ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Петербургский государственный университет путей сообщения Императора Александра I»
(ФГБОУ ВО ПГУПС)

Петрозаводский филиал ПГУПС

ОДОБРЕНО
на заседании цикловой комиссии
протокол № 11 от 23.06.2017
Председатель цикловой комиссии:
_____ (Камаков)

УТВЕРЖДАЮ
Начальник УМО
_____ А.В. Калько
«23» 06 2017г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по организации и проведению практических занятий

По учебной практике: УП.02.02. Межсетевое взаимодействие крупных сетей

Специальность: 09.02.02 Компьютерные сети

Выполнил: преподаватель ПФ ПГУПС Усков А.А.

2017г.

ВВЕДЕНИЕ

Методическое пособие по проведению учебной практики, входящей в состав ПМ.02. Организация сетевого администрирования составлено в соответствии с требованиями Федерального государственного образовательного стандарта по специальности среднего профессионального образования (далее СПО) 09.02.02 Компьютерные сети

Настоящее методическое пособие рассчитано на самостоятельную работу обучающихся в учебном кабинете под руководством преподавателя, а также является руководством для преподавателей при подготовке к проведению учебной практики.

Для успешного прохождения учебной практики могут быть использованы теоретические знания, полученные обучающимися при изучении ПМ.02.Организация сетевого администрирования

УП.02.02. Межсетевой взаимодействие крупных сетей направлена на:

- приобретение студентами профессиональных навыков и первоначального опыта в профессиональной деятельности;

- формирование основных профессиональных компетенций, соответствующих виду профессиональной деятельности (ВПД) Организация деятельности коллектива исполнителей

- воспитание сознательной трудовой и производственной дисциплины;

- усвоение студентами основ законодательства об охране труда, системы стандартов безопасности труда, требований правил гигиены труда и производственной санитарии, противопожарной защиты, охраны окружающей среды в соответствии с новыми нормативными и законодательными актами.

Результатом освоения учебной практики является овладение обучающимися видом профессиональной деятельности (ВПД): Организация деятельностиколлектива исполнителей, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

	Наименование результата обучения
ПК 2.1.	Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.
ПК 2.2.	Администрировать сетевые ресурсы в информационных системах.
ПК 2.3.	Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.
ПК 2.4.	Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

Каждый студент обязан оформлять отчет о проделанной работе. Отчет должен содержать:

- титульный лист;

- цель работы;

- задание;

- выполненное практическое занятие в соответствии с заданием;

- вывод;

Правила охраны труда при проведении учебной практики.

1. Общие требования охраны труда.

1.1. К работе в учебном кабинете допускаются студенты, прошедшие инструктаж по охране труда, знающие правила пожарной безопасности.

1.2. При работе в кабинете должны соблюдаться правила поведения, расписание учебных занятий, установленный режим труда и отдыха.

1.3. При проведении занятий возможно воздействие на студентов следующих опасных факторов:

- нарушение осанки, искривление позвоночника, развитие близорукости при неправильном подборе мебели;

- нарушение остроты зрения при недостаточной освещенности в кабинете;

- поражение электрическим током при неисправном оборудовании кабинета;

1.4. В процессе занятий студенты должны соблюдать правила личной гигиены, содержать в чистоте рабочее место.

2. Требования безопасности перед началом занятия.

2.1. Включить полностью освещение в кабинете, убедиться в правильности работы светильников. Наименьшая освещенность в кабинете должна быть не менее 300Лк (20ВТ/м^2) при люминесцентных лампах.

2.2. Убедиться в исправности электрооборудования кабинета: коммуникационные коробки выключателей и розеток не должны иметь трещин, сколов, а также оголенных контактов.

2.3. Проверить санитарное состояние кабинета, убедиться в целостности стекол в окнах и провести сквозное проветривание кабинета.

3.Требование безопасности во время занятия.

3.1. Используемые в кабинете демонстрационные электрические приборы должны быть исправны и иметь заземление и зануление.

4. Требования безопасности в аварийных ситуациях.

4.1. При возникновении аварийных ситуаций немедленно эвакуировать студентов и сообщить администрации учреждения.

5. Требования безопасности по окончании занятия.

