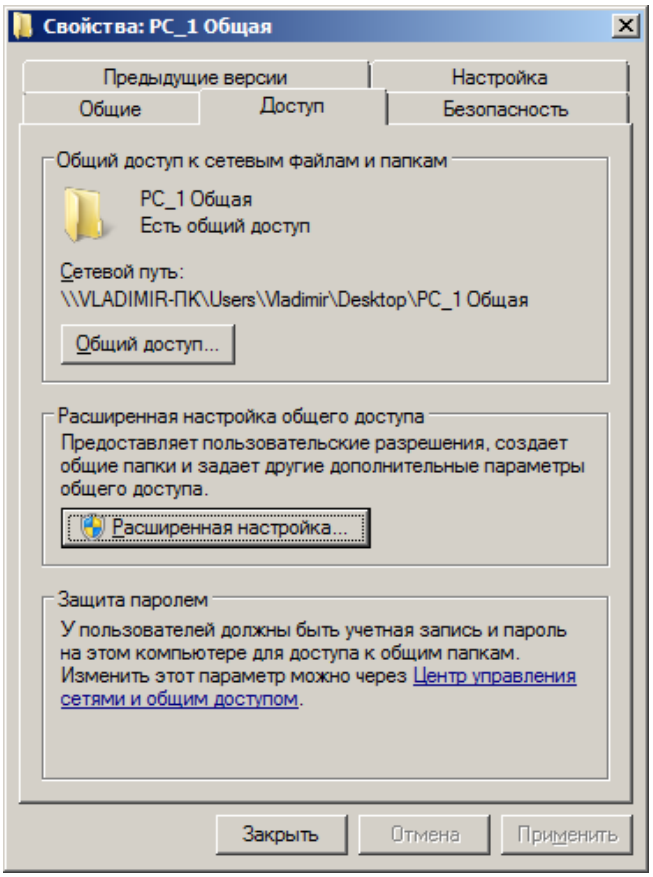


Рис. 12.14. Окно свойств папки

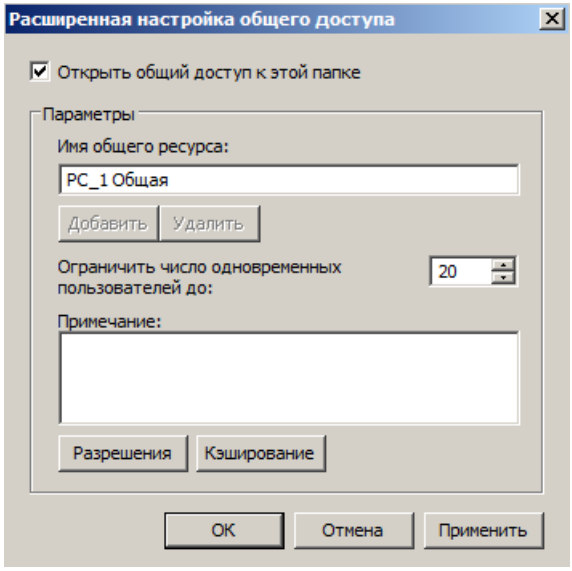


Рис. 12.15. Расширенная настройка общего доступа папки PC_1 Общая

В этом окне вы можете настраивать разрешения для папки, а также, используя кнопку **Добавить**, выбирать тип объекта (рис. 12.16).

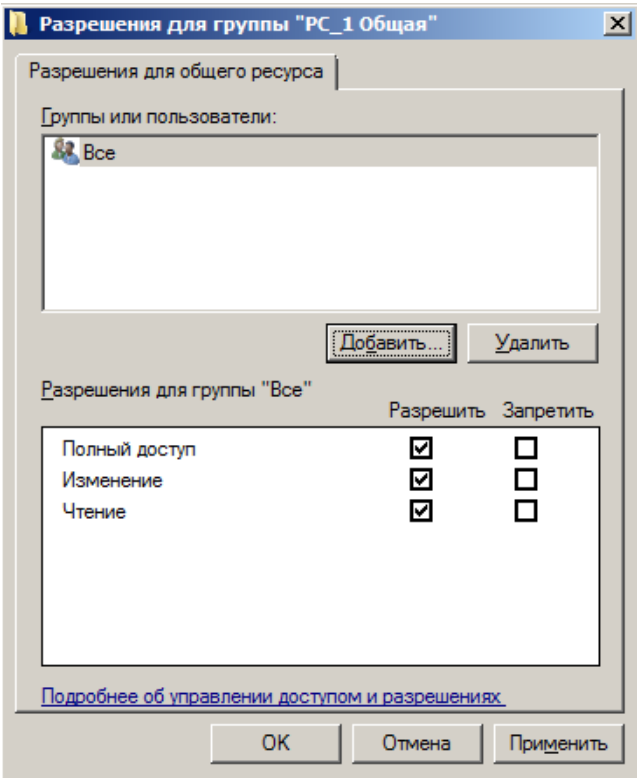


Рис. 12.16. В этом окне все пользователи получили полный доступ к папке

Теперь давайте войдем в виртуальный **PC_2 (клон)**, запустим там программу **Проводник** и в панели навигации выберем **Сеть** (рис. 12.17).

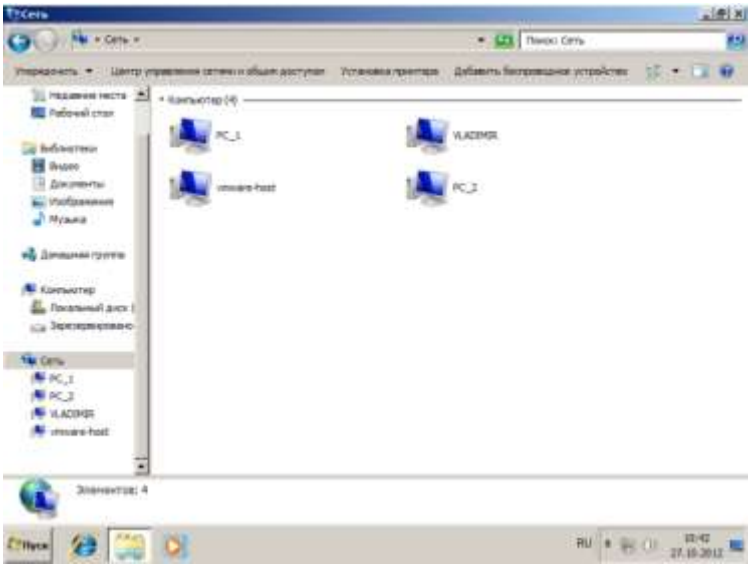


Рис. 12.17. Список доступных компьютеров виртуальной сети

Теперь выберите компьютер, папку которого вы открывали для использования общего доступа, например, PC_1. Общие папки будут отображены в проводнике Windows, как показано на рис. 12.18.

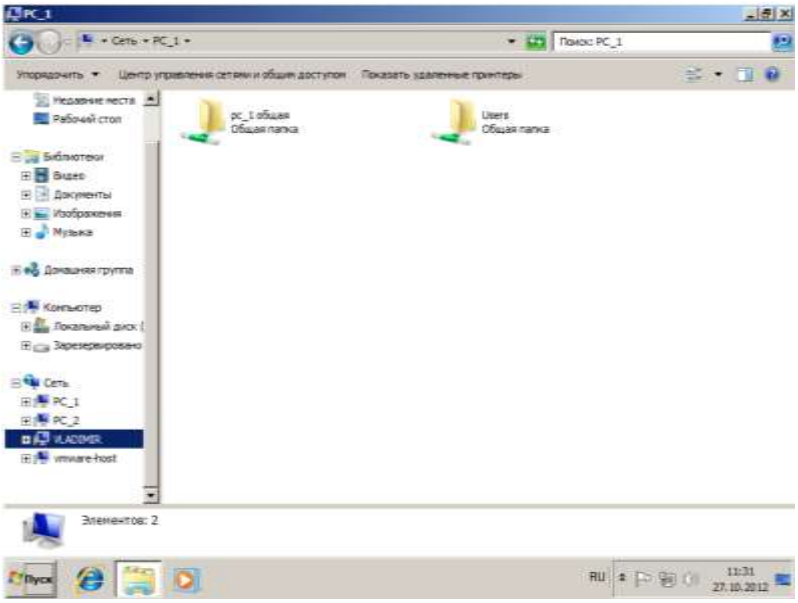


Рис. 12.18. Общедоступные папки на PC_1

Общий доступ с парольной защитой

В целях безопасности, по умолчанию доступ к общим папкам защищен паролем. Для того чтобы отключить доступ с парольной защитой, выполните следующее: откройте окно **Дополнительные параметры общего доступа**, разверните сетевой профиль и в группе **Общий доступ с парольной защитой** активируйте переключатель **Отключить общий доступ с парольной защитой** — рис. 12.19.