5.1. Выключить демонстрационные электрические приборы;

5.2. Закрыть окна и выключить свет

Перечень практических занятий по УП.02.02 Межсетевое взаимодействие

Практическое занятие №1

Определение требований заказчика к сети. Сбор данных для анализа использования программно-технических средств компьютерных сетей.

Цель: Определить требования заказчика к сети.

Требования к проектированию аппаратных (серверных комнат) Кроссовых комнат

Аппаратная – помещение, занимаемое телекоммуникационным и/или серверным оборудованием, обслуживающим пользователей в здании. Часто аппаратные являются помещениями специального назначения. Аппаратные соединяются с магистралями и обычно считаются средствами обслуживания здания.

Размещение в здании

- Помещение аппаратной не должно быть проходным. Желательно, чтобы оно не имело окон и не примыкало вплотную к внешним стенам здания. Если же в техническом помещении предусмотрены окна, то рекомендуется располагать аппаратную на северной или северо-восточной стороне здания. Крайне нежелательно размещать аппаратную рядом с теми внутренними конструкциями здания, которые ограничивают ее возможное расширение в будущем: лифтовые шахты, лестничные марши, вентиляционные камеры и т.д.
- Запрещается располагать аппаратную рядом с помещениями для хранения пожароопасных или агрессивных химических материалов.
- Не рекомендуется выделять помещение для аппаратной на верхних этажах здания, т.к. они наиболее подвержены повреждениям в случае пожара и могут заливаться при протечках крыши.
- Не допускается размещение аппаратной под помещениями, связанными с потреблением воды (туалеты, душевые, столовые, буфеты и т.д.). При размещении аппаратной в подвале, необходимы дополнительная гидроизоляция и тщательный выбор трасс прокладки трубопроводов. Через аппаратную не должны прокладываться транзитом трубопроводы инженерных систем здания.
- Предпочтительно размещать аппаратную недалеко от грузовых или грузопассажирских лифтов, используемых для транспортировки тяжелого оборудования, например ИБП. В тоже время, следует избегать близкого размещения мощных источников электрических и магнитных полей, а также оборудования, которое может вызвать повышенную вибрацию.
- Многие источники рекомендуют располагать аппаратную в геометрическом центре здания хотя бы потому, что это позволяет существенно сэкономить на

прокладке кабеля.

Помещение аппаратной

- Минимальный допустимый размер аппаратной - 14 квадратных метров.
- Минимальная высота потолка аппаратной должна составлять 2,44 м.
- Пол в аппаратной должен быть ровным и иметь антистатическое покрытие

Размещение кроссовых

- В соответствии с классификацией, кроссовые подразделяются на кроссовые внешних магистралей (КВМ), здания (КЗ) и этажа (КЭ).
- КЭ представляет собой служебное помещение, в которое вводятся кабели подсистемы внутренних магистралей СКС и кабели горизонтальной подсистемы. В этом помещении монтируются коммутационные панели, сетевые приборы и другие вспомогательные устройства. В кроссовых нельзя размещать оборудование, которое не имеет непосредственного отношения к тем функциям, для выполнения которых организуется данное техническое помещение, например силовые распределительные щиты электропитания этажа.
- В небольших СКС с количеством портов до 150-200 согласно накопленной статистике кроссовая зачастую является единственным техническим помещением и естественным образом совмещается с аппаратной.

Задание:

1. Ознакомится с требованиями заказчика:
    a. Скорость передачи данных не ниже 5000 Мбит/с;
    b. В каждом рабочем помещении по 2 ПК + 1 резервная розетка;
    c. На каждом этаже по 2 сетевых принтера;
    d. Серверная на 2 этаже здания;
    e. Кроссовые этажей на 1 и 3 этажах с возможностью расширения;
    f. Требования к оборудованию:
        - ПК: корпус miniTower с блоком питания не менее 350 Вт, HDD не менее 320 Гб, ОП не менее 4 Гб, DVD-привод, процессор не менее Intel Core i3, ОС + офисное ПО;
        - Монитор не менее 18” + клавиатура + мышь + сетевой фильтр;
        - Коммутаторы не менее 24 портов + патч-панели не менее 24 портов;
        - Сервер выполняет функции файл-сервера и принт-сервера
        - Стойка серверная 8 U
        - ИБП (серверный) минимум 1 час работы сервера и коммутаторов
    g. Файл сервер доступен всем но с разными правами: 3 группы допуска (администраторы, руководство, сотрудники)

    h. Доступ в Интернет всех пользователей
    i. Минимальные затраты при вышеуказанных требованиях
    j. Доступ к сетевым принтерам с любого ПК
2. Ознакомится с планировкой здания.
3. Проанализировать требования заказчика.
4. Выбрать места расположения серверной и кроссовых.

Практическое занятие №2

Определение оборудования, удовлетворяющего требованиям заказчика. Расчёт стоимости сетевого оборудования и программного обеспечения.

Цель: Поиск и расчет стоимости оборудования, удовлетворяющего требованиями заказчика.

Теория:

Выбор основных комплектующих

Самостоятельно выбирая компьютерные комплектующие, вы не только сможете подобрать компоненты, максимально удовлетворяющие вашим запросам, но и значительно снизить итоговую стоимость компьютера в целом.

Первым делом нам потребуется начинка для системного блока. Начнем с **процессора**. Сначала четко определитесь: для каких целей будет использоваться стационарный ПК. Помните: чем мощнее процессор, тем выше скорость работы компьютерного устройства.

Обращайте внимание на два показателя: тактовую частоту (не менее 2 ГГц) и оперативную память (не менее 2 ГБ). Лучше, если эти показатели буду даже выше.

Материнская плата — основа «машины». На сегодняшний день наиболее маститыми производителями этого компьютерного элемента являются: Asus, Gigabyte, Foxconn, Msi и др. Для мощного компьютера потребуется материнская плата формата ATX, поскольку она имеет большее количество разъемов и слотов, позволяющих ее усовершенствовать. Кроме того, такую материнку намного проще устанавливать в системник. Совет. Обязательно проверьте перед покупкой материнки ее совместимость с выбранным процессором (тип разъема материнки и процессора должны совпадать), иначе могут возникнуть проблемы при установке.

Ну и наконец — **оперативная паямять**. На данный момент наибольшей популярностью пользуется оперативная память типа DDR3. Именно на таком варианте мы и остановимся. Но выбрать тип оперативки — это еще не все. Обращайте внимание также на объем оперативки — выбирать следует модели, имеющие минимум 4 Гб рабочего объема, а еще лучше — 8 Гб.

Минимальная мощность выбранного **блока питания** должна составлять от 350 ватт. И самое главное, суммарная выходная мощность блока питания. Имейте в виду, что она должна быть на 40-50% больше мощности, потребляемой всеми остальными компонентами системного блока. Важно понимать, что главная задача жесткого диска — долгосрочное хранение информации. Исходя из этого и следует выбирать его емкость. В последнее время цены на винчестеры значительно снизились и вполне

реально приобрести диск объемом 1 Тб.

Выбор рабочего монитора в большей степени должен определяться преследуемыми в ходе эксплуатации компьютера целями. Если вы планируете большую часть времени работать за ним, то не стоит выбирать слишком большую диагональ. Если же вы — игроман или хотите устраивать по вечерам свой собственный кинотеатр, диагональ уже нужна побольше, как и разрешающая способность (от нее зависит четкость экранной картинки). Соответственно, и стоимость такого монитора будет большей.

При выборе клавиатуры уже можно разгуляться. Опять-таки, если компьютер будет использоваться преимущественно для работы, то следует отдать предпочтение «клаве» с пирамидальной раскладкой.

Выбор мыши, пожалуй, наиболее легкий этап подбора компьютерных комплектующих. Достаточно, чтобы она была максимально удобной для вашей руки и устраивала вас своими внешними характеристиками.

Задание:

1. Подготовить таблицу в MS Office Exel, в которой будет перечень оборудования, информация об оборудовании, критерии по которым оборудование выбиралось, цена оборудования.
2. Поиск требуемого оборудования и ПО, заполнить таблицу.
3. Рассчитать полную стоимость.

Практическое занятие №3

Создание схемы сети (инвентарная ведомость, логическая топология).

Цель: Выполнить схему здания, схемы сети.