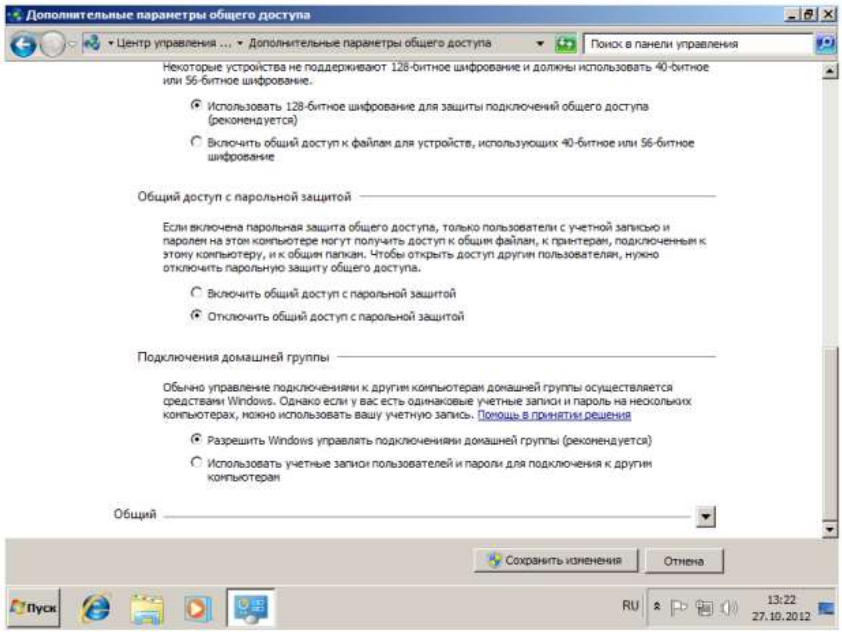


Рис.12.19. Отключение парольной защиты для общего доступа

Здесь же можно установить переключатель **Разрешить Windows управлять подключениями домашней группы**.

Краткие итоги

Мы научились получать сведения о сетевом подключении и настраивать доступ к ресурсам сети. Познакомились с понятиями: сетевые профили и сетевое обнаружение, центр управления сетями и общим доступом, сетевое размещение, карта сети, просмотр сетевых подключений и ряд других, связанных с элементами управления сетью в интерфейсе ОС Windows 7.

Задание. Произведите отключение пользователя от папки с общим доступом

Контрольные вопросы:

1. Что такое компьютерная сеть?
2. Что необходимо для создания компьютерных сетей?
3. Какова основная задача, решаемая при создании компьютерных сетей?
4. Что такое протоколы? Для чего они предназначены?
5. По какому принципу компьютерные сети делятся на локальные и глобальные?
6. Что такое интерфейсы?
7. Что такое серверы сети?
8. Какие сети называются одноранговыми?
9. Что такое рабочие станции?
10. Какие кабели можно использовать в качестве передающей среды в проводных сетях?
11. Что используются в качестве передающей среды в беспроводных локальных сетях?
12. Что представляет технология Ethernet?
13. Что такое сетевой адаптер?

Практическая работа № 28-29

ПОСТРОЕНИЕ СОСТАВНОЙ СЕТИ.

Цель работы: Получить навыки по моделированию локальных компьютерных сетей.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия.

Общие сведения:

1. Общие сведения о среде Cisco Packet Tracer

В процессе проектирования компьютерных важным этапом является исследование технических решений на предмет выполнения ими заданных функций. Такое исследование может быть проведено двумя способами: натурным экспериментом и компьютерным имитационным моделированием. В первом случае проектировщики, используя реальное оборудование, собирают требуемую компьютерную сеть и проводят необходимые эксперименты. Очевидно, что стоимость таких экспериментов достаточно высока и определяется в большей степени стоимостью используемого оборудования. С целью сокращения стоимости экспериментов используется компьютерное имитационное моделирование, в котором вместо реального оборудования используется их программные аналоги.

На рынке программного обеспечения существует множество различных сред имитационного моделирования компьютерных сетей. Наибольшую популярность получили две среды имитационного моделирования компьютерных сетей: GNS31 и CISCO Packet Tracer2.

Первая среда является свободно распространяемой и реализует имитационное моделирование путем виртуализации реального оборудования. Вторая среда распространяется свободно, но в рамках сетевых академий компании Cisco systems, Inc, и моделирует только оборудование этого производителя. В рамках практической работы, в основном, будет использоваться среда CISCO Packet Tracer.

2. Графический интерфейс среды Cisco Packet Tracer

Запустив программу, пользователь видит основное окно рисунок 13.1 содержащее:

- Основное меню;
- Панели инструментов (главную, вертикальную и нижнюю);
- Переключатели режимов моделирования (реального времени и пошаговый) и видов схем (логическая и физическая).

Рис.13.1

Основное меню программы содержит пункты: Файл (File), Редактирование (Edit), Настройки (Options), Вид (View), Утилиты (Tools), Дополнения (Extensions), Помощь (Help).

Пункт меню «Файл» используется для выполнения операций с текущим файлом (открыть, закрыть, сохранить, распечатать и т.п.), а также позволяет завершить работу среды.

В пункте «Редактирование» содержатся стандартные операции с буфером обмена (скопировать выделенный объект в буфер, вырезать, вставить), а также управления действиями в среде (отменить и повторить последнее действие).

Пункт «Настройки» позволяет сконфигурировать среду моделирования и пользовательское окружение.

Пункт меню «Вид» настраивает масштаб отображения объектов в рабочей области и режим отображения панелей инструментов.

В пункте «Утилиты» содержатся ссылки на вывод панели графических объектов и создания собственного устройства. Управлять дополнениями возможно в меню «Дополнения». К таким дополнениям, например, относится взаимодействие между несколькими средами моделирования.

Панели инструментов по умолчанию отображаются три: главная, вертикальная и нижняя.

Доступна также панель графических примитивов.

Главная панель инструментов дублирует некоторые пункты основного меню, обеспечивая быстрый и удобный доступ к созданию нового файла, сохранения и печати текущей схемы, отображения окна дополнения «Самопроверка заданий (Activity Window)», действий с буфером обмена, изменения масштаба отображения схемы, доступа к панели графических примитивов и создания нового объекта моделирования.

Вертикальная панель инструментов содержит действия, выполняемый с объектами моделируемой схемы сети таблица 13.1

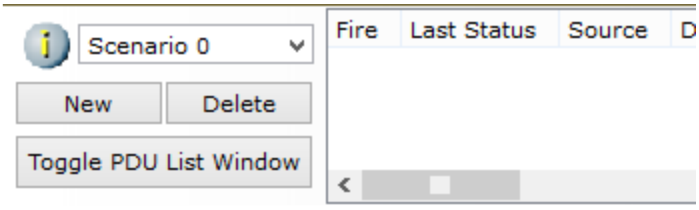
Кнопки вертикальной панели инструментов Таблица13.1

	Инструмент **Select** (быстрый доступ – Esc). Позволяет выделить один или несколько объектов моделируемой компьютерной сети (логической или физической топологии)
	Инструмент **Move Layout** (быстрый доступ - M). Используется для прокрутки схемы модулируемой сети в основном окне рабочего пространства. Для выполнения этого действия могут также использоваться полосы прокрутки.

	Инструмент **Place Note** (быстрый доступ - N). Позволяет добавить в текущую моделируемую схему текстовую надпись.
	Инструмент **Delete** (быстрый доступ – Del). Переключает в режим удаления выделяемых объектов схемы компьютерной сети.
	Инструмент **Inspect** (быстрый доступ – I). Позволяет просматривать таблицы состояния (таблица маршрутизации и т.п.) объектов моделируемой компьютерной сети.
	Инструмент **Resize Shape** (быстрой доступ – Alt+R). Используется для изменения размеров графических объектов, размещаемых на схеме с использованием панели «Графические объекты».
	Инструмент **Add Simple PDU** (быстрый доступ – P). Позволяет создать эмуляцию простой передачи пакета данных (ICMP, ping) от одного устройства сети к другому.
	Инструмент **Add Complex PDU** (быстрый доступ – P). Создает эмуляцию передачи пакета данных от одного устройства к другому. Позволяет задать параметры пакета (тип протокола, исходящий порт и т.п.).

Нижняя панель инструментов позволяет создавать объекты исследуемой схемы компьютерной сети рисунок 13.2а, а также задавать задачи по эмуляции передачи данных в ней рисунок 13.2б.