Теория:

Сетевые диаграммы (далее L3-схемы) являются чрезвычайно важными при решении проблем, либо планировании изменений в сети предприятия. Логические схемы во многих случаях оказываются более ценными, чем схемы физических соединений. Иногда мне встречаются «логически-физически-гибридные» схемы, которые практически бесполезны. Если вы не знаете логическую топологию вашей сети, *вы слепы*.

Какая информация должна быть представлена на L3-схемах?

Для того, чтобы создать схему сети, вы должны иметь точное представление о том, *какая* информация должна присутствовать и *на каких именно* схемах. В противном случае вы станете смешивать информацию и в итоге получится очередная бесполезная «гибридная» схема. Хорошие L3-схемы содержат следующую информацию:

- подсети
  - VLAN ID (все)
  - названия VLAN'ов
  - сетевые адреса и маски (префиксы)
- L3-устройства
  - маршрутизаторы, межсетевые экраны (далее МСЭ) и VPN-шлюзы (как минимум)
  - наиболее значимые серверы (например, DNS и пр.)
  - ip-адреса этих серверов
  - логические интерфейсы
- информацию протоколов маршрутизации

Какая информация не должна присутствовать на L3-схемах:

Перечисленной ниже информации не должно быть на сетевых схемах, т.к. она относится к другим уровням [модели OSI, *прим. пер.*] и, соответственно, должна быть отражена *на других схемах*:

- вся информация L2 и L1 (в общем случае)
- L2-коммутаторы (может быть представлен только интерфейс управления)
- физические соединения между устройствами

Какая информация необходима для создания L3-схемы?

Для того, чтобы создать логическую схему сети, понадобится следующая информация:

- **Схема L2 (или L1)** — представление физических соединений между устройствами L3 и коммутаторами
- **Конфигурации устройств L3** — текстовые файлы либо доступ к GUI, и т.д.
- **Конфигурации устройств L2** — текстовые файлы либо доступ к GUI, и т.д.

Задание:

1. Выполнить схему здания в MS Visio с обозначениями розеток на рабочих местах.
2. Выполнить схему прокладки кабеля (указать расположение кроссовых шкафов).
3. Выполнить в MS Visio схему серверной стойки и коммутационных шкафов на этажах.
4. Выполнить логическую схему сети.

Практическое занятие № 4

Разработка схемы разбиения на IP-подсети с обеспечением возможности для расширения

Цель: Разработать схему разбиения на IP-подсети.

Теория:

Причины разбиения на подсети.

Ранее при развёртывании сети организации часто подключали все компьютеры и другие сетевые устройства к одной IP-сети. Всем устройствам в организации назначались IP-адреса с одинаковой сетевой частью. Конфигурация такого типа называется плоской архитектурой сети. В небольшой сети с небольшим количеством устройств плоская архитектура не представляет проблемы. Однако по мере расширения сети с такой конфигурацией могут возникнуть серьёзные трудности.

Подумайте о том, как в сети Ethernet устройства выполняют поиск необходимых служб и устройств с помощью широковещательной рассылки. Как вы помните, широковещательное сообщение доставляется всем узлам данной сети. Протокол DHCP — пример сетевой службы, которая зависит от широковещательной рассылки. Устройства отправляют по сети широковещательные запросы, чтобы определить местонахождение DHCP-сервера. В крупной сети из-за этого может создаваться значительный трафик, который замедлит общую работу сети. Кроме того, поскольку широковещательная рассылка выполняется по всем устройствам,

им необходимо принять и обработать трафик, что приводит к повышению требований к обработке. Если устройство должно обработать значительный объём широковещательных рассылок, это может даже привести к замедлению работы устройства. По этой причине более крупные сети необходимо разделить на более мелкие подсети, предназначенные для небольших групп устройств и служб.

Процесс сегментации сети путём разделения её на несколько более мелких сетей называется разбиением на подсети. Эти более мелкие сети называются подсетями. Сетевые администраторы могут группировать устройства и службы в подсети по их географическому местоположению (например, 3-й этаж здания), организационному подразделению (например, отдел продаж) или по типу устройств (принтеры, серверы, глобальная сеть и т.п.) или по другому значимому для сети принципу. Разбиение на подсети может снизить общую нагрузку на сеть и повысить её производительность.