а) создания объектов компьютерной сети и



б) задачи по эмуляции передачи данных по сети

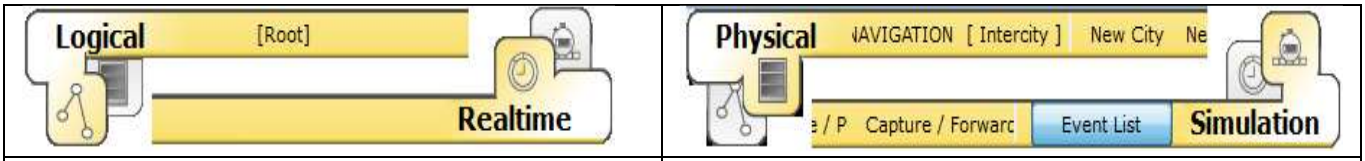
Рис. 13.2 – Элементы нижней панели инструментов:

В области задач по моделированию передачи данных по сети располагается перечень действий, созданных кнопками Add Simple PDU и Add Complex PDU. Таких перечней (сценариев) пользователь может создать несколько.

Межу верхней панелью инструментов и рабочим пространством находится строка *переключения режима отображения моделируемой сети*: логическая или физическая топология рисунок 13.3. В режиме «логическая сеть» располагаются сетевые объекты и указываются связи между ними. В режиме «физическая сеть» указывается расположение сетевых объектов и каналов связей в помещениях (как они расположены, в каких стойках и т.п.). В этой же строке располагаются кнопки управления отображением: <Root> - уровень детализации, «New Cluster» - создать объединенное устройство, «Set Tiled Background» - установить фон рабочей области, «NAVIGATION» - навигация между уровнями отображения физической сети (Район, Город, этаж).

После рабочего пространства располагается строка *переключения режимов моделирования*: реального времени или пошаговое моделирование рисунок 13.3. В режиме пошагового моделирования пользователю предоставляется возможность посмотреть, как передается информация между сетевыми устройствами в заданных им ситуациях.

В реальном масштабе времени указывается лишь состояние сетевых устройств, результаты передачи отображаются «по факту».



а – логическая сеть и режим реального времени	б – физическая сеть и режим пошагового выполнения

Рис. 13.3 – Переключатели режимов рабочей области и модельного времени

3. Работа с объектами компьютерной сети

Для размещения сетевого объекта на схеме необходимо выбрать в нижней панели инструментов его класс (маршрутизаторы (routers), коммутаторы (switches), концентраторы (hubs), беспроводные устройства (wireless devices), соединительные кабели (connections), терминальные устройства (End devices), «интернет» (WAN emulation), пользовательские объекты и многопользовательское соединение, а затем модель (например, маршрутизатор 1841 или Laptop-PT). Выбрав необходимое оборудование его можно «перетащить» в рабочую область или щелчком мышки указать место в рабочей области, куда следует его поместить.

Для соединения сетевых устройств необходимо выбрать класс «Соединительные кабели», далее выбрать необходимый тип кабеля (или выбрать «автоматическое определение»), указать начальное устройство, выбрать один из его сетевых портов рисунок 13.4, затем указать оконечное устройство и один из его портов. В случае применения объекта «Автоматическое определение типа сетевого кабеля», порт и тип кабеля будут выбираться автоматически (номер порта будет выбираться в порядке возрастания).

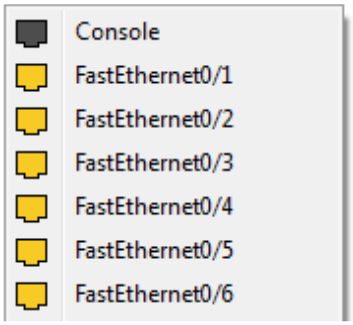


Рисунок 13.4 – Меню выбора сетевого интерфейса коммутатора

Конфигурирование сетевого устройства производится по двойному щелчку на нем рисунок 13.5(а-в)

В открывшемся окне пользователь может включить/выключить устройство (соответствующим тумблером на его изображении в области «Physical Device View»), изменить аппаратурную конфигурацию добавив или удалив модули, используя область MODULES, изменить картинку для отображения этого устройства в режиме логической сети и в режиме физической сети.

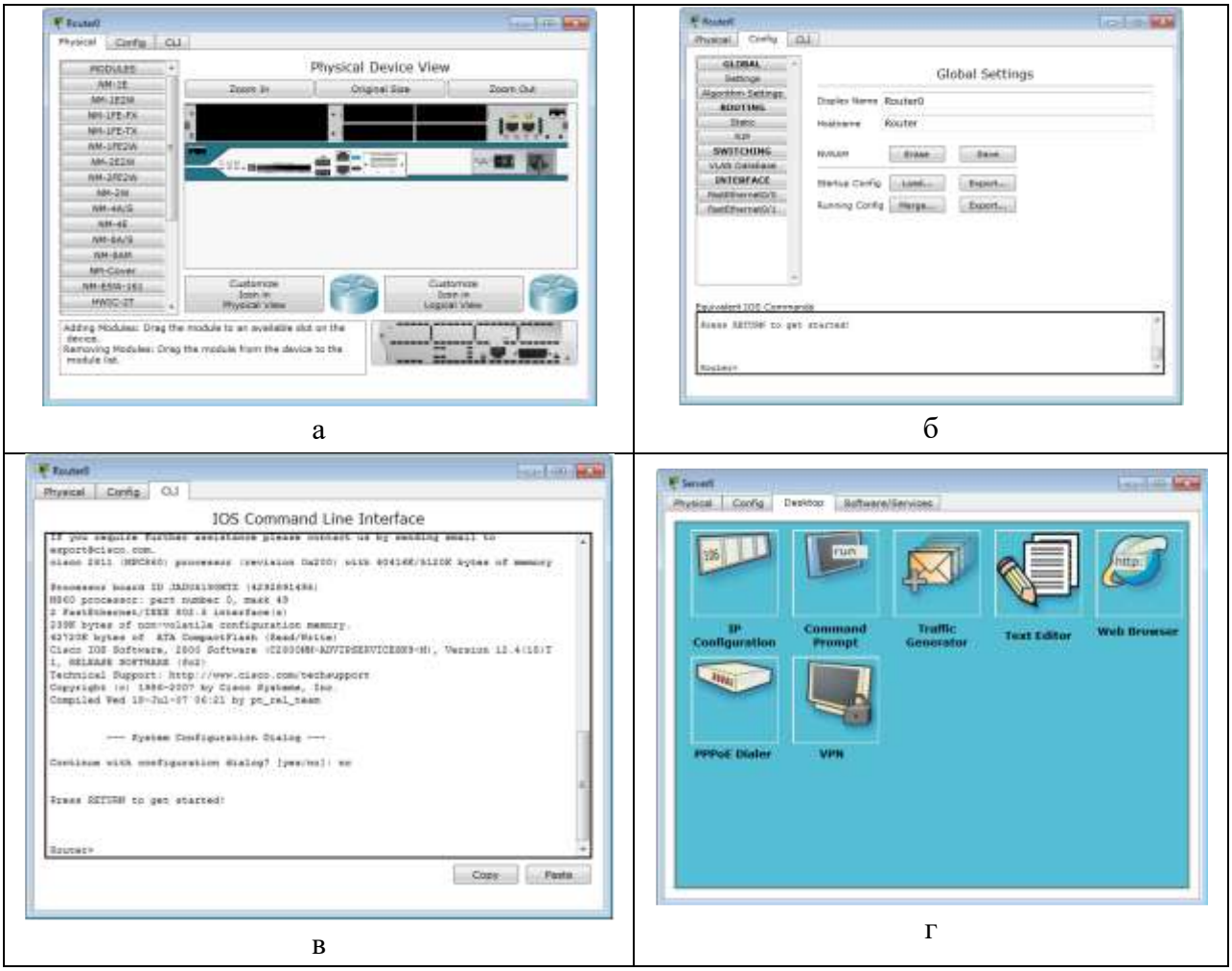
Выбрав вкладку «Config» пользователь может задать некоторые конфигурационные параметры (например, настроить сетевой интерфейс, определить имя устройства и т.п.).

На вкладке «CLI» предоставляется доступ к командному интерфейсу устройства (если он предусмотрен).

Для оконечных устройств реализованы дополнительные вкладки например, рисунок 13.5г.