При планировании необходимо определить параметры каждой подсети: размер, количество узлов в каждой подсети, а также способы назначения адресов узлов.

Как показано на рисунке, при планировании подсетей требуется учитывать требования организации к использованию сети и предполагаемую структуру подсетей. Для начала необходимо изучить требования к сети. Это означает, что нужно изучить всю сеть, определить её основные части и разделить их на сегменты. План распределения адресов содержит информацию о требуемом размере подсети, количестве узлов и принципе назначения адресов узлам. Кроме того, необходимо определить узлы, которым нужно выделить статические IP-адреса, и узлы, которые смогут получать сетевые настройки по протоколу DHCP.

Определяя размер подсети, необходимо оценить количество узлов, которым потребуются IP-адреса в каждой подсети в рамках разделённой частной сети. Например, при проектировании сети студенческого городка нужно оценить количество узлов в локальной сети администраторов, в локальной сети

преподавателей и в локальной сети учащихся. В домашней сети можно оценить количество узлов в локальной сети жилой зоны и в локальной сети домашнего офиса.

Как уже упоминалось ранее, диапазон частных IP-адресов, используемых в локальной сети, выбирается сетевым администратором, и к выбору этого диапазона следует отнестись с должным вниманием. Необходимо убедиться, что количества адресов будет достаточно для активных в данный момент узлов и для будущего расширения сети. Запомните диапазоны частных IP-адресов:

- 10.0.0.0 с маской подсети 255.0.0.0
- 172.16.0.0 с маской подсети 255.240.0.0
- 192.168.0.0 с маской подсети 255.255.0.0

На основании требований к IP-адресам можно определить диапазон или диапазоны узлов для развёртывания. После разбиения выбранного пространства частных IP-адресов на подсети будут получены адреса узлов, соответствующие требованиям к сети.

Определите стандарты присвоения IP-адресов в диапазоне каждой подсети. Например:

- Принтерам и серверам будут назначены статические IP-адреса
- Пользователи будут получать IP-адреса от DHCP-серверов в подсетях /24
- Маршрутизаторам назначаются первые доступные адреса узла в диапазоне.

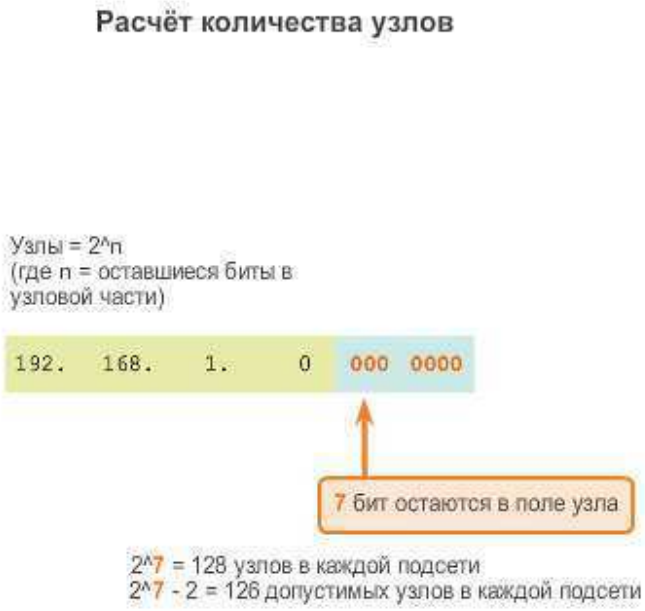
Два существенных фактора, влияющих на определение необходимого блока частных адресов, — это количество необходимых подсетей и максимальное количество узлов в каждой подсети. Каждый из этих блоков адресов позволит распределить узлы исходя из размера сети, количества узлов, активных в настоящий момент, или добавляемых в ближайшем будущем. Требования к IP-пространству определят диапазон или диапазоны используемых узлов.