На вкладке «Desktop» расположены эмуляторы работы некоторых утилит рабочего стола (командная строка, интернет-браузер и т.п.). «Software/Services» - конфигурирование программно-

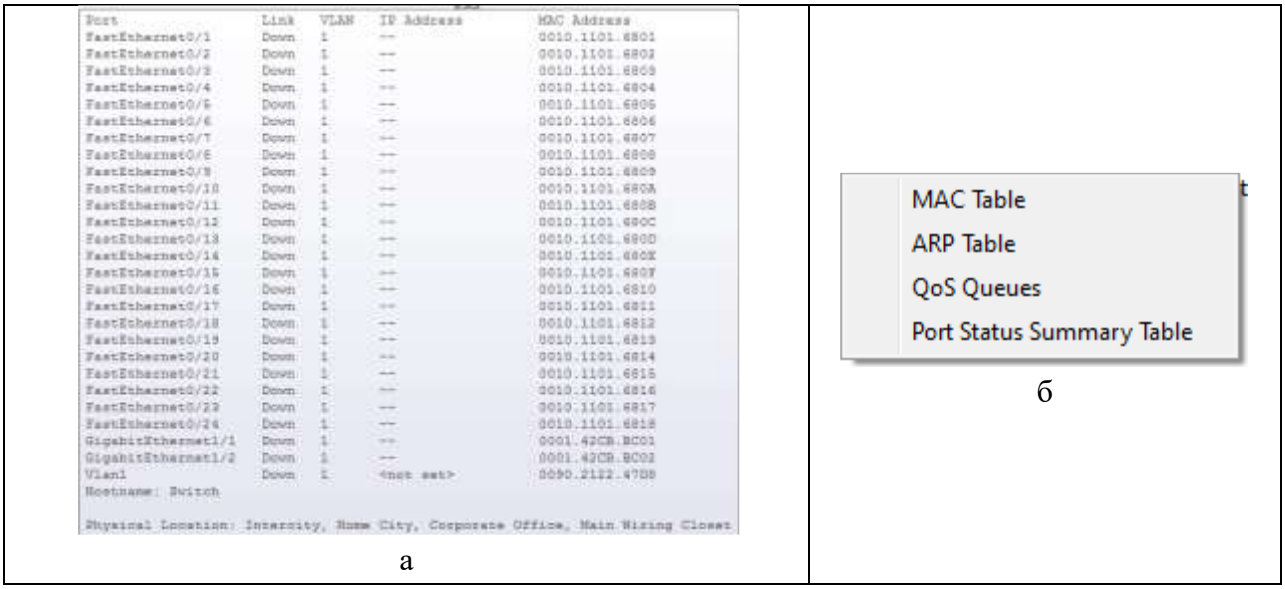
го обеспечения, которое должно быть установлено на реально действующем оконечном устройстве.



а б в г

Рис 13.5 – Окно конфигурирования сетевого устройства

Наведя курсор мышки на объект и подождав несколько секунд пользователь получит краткую информацию о состоянии объекта. Более подробную информацию пользователь может получить воспользовавшись инструментом «Inspect». Следует отметить, что всплывающая подсказка при наведеии мыши соответствует пункту меню «Port Status Summary Table» инструмента «Inspect».



а б

Рисунок 13.6 – Всплывающая подсказка (а) и меню инструмента Inspect (б)

Многопользовательская работа

Среда CISCO Packet Tracer позволяет организовать обмен информацией меду несколькими моделируемыми сетями. При этом сети могут моделироваться как на одном, так и на разных компьютерах. В последнем случае для взаимодействия моделируемых сетей используется физическая сеть, соединяющая компьютеры.

Настройка среды удалённого взаимодействия (многопользовательского режима) производится в меню «Extencions»->«Multiuser». Настроить необходимо сетевой порт, который будет использоваться на компьютере для взаимодействия с другими средами имитационного моделирования, а также поведение системы моделирования при создании новых исходящих и входящих соединений.

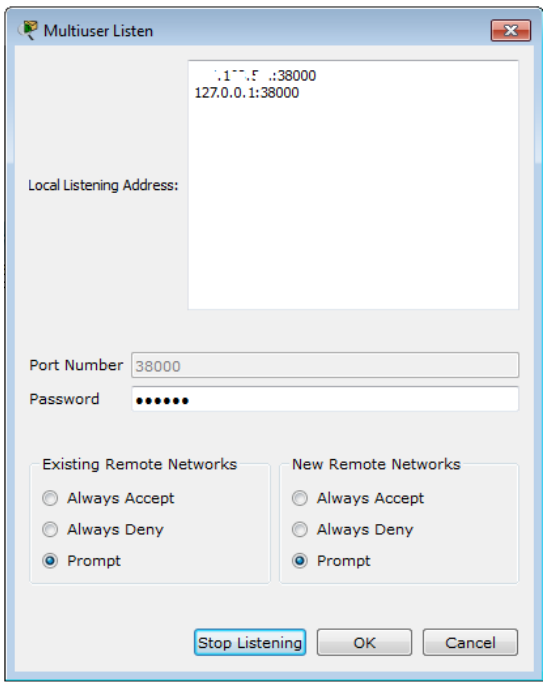


Рис. 13.7 – Окно настройки удалённого взаимодействия

Для обозначения взаимодействия с другими средами моделирования используется объект «Remote network» из класса «Multiuser Connections». В свойствах этого объекта указывается тип создаваемого подключения (входящий или исходящий, в зависимости от того, какая система имитационного моделирования инициирует подключение), а также параметры второй среды имитационного моделирования.

Взаимодействие двух систем моделирования всегда начинается с установления связи между ними. И лишь после успешного установления связи, начинается процесс имитационного моделирования, в котором данные передаются от одной части сети к другой.

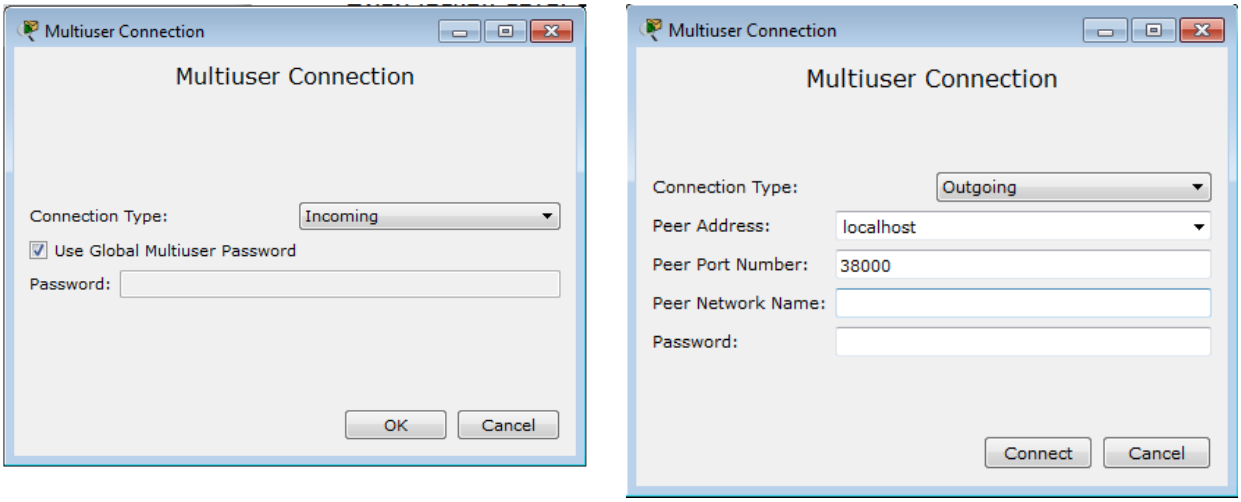


Рис. 13.8 – Окна конфигурирования удалённого подключения

Пошаговая отладка передачи информации в исследуемой сети

Отладка исследуемой сети может производиться двумя способами: имитируя деятельность администратора с реальным оборудованием и с применением средств моделирования. В первом случае пользователь среды может выполнять необходимые действия над сетевыми объектами и принимать решения о функциональности собранной им сети. Во втором случае используются встроенные средства среды имитационного моделирования, которые позволяют пошагового наглядно продемонстрировать этапы передачи информации по сети. Анализируемые задания по передачи данных по сети объединяются в сценарий. В среде допускает создавать несколько сценариев и переключаться между ними для анализа работы сети.

Для создания задания по передаче данных по протоколу ICPM (ping) используется кнопка «Add Simple PDU». Пользователь задает начальный сетевой узел (который будет генерировать данные) и конечный сетевой узел. В результате автоматически создается одно задание в текущем сценарии.

Для формирования передач данных по сети с указанием параметров передаваемой информации (протокол, порт и т.п.) используется кнопка «Add Complex PDU». Нажав на соответствующую кнопку в вертикальной панели пользователь должен указать протокол передачи, источник передаваемой информации и задать параметры: сетевой порт через который данные будут передаваться, адрес источника и получателя, порт получателя и отправителя, время жизни и обслуживания, номер пакета в последовательности, размер пакета, а также определить будет ли эта передача носить разовый характер или повторяться в течение некоторого периода времени.