Расчёт подсетей

Для расчёта количества подсетей используйте следующую формулу:

2^n (где n = количество заимствованных бит)

Как показано на рисунке 1 для примера 192.168.1.0/25, расчёт выглядит следующим образом:
2^1 = 2 подсети



Расчёт узлов

Для расчёта количества узлов в одной сети используйте следующую формулу:
2^n (где n = количество бит, оставшихся в узловой части адреса)
Как показано на рисунке 2 для примера 192.168.1.0/25, расчёт выглядит следующим образом:
2^7 = 128
Поскольку для узлов не может использоваться сетевой адрес или широковещательный адрес из подсети, эти два адреса нельзя назначить узлам. Это означает, что в каждой из подсетей можно использовать 126 (128-2) адресов узлов.

Таким образом, в этом примере заимствование одного бита узла для сети приведёт к созданию двух подсетей, в каждой из которых можно назначить 126 узлов.

Задание:

1. Рассчитать адресное пространство для 3 подсетей (1 подсеть на этаж);
2. Разработать схему разбиения на подсети.

Практическое занятие № 5
Внедрение схемы IP-адресации.

Цель: Собрать схему и настроить IP-адресацию сети в Cisco Packet Tracer.

Теория:

Cisco Packet Tracer

Cisco Packet Tracer – это эмулятор сети, созданный компанией Cisco. Программа позволяет строить и анализировать сети на разнообразном оборудовании в произвольных топологиях с поддержкой разных протоколов. В ней вы получаете возможность изучать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров и т.д. Данное приложение является наиболее простым и эффективным среди своих конкурентов. Так, например, создание нового проекта сети в Cisco Packet Tracer занимает существенно меньше времени, чем в аналогичной программе - GNS3, Packet Tracer проще в установке и настройке.

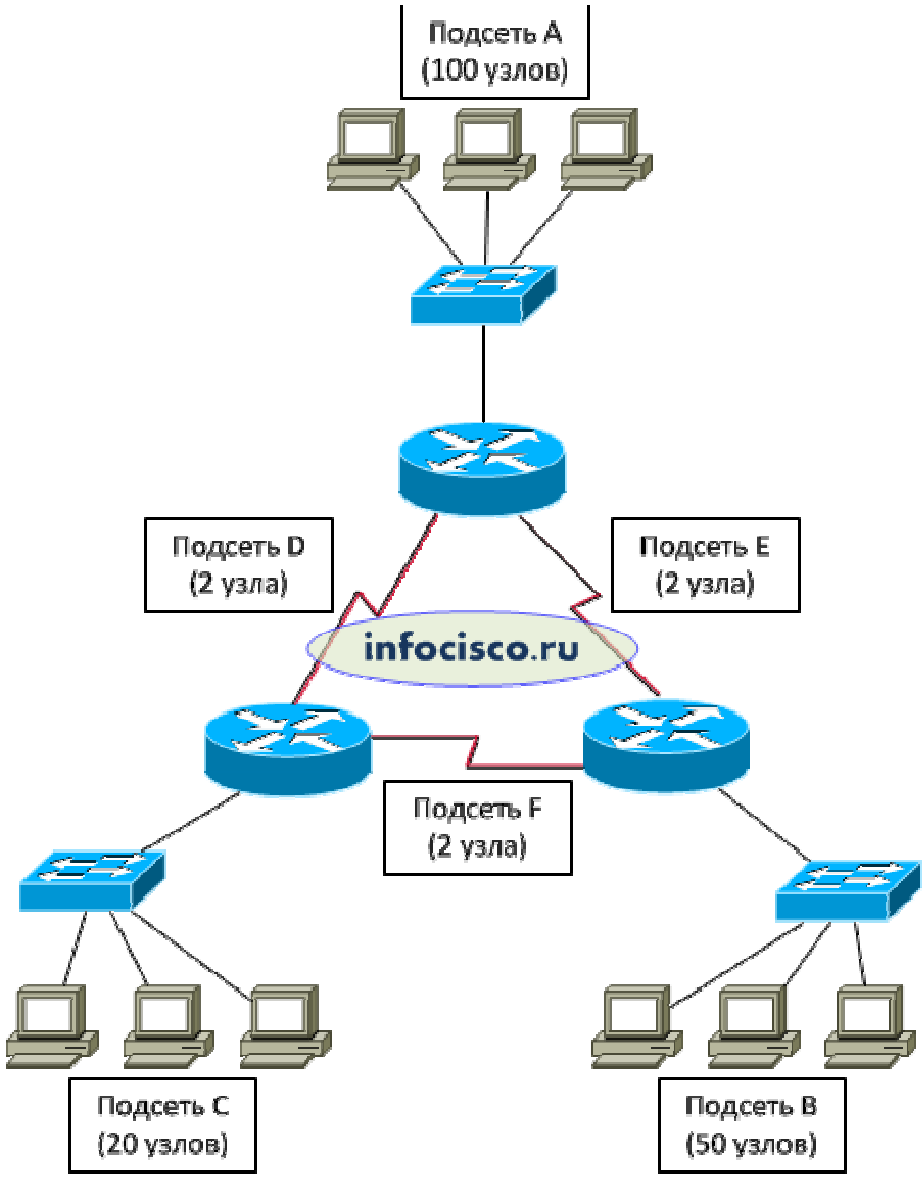
Задание:

1. По составленной ранее схеме сети собрать ее в Cisco Packet Tracer.
2. Выполнить настройку оборудования согласно схеме IP-адресации.

Практическое занятие № 6
Разбиение сети на подсети

Цель: Разбить сети на подсети в Cisco PT посредством VLAN.

Пример деления сети на подсети.
Процесс деления сети на подсети проще объяснить на конкретном примере.
Представим, что у нас есть сеть из трех маршрутизаторов, трех коммутаторов и нескольких компьютеров, которую требуется разделить на 6 подсетей. Схема сети показана на рисунке ниже.



На всю сеть нам выделили один IP-адрес 192.168.0.0/24, который нам и требуется разделить на 6 подсетей. В двоичном виде этот IP-адрес выглядит так (порцию сети я выделю более жирным шрифтом): **11000000.10101000.00000000.**00000000 .
Требуемое количество узлов (хостов, в данном случае компьютеров) в каждой подсети:

- Подсеть A - 100 узлов

- Подсеть B - 50 узлов
- Подсеть C - 20 узлов
- Подсеть D - 2 узла
- Подсеть E - 2 узла
- Подсеть F - 2 узла

Запомните, начинать делить сеть требуется с сети с максимальным количеством узлов.
"/24" - это префикс маски подсети (краткая запись маски). Полная запись маски подсети 255.255.255.0. В двоичном отображении маска подсети выглядит так: 11111111.11111111.11111111.00000000 - это значит, что нам доступно 8 бит для деления сети.

BIN to DEC	
0000**0000**	0
0000**0001**	**1**
0000**0011**	3
0000**0111**	**7**
0000**1111**	15
0001**1111**	31
0011**1111**	63
0111**1111**	127
1111**1111**	255

infocisco.ru

Воспользуемся шпаргалкой выше (а именно таблицей "BIN to DEC"). Первой подсети A нам требуется выделить IP-адреса для 100 узлов. В таблице "BIN to DEC" мы видим, что заняв в маске один бит из восьми, мы получим 1 бит к порции сети (а это 2 подсети) и 7 битов в порции адреса (01111111 = 127). 127 вместе с нулем по количеству равен 128, это полное количество адресов, что удовлетворяет требованиям (и даже остается несколько адресов про запас).
И так, меняем маску с "/24" на "25" (в двоичном формате будет 11111111.11111111.11111111.10000000). Применим новую маску к нашей сети и получим 2 подсети (порцию сети я выделю более жирным шрифтом):
1 - **11000000.10101000.00000000.0**0000000 (сеть 192.168.0.0/25)
2 - **11000000.10101000.00000000.1**0000000 (сеть 192.168.0.128/25)
В новых двух сетях порция сети составляет 7 битов. По формуле (которая есть в шпаргалке) проверим, хватит ли нам 7 битов для сети со 100 узлами. 2^7-2=128-2=126, это значит что 7 битов даёт нам 126 адресов для узлов. (Напомню формулу: 2^X-2=количество адресов для узлов, где X равен количеству нулей, а "-2" - это под специальные адреса, которые нельзя назначать узлам.)
Осталась у нас одна сеть 192.168.0.128/25, и требуется для подсети B 50 адресов для узлов. Как и в предыдущий раз, мы видим в таблице "BIN to DEC" 00111111 = 63, это