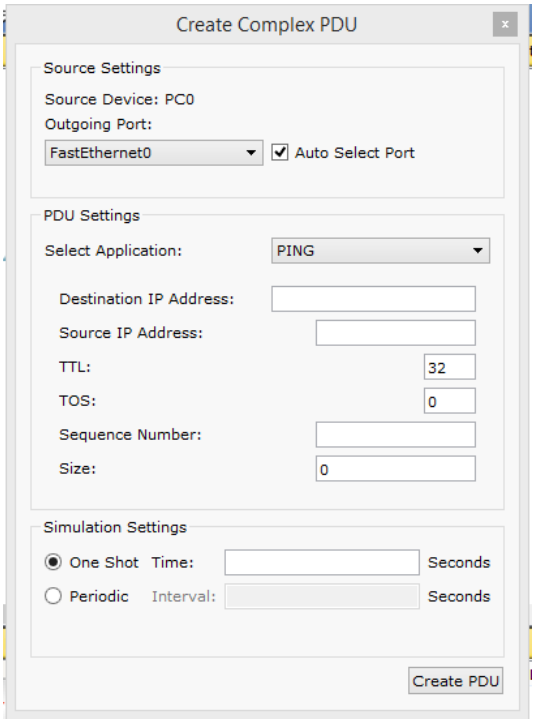


Рис. 13.9 – Окно настроек параметров передачи информации по сети

Результаты выполнения заданий по передаче данных отображаются в области сценариев. В режиме реального времени результаты выполнения заданий выводятся сразу же по окончании имитации.

В случае, если пользователь попытается при создании простого задания указать устройство (источник или приемник), не имеющего настроенного сетевого интерфейса, то сразу будет выдано сообщение об ошибке.

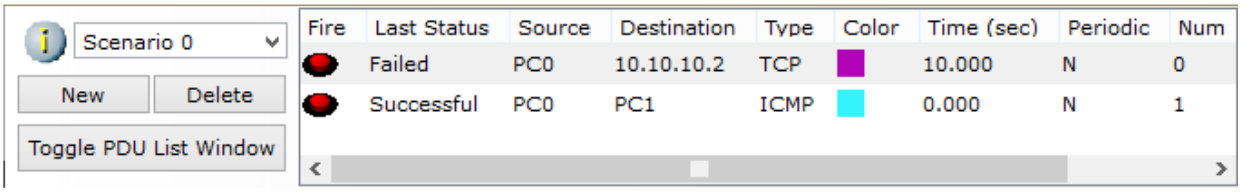


Рис. 13.10 – Пример результатов выполнения сценария передачи данных (в реальном времени)

Переключившись в режим пошагового выполнения пользователь получает возможность наглядно посмотреть каким образом передаются данные по сети (согласно созданным заданиям).

Переход к следующему шагу производится нажатием на кнопку «Capture / Forward». Перейти к предыдущему шагу можно нажав на клавишу «Back». Нажав на кнопку «Auto Capture / Play» запускается автоматический переход к следующему шагу (время перехода указывается в области настроек пошагового выполнения, рис.13.11). Кнопка «Power Cycle Device» - сбрасывает исследуемую сеть в исходное состояние. В панели настроек можно указать дополнительные фильтры на вывод информации о передаче данных по сети (указать интересующие протоколы).

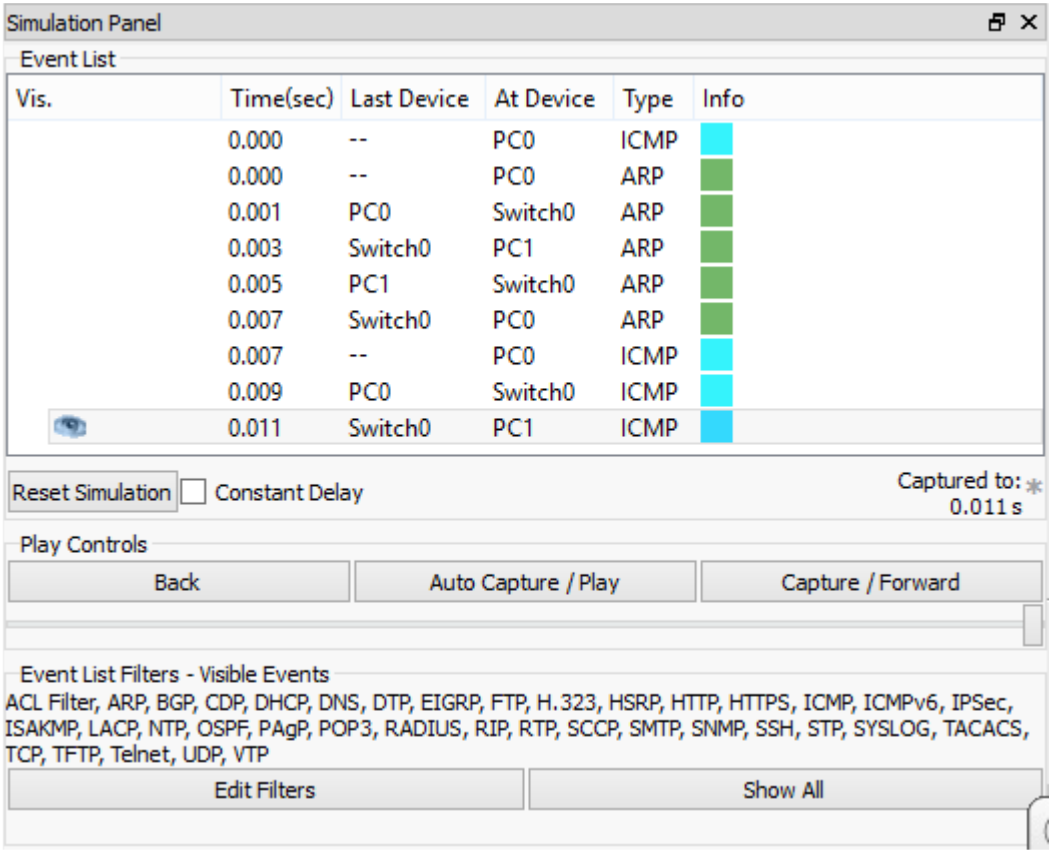


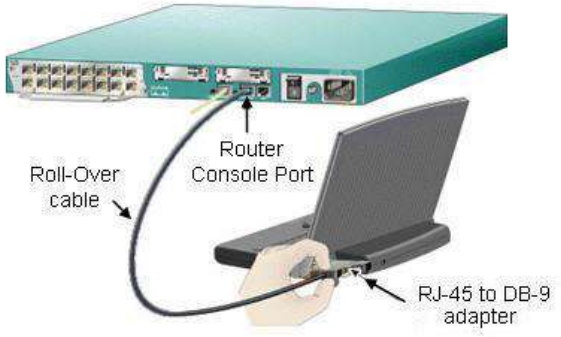
Рис. 13.11 – Панель настроек пошагового моделирования

Командная строка управления устройствами (CLI)

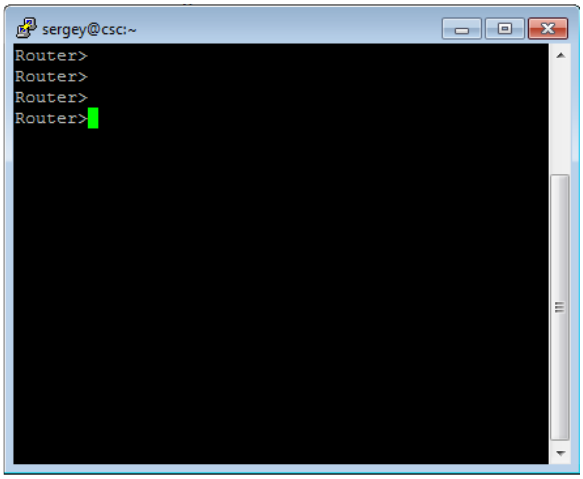
Большинство сетевых устройств компании CISCO допускают конфигурирование. Для этого администратор сети должен подключиться к устройству используя: прямое кабельное (консольное) подключение, удалённое терминальное подключение или Web-интерфейс. Задавая параметры устройства, администратор сети определяет его поведение и настраивает порядок его работы.

Подключившись к устройству напрямую рисунок 12а или через удалённый терминал рисунок 12б пользователю предлагается командная строка (Command Line Interface – CLI), в которой он может задавать необходимые действия и, тем самым, определять параметры конфигурации оборудования.

В среде моделирования интерфейс командной строки для устройств доступен в окне настроек параметров сетевого устройства на вкладке «CLI». Это окно имитирует прямое кабельное (консольное) подключение к сетевому устройству. Создав новое устройство в этом окне можно наблюдать процесс его загрузки (сервисные сообщения).



а



б

Рис. 13.12 – Пример подключения к сетевому устройству.

Для управления сетевыми устройствами чаще всего используется интерфейс командной строки.

Принципы настройки оборудования с использованием Web-интерфейса аналогичны и отличаются лишь внешним видом. Следует отметить, что при подключении к устройству напрямую для начала сессии администратору необходимо нажать хотя бы один раз клавишу <ENTER>. При других способах подключения сессия начинается автоматически.

Общие сведения о командной строке

Командная строка представляет собой место, куда пользователь вводит символы, формирующие управляющее воздействие. Это место обозначается: приглашением и следующим за ним курсором (который может мигать). Приглашение командной строки обычно содержит имя сетевого узла и один (или несколько) специальных символов, отвечающих за подсказку администратору, в каком режиме сейчас находится командная строка или в какой части конфигурационных параметров сейчас будут производиться действия. Ввод команд завершается нажатием клавиши <ENTER>.

Команда начинает интерпретироваться (исполняться) после нажатия клавиши <ENTER>. Если команда написана правильно, то будет выполнено соответствующее действие. Иначе появится сообщение об ошибке, указывающее на некорректное место в командной строке.

Пользователь может набрать несколько букв в командной строке и нажать клавишу <TAB>. В этом случае команда или её параметр будет продолжен (если набранная последовательность однозначно определяет их) или не произойдет никаких действий. Проверить почему команда или параметр не были продолжены можно с помощью контекстной помощи. Набрав ?, администратору будут показаны возможные альтернативы.

Для отмены действия, выполненного какой-либо командой, необходимо выполнить её ещё раз указав перед ней команду no рисунок 13.14

В случае, если в результате выполнения команды выводится информация, не помещающаяся в одном окне, то в нижней строке выводится фраза –More--. Построчная прокрутка текста осуществляется клавишей <Enter>. Постраничная прокрутка – клавише <Пробел>.

Подробнее о командах по управлению сетевых устройств CISCO следует прочитать в официальной документации.

Режимы работы с устройством при использовании CLI

Работа с командной строкой осуществляется в нескольких режимах (см. таблицу 13.2). Едиными для всех устройств режимами являются: пользовательский, привилегированный и глобальной конфигурации. Остальные режимы зависят от типа устройства и его внутренней организации.

Режимы командного интерфейса Таблица 13.2

Режим	Переход в режим	Вид командной строки	Выход из режима
Пользовательский (User EXEC)	Подключение	Router>	logout
Привилегированный (Privileged EXEC)	enable.	Router#	disable
Глобальная конфигурация	configure terminal	Router(config)#	exit, end или Ctrl-Z

Настройка интерфейсов	Interface	Router(config-if)	exit
ROM monitor	В привилегированном режиме необходимо выполнить команду reload, а затем при перезагрузке устройства нажать клавишу Break		Continue

Подключившись к устройству, администратор получает командную строку, находящуюся в пользовательском режиме. В этом режиме доступны команды, позволяющие посмотреть некоторую (открытую) часть текущей конфигурации сетевого устройства, запустить процесс проверки работоспособности сети (команды ping и traceroute), открыть терминальную сессию для подключения к другому сетевому устройству и т.п.

В привилегированном режиме администратору доступно больше информации о всех конфигурации сетевого устройства, а также предоставляется доступ к команде перехода в режим конфигурирования (изменения конфигурационной информации).

Встроенная в CLI контекстная система документации

Внутри командной строки имеется встроенная контекстная документация (подсказка или помощь), выводимая командной help или ? (см., , рисунок 13). Если знает начальные символы команды, но не помнит её продолжение, или не уверен какие параметры следует указать команде, то он указывает в нужном месте командной строки знак ? и ему выводится информация о соответствующих командах или параметрах.

```
Router>? <Enter>
Exec commands:
  <1-99>          Session number to resume
  connect         Open a terminal connection
  disable         Turn off privileged commands
```

Рис.13.13 Пример вызова контекстной справки в командной строке Cisco IOS.

Настройка имени сетевого узла и приветственного сообщения

В качестве примеров настройки устройства приведем команды изменения имени устройства и определения сообщения, выдаваемого администратору при подключении (вход в пользовательский режим). Для этого необходимо подключиться к устройству, перейти в привилегированный режим, затем в режим глобальной конфигурации. Команда для изменения имени – *hostname10,* для определения приветственного сообщения – *banner* (см. рисунок 13.14).

Конфигурирование сетевых интерфейсов

Все сетевые устройства имеют одно или несколько подключений к телекоммуникационной сети – *сетевых интерфейса*. Каждый сетевой интерфейс (или кратко – интерфейс) имеет свои тип, определяющий способ подключения к нему (например, Ethernet, FastEthernet, Serial и т.п.) и уникальный номер. Номер интерфейса, обычно, имеет вид: номер контроллера/номер интерфейса внутри контроллера. Например, запись Ethernet 0/1 означает интерфейс с типом подключения Ethernet, расположенные на контроллере с номером 0 и имеющий на нем порядковый номер 1.

```
Router>enable
Router#configure terminal
Router(config)#hostname MainRouter
MainRouter(config)#banner motd /
Enter TEXT message. End with the character '/'.
############
```

```
# Hello world! #
############
/
MainRouter(config)#no hostname
Router (config)#
```

Рис. 13.14 Пример настройки имени сетевого устройства и определения приветственного сообщения.

Для конфигурирования сетевого интерфейса необходимо в режиме глобальной конфигурации ввести команду interface с указанием его типа и номера рисунок 13.15). Вернутся в режим глобальной конфигурации можно командой exit.

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#description Connect to main office
Switch(config-if)#no shutdown
Swtich(config-if)#exit
Switch(config)#
```

Рис 13.15 Пример настройки описания и состояния сетевого интерфейса.

Каждый интерфейс в зависимости от своего типа имеет ряд настроек. Для всех интерфейсов присутствует две настройки: описание и состояние (включен или нет). Первая настройка задается командой description, вторая – shutdown. На рисунке 15 приведен пример задания описания и включения интерфейса fastEthernet 0/1. Если администратору необходимо произвести одинаковую настройку для нескольких однотипных интерфейсов, то он может сделать это «в один прием», указав в команде interface диапазон конфигурируемых интерфейсов (параметр range). Диапазон задается следующим образом. Указывается тип интерфейсов, а в номере указывается диапазон. Например, запись range fastEthernet 0/1-4 означает, что будут задаваться параметры для интерфейсов 0/1, 0/2, 0/3 и 0/4 с типом fastEthernet рисунок 13.16.

```
Switch(config)#interface range fastEthernet 0/1-4
Switch(config-if-range)#description Connect to main office
Switch(config-if-range)#no shutdown
Swtich(config-if-range)#exit
Switch(config)#
```

Рис.13.16 Пример настройки описания и состояния группы сетевых интерфейсов.

Посмотреть текущие настройки сетевого интерфейса можно в привилегированном режиме с помощью команды show interface (см. рисунок 17). Чтобы посмотреть настройки сразу всех интерфейсов используется команда show interfaces.

Настройка режимов подключения к устройству для его администрирования

Подключившись к устройству администратор по умолчанию получает полный доступ не вводя никаких авторотационных данных. Очевидно, что такой режим в действующих сетях не всегда приемлем. Задать параметры авторизации можно в режиме глобальной конфигурации с помощью команды line. В качестве параметров команды указывается способ подключения (консоль или удалённый терминал) и номер линии для подключения. Пример настройки пароля для доступа к устройству приведен на рисунке 13.17.

```
Switch(config)#line console 0
Switch(config-line)#password qwerty
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#line vty 0 3
```

```
Switch(config-line)#password qwerty
Switch(config-line)#login
Switch(config-line)#transport input telnet
Switch(config-line)#exit
Switch(config)#
```

Рис.13.17 Пример настройки параметров подключений к устройству.

Сохранение и восстановление конфигурации оборудования

Конфигурацию оборудования можно стереть, сохранить в отдельный файл и затем восстановить её из него. Сделать это можно с помощью окна настроек оборудования (вкладка Config). Следует отметить, что конфигурация оборудования изменяется в режиме реального времени. Перезагрузка устройства приведет к тому, что изменения не будут сохранены. Чтобы изменения сохранились и остались неизменными при перезагрузке устройства, то их надо сохранить в энергонезависимой памяти. Для этого в привилегированном режиме следует выполнить команду copy running-config startup-config или выбрать соответствующие кнопки в окне свойств сетевого объекта.

Посмотреть содержимое текущей конфигурации или конфигурации, сохранённой на диске, можно в привилегированном режиме с помощью команды show рисунок 13.18.

```
Switch#show running-conf
Building configuration...

Current configuration : 1235 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
…
Switch#copy running-config startup-config
Switch#
```

Рис.13.18 Пример работы с конфигурацией оборудования.

Задание

1. Запустите среду моделирования Cisco packet tracer. Ознакомьтесь с ещё интерфейсом.

2. Сконфигурируйте в среде моделирования сеть, представленную на рисунке 19. Обратите внимание на используемые типы кабелей и модели оборудования (номера сетевых интерфейсов, которыми Вы соедините оборудование значение не имеют).

3. Добавьте в созданную сеть новый ноутбук и сервер. Сконфигурируйте их так, чтобы они подключались к беспроводной сети. Сервер должен иметь также подключение к проводной сети (в том же коммутаторе, что и точки беспроводного доступа).

4. Используя командную строку задайте сетевым узлам:

a. Уникальные сетевые имена;

b. Приветственные приглашения, в которых будет указываться краткая информация о сетевом устройстве;

c. Пароли для прямого подключения к устройствам и режим их проверки;

d. Для устройств, соединяющих главный и дополнительный офисы задайте описания для соответствующих сетевых интерфейсов.

e. Переведите сетевые интерфейсы в состояния, соответствующие рисунку 13.19.

5. Сохраните настройки сетевых устройств в их энергонезависимой память. Для маршрутизаторов, соединяющих основной и дополнительный офисы сохраните конфигурацию в отдельные файлы.

6. Создайте сценарий проверки работоспособности сети, в котором необходимо проверить передачу следующих данных:

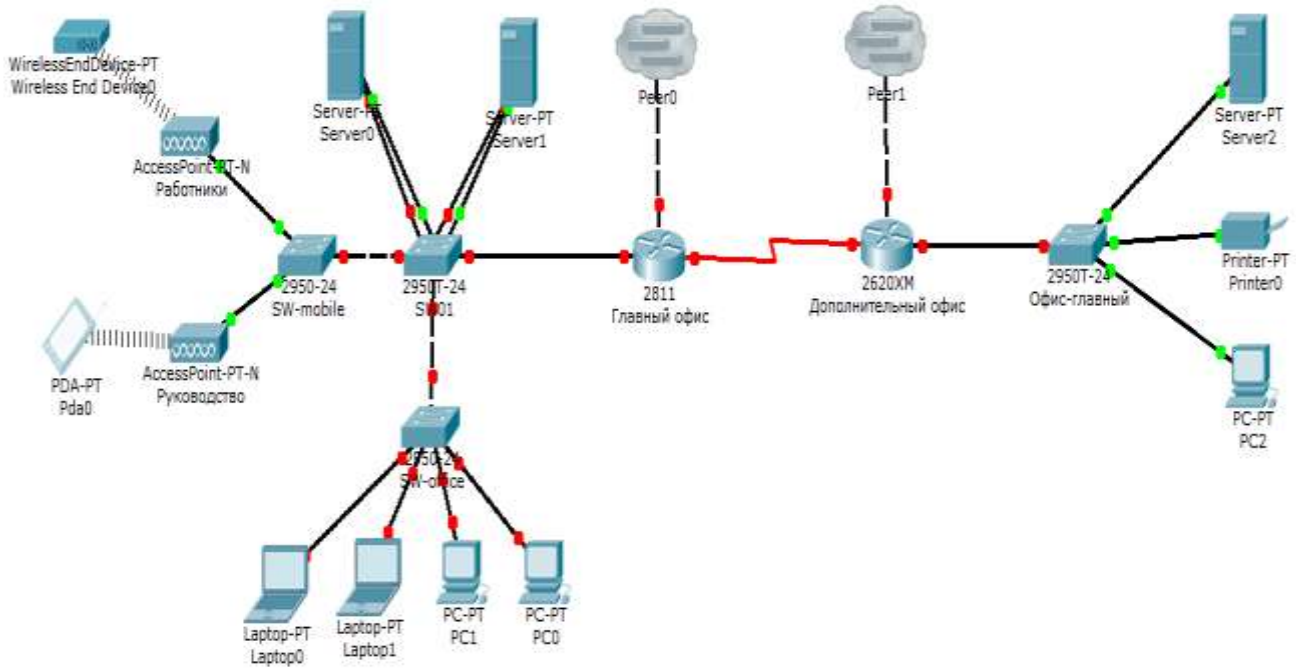
a. ping от компьютера PC1 в главном офисе до компьютера PC2 в дополнительном офисе;

b. ping от компьютера PC0 в главном офисе до сервера Server0 в главном корпусе;

c. ping от компьютера PC2 в главном офисе до сервера Server2 в дополнительном офисе;

d. http запрос от LaptopPT к Server2;

e. DNS запрос от PDA-PT к Server1.



Контрольные вопросы:

1. Зачем используются среды имитационного моделирования компьютерных сетей?
2. Чем отличается режим рабочей области «Логический» от «Физический»?
3. Какие элементы имеются в основном окне среды CISCO Packet Tracer?
4. Для чего используется многопользовательский режим работы среды моделирования Cisco Packet tracer?
5. Чем отличается маршрутизатор от коммутатора и концентратора?
6. Каким образом можно производить конфигурирования сетевых устройств?
7. Что такое “CLI”, как и зачем он используется?
8. Каким образом в командной строке можно настроить режимы работы сетевых интерфейсов?
9. Чем отличается текущая конфигурация, от загрузочной конфигурации оборудования?

Практическая работа № 30

СЕТЕВЫЕ УТИЛИТЫ

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

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия.

Общие сведения:

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

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

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

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

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

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

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

Аппаратура локальной сети обычно состоит из кабеля, разъемов, Т-коннекторов (рис. 14.1), терминаторов и сетевых адаптеров. Кабель, очевидно, используется для передачи данных между рабочими станциями. Для подключения кабеля используются разъемы. Эти разъемы через Т-коннекторы подключаются к сетевым адаптерам - специальным платам, вставленным в слоты расширения материнской платы рабочей станции. Терминаторы подключаются к открытым концам сети.

Рис. 14.1. Т-коннектор

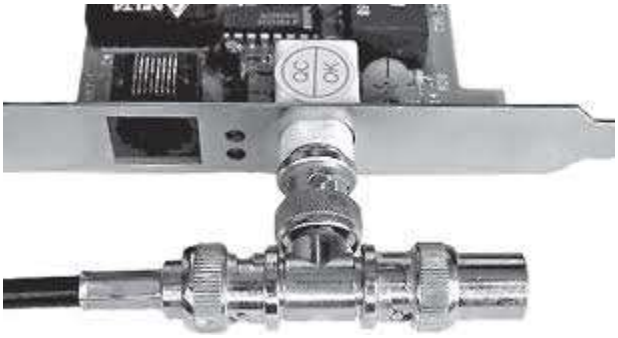


Рис. 14.2. Т-коннектор, присоединенный к сетевой карте

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

Сети можно создавать с любым из типов кабеля.

1. Витая пара (TP - Twisted Pair)– это кабель, выполненный в виде скрученной пары проводов (рис. 14.3). Он может быть экранированным и неэкранированным. Экранированный кабель более устойчив к электромагнитным помехам. Витая пара наилучшим образом подходит для малых учреждений. Недостатками данного кабеля является высокий коэффициент затухания сигнала и высокая чувствительность к электромагнитным помехам, поэтому максимальное расстояние между активными устройствами в ЛВС при использовании витой пары должно быть не более 100 метров.

Рис. 14.3 Кабель на основе витой пары

2. Коаксиальный кабель (рис. 14.4) состоит из одного цельного или витого центрального проводника, который окружен слоем диэлектрика. Проводящий слой алюминиевой фольги, металлической оплетки или их комбинации окружает диэлектрик и служит одновременно как экран против наводок. Общий изолирующий слой образует внешнюю оболочку кабеля.

Рис. 14.4. Устройство коаксиального кабеля

1 — внутренний проводник (медная проволока),

2 — изоляция (сплошной полиэтилен),

3 — внешний проводник (оплётка из меди),

4 — оболочка (светостабилизированный полиэтилен).

Коаксиальный кабель может использоваться в двух различных системах передачи данных: без модуляции сигнала и с модуляцией. В первом случае цифровой сигнал используется в таком виде, в каком он поступает из ПК и сразу же передается по кабелю на приемную станцию. Он имеет один канал передачи со скоростью до 10 Мбит/сек и максимальный радиус действия 4000 м. Во втором случае цифровой сигнал превращают в аналоговый и направляют его на приемную станцию, где он снова превращается в цифровой. Операция превращения сигнала выполняется модемом; каждая станция должна иметь свой модем. Этот способ передачи является многоканальным (обеспечивает передачу по десяткам каналов, используя для этого всего

лишь один кабель). Таким способом можно передавать звуки, видео сигналы и другие данные. Длина кабеля может достигать до 50 км.

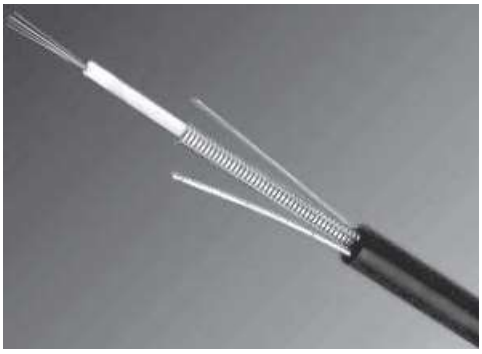


Рис. 14.5. Оптоволоконный кабель

Оптоволоконный кабель (рис. 14.5) является более новой технологией, используемой в сетях. Носителем информации является световой луч, который модулируется сетью и принимает форму сигнала. Такая система устойчива к внешним электрическим помехам и таким образом возможна очень быстрая, секретная и безошибочная передача данных со скоростью до 2 Гбит/с. Количество каналов в таких кабелях огромно. Передача данных выполняется только в симплексном режиме, поэтому для организации обмена данными устройства необходимо соединять двумя оптическими волокнами (на практике оптоволоконный кабель всегда имеет четное, парное кол-во волокон). К недостаткам оптоволоконного кабеля можно отнести большую стоимость, а также сложность подсоединения.

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

Выделяют следующие виды сетевого оборудования.

1. Сетевые карты – это контроллеры, подключаемые в слоты расширения материнской платы компьютера, предназначенные для передачи сигналов в сеть и приема сигналов из сети (рис. 14.6).

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

3. Концентраторы (Hub) – это центральные устройства кабельной системы или сети физической топологии "звезда", которые при получении пакета на один из своих портов пересылает его на все остальные (рис. 14.7). В результате получается сеть с логической структурой общей шины. Различают концентраторы активные и пассивные. Активные концентраторы усиливают полученные сигналы и передают их. Пассивные концентраторы пропускают через себя сигнал, не усиливая и не восстанавливая его.

Рис. 14.6. Сетевая карта в виде платы расши-

Рис. 14.7. Концентратор с фиксированным количеством портов

рения, устанавливаемой в PCI-слот

4. Повторители (Repeater)- устройства сети, усиливает и заново формирует форму входящего аналогового сигнала сети на расстояние другого сегмента (рис. 14.8). Повторитель действует на электрическом уровне для соединения двух сегментов. Повторители ничего распознают сетевые адреса и поэтому не могут использоваться для уменьшения трафика.

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

Рис. 14.8. Повторители (Repeater)

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

5. Коммутаторы (Switch) - управляемые программным обеспечением центральные устройства кабельной системы, сокращающие сетевой трафик за счет того, что пришедший пакет анализируется для выяснения адреса его получателя и соответственно передается только ему (рис.14.9).

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

Рис. 14.9. Коммутатор

6. Маршрутизаторы (Router) - стандартные устройства сети, работающие на сетевом уровне и позволяющее переадресовывать и маршрутизировать пакеты из одной сети в другую, а также фильтровать широковещательные сообщения (рис. 14.10).

7. Мосты (Bridge)- устройства сети, которое соединяют два отдельных сегмента, ограниченных своей физической длиной, и передают трафик между ними (рис.14.11). Мосты также усиливают и конвертируют сигналы для кабеля другого типа. Это позволяет расширить максимальный размер сети, одновременно не нарушая ограничений на максимальную длину кабеля, количество подключенных устройств или количество повторителей на сетевой сегмент.

Рис. 14.10. Беспроводной маршрутизатор

Рис. 14.11. Мосты (Bridge)-

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

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

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

Беспроводные локальные сети считаются перспективным направлением развития ЛС. Их преимущество - простота и мобильность. Также исчезают проблемы, связанные с прокладкой и

монтажом кабельных соединений - достаточно установить интерфейсные платы на рабочие станции, и сеть готова к работе.

Сердцем любой беспроводной сети является точка доступа (рис. 14.12), через которую конечные устройства по радио связываются с корпоративной сетью. Она определяет не только радиус действия и скорость передачи данных, но и решает элементарные задачи управления и обеспечения безопасности.

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

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

Рис. 14.12. Точка доступа

Программное обеспечение локальных сетей.

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

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

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

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

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

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

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

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

Контрольные вопросы:

1. Что такое топология сети?
2. Что представляет собой проводник витая пара?
3. Каково устройство коаксиального кабеля?
4. Почему оптоволоконный кабель является приоритетным для проводных сетей? В чем его недостатки?
5. Что такое шлюзы? Какими могут быть шлюзы?
6. Зачем нужны повторители?
7. В чем состоят преимущества использования коммутаторов?
8. Для чего служит межсетевой экран (брандмауэр)?
9. Что такое концентратор?
10. Что такое маршрутизатор?
11. В чем заключаются преимущества и недостатки сетей с выделенным сервером?
12. Для чего предназначена программа NetLink?
13. Чем отличается выделенные файл-серверы от невыделенных?

Практическая работа № 31-32

РАЗГРАНИЧЕНИЕ ДОСТУПА

Цель работы: осуществлять настройку программного обеспечения компьютерной сети.

Оборудование и программное обеспечение (материалы, дидактическое обеспечение): методические рекомендации к выполнению работы, задание и инструкционная карта для проведения практического занятия.

Общие сведения:

Основными устройствами для быстрой передачи информации на большие расстояния в настоящее время являются телеграф, радио, телефон, телевизионный передатчик, телекоммуникационные сети на базе вычислительных систем.

Передача информации между компьютерами существует с самого момента возникновения ЭВМ. Она позволяет организовать совместную работу отдельных компьютеров, решать одну задачу с помощью нескольких компьютеров, совместно использовать ресурсы и решать множество других проблем.

Под ***компьютерной сетью*** понимают комплекс аппаратных и программных средств, предназначенных для обмена информацией и доступа пользователей к единым ресурсам сети.

Основное назначение компьютерных сетей - обеспечить совместный доступ пользователей к информации (базам данных, документам и т.д.) и ресурсам (жесткие диски, принтеры, накопители CD-ROM, модемы, выход в глобальную сеть и т.д.).

Абоненты сети– объекты, генерирующие или потребляющие информацию.

Абонентами сети могут быть отдельные ЭВМ, промышленные роботы, станки с ЧПУ (станки с числовым программным управлением) и т.д. Любой абонент сети подключён к станции.

Станция– аппаратура, которая выполняет функции, связанные с передачей и приёмом информации.

Для организации взаимодействия абонентов и станции необходима физическая передающая среда.

Физическая передающая среда– линии связи или пространство, в котором распространяются электрические сигналы, и аппаратура передачи данных.

Одной из основных характеристик линий или каналов связи является скорость передачи данных (пропускная способность).

Скорость передачи данных– количество бит информации, передаваемой за единицу времени.

Обычно скорость передачи данных измеряется в битах в секунду (бит/с) и кратных единицах Кбит/с и Мбит/с.

Соотношения между единицами измерения: 1 Кбит/с =1024 бит/с; 1 Мбит/с =1024 Кбит/с; 1 Гбит/с =1024 Мбит/с.

На базе физической передающей среды строится коммуникационная сеть. Таким образом, компьютерная сеть – это совокупность абонентских систем и коммуникационной сети.

Задания:

Задание №1. Зайдите в Internet и изучите материал «Сетевые операционные системы для локальных сетей» - http://yuschikev.narod.ru/comp_set/Loc_seti.htm

Задание №2. Ответить на вопросы:

1. Отличительные черты LAN Server:	
2. Отличительные черты Windows NT	
3. Перечислите этапы настройки сетевых средств Windows	
4. С помощью какой вкладки устанавливается способ управления доступом к общим ресурсам	
5. *Решите задачу.* Максимальная скорость передачи данных в локальной сети 100 Мбит/с. Сколько страниц текста можно передать за 1 сек, если 1 страница текста содержит 50 строк и на каждой строке - 70 символов	

Задание №3. Сделать вывод о проделанной работе

Контрольные вопросы:

1. Что называют Сетевыми Операционными Системами?
2. Основное направление развития современных Сетевых Операционных Систем

СПИСОК РЕКОМЕНДУЕМЫХ ИСТОЧНИКОВ

Основная литература:

1. Баринов В. В., Баринов И. В., Пролетерский А. В. , Пылькин А. Н. Компьютерные сети: учебник для студ. учреждений СПО/ И. В..- 1-е изд.-М.: Академия,2018.-192 с. - Текст : электронный https://www.academia-moscow.ru/
2. Замятина, О. М. Инфокоммуникационные системы и сети. Основы моделирования: учебное пособие для среднего профессионального образования. — Москва : Издательство Юрайт, 2019. — 159 с. — (Профессиональное образование). — ISBN 978-5-534-10682-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/
3. Максимов Н. В., Попов И.И. Компьютерные сети: учебное пособие для студ. учреждений СПО - 6-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2019. - 464 с.: ил.- (Профессиональное образование). - Текст : электронный. - URL: https://new.znanium.com//
4. Назаров А. В., Енгалычев А.Н., Мельников В.П. Эксплуатация объектов сетевой инфраструктуры : учебник - Москва : КУРС; ИНФРА-М, 2019. — 360 с. — (Среднее профессиональное образование). - ISBN 978-5-16-105198-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1027558