больше 50, а значит удовлетворяет требованиям. Занимаем еще один бит у порции адреса, остается 6 (2^6-2=62). Маска становится на единицу больше /26, применяем её к нашей сети и получаем две новых подсети (порцию сети я выделю более жирным шрифтом):
1 - **11000000.10101000.00000000.10**000000 (сеть 192.168.0.128/26)
2 - **11000000.10101000.00000000.11**000000 (сеть 192.168.0.192/26)
Таким же образом отделяем еще 1 бит от порции адреса узла (00011111 = 31, что больше 20, и следовательно нам подходит), маска уже /27. Снова две сети: 1 - **11000000.10101000.00000000.110**00000 (сеть 192.168.0.192/27)
2 - **11000000.10101000.00000000.111**00000 (сеть 192.168.0.224/27)
Осталось нам выделить 3 подсети по 2 адреса для узлов. По таблице видим, что нам достаточно для порции адреса узла всего двух битов (00000011 = 3), 2^2-2=2 адреса для двух узлов.
В свою очередь для трех, одинаковых по размеру, подсетей достаточно тоже двух битов (2^2=4, формула из шпаргалки). Всего в IP-адресе 32 бита, вычитаем требующиеся нам 2 и получаем 30, следовательно используем маску /30. Для нашей оставшейся сети это выглядит так (порцию сети я выделю более жирным шрифтом): **11000000.10101000.00000000.11100**00 (сеть 192.168.0.224/30) .
Делим нашу новую сеть на 3 подсети:
1 - **11000000.10101000.00000000.11100**00 (сеть 192.168.0.224/30) .
2 - **11000000.10101000.00000000.11100**10 (сеть 192.168.0.228/30) .
3 - **11000000.10101000.00000000.11101**00 (сеть 192.168.0.232/30) .
Готово, задача выполнена:

- Подсеть A - 192.168.0.0/25
- Подсеть B - 192.168.0.128/26
- Подсеть C - 192.168.0.192/27
- Подсеть D - 192.168.0.224/30
- Подсеть E - 192.168.0.228/30
- Подсеть F - 192.168.0.232/30

Задание:

1. По выше приведенному примеру, разбить вашу сеть на подсети.

Практическое занятие № 7
Определение маршрутов следования информации в сети с помощью командной строки Cisco IOS.

Цель: Научится определять маршруты следования информации в сети с помощью командной строки Cisco IOS

Задачи
Часть 1. Проверка подключения к сети с помощью эхо-запроса с помощью команды ping
Часть 2. Отслеживание маршрута к удалённому серверу с помощью утилиты Windows «traceroute»
Часть 3. Отслеживание маршрута к удалённому серверу с помощью программных и веб-средств
Часть 4. Сравнение результатов трассировки

Исходные данные

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 лабораторной работы необходима программа VisualRoute. Если на вашем компьютере программа VisualRoute не установлена, загрузите её по следующей ссылке:
http://www.visualroute.com/download.html

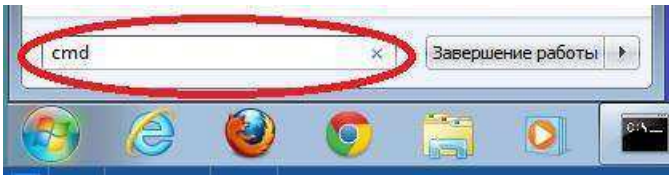
Если с загрузкой или установкой программы VisualRoute возникнут проблемы, обратитесь за помощью к инструктору. Убедитесь, что выполняется загрузка Lite Edition.

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

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.

1. 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.

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



3. 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
```

- 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.

- Возьмём приведённую ниже часть полученных результатов

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.

```
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

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
```

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**

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.
```

Сохраните результаты, полученные после ввода команды «tracert», в текстовый файл, выполнив указанные ниже действия.

Нажмите правой кнопкой мыши на строку заголовка окна командной строки и выберите параметры **Изменить** > **Выделить всё**.

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

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

Стандартные > **Блокнот**.

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

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

последовательно пронумерованные файлы.

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

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

© 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?

a. 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.

a. 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.

e. 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.

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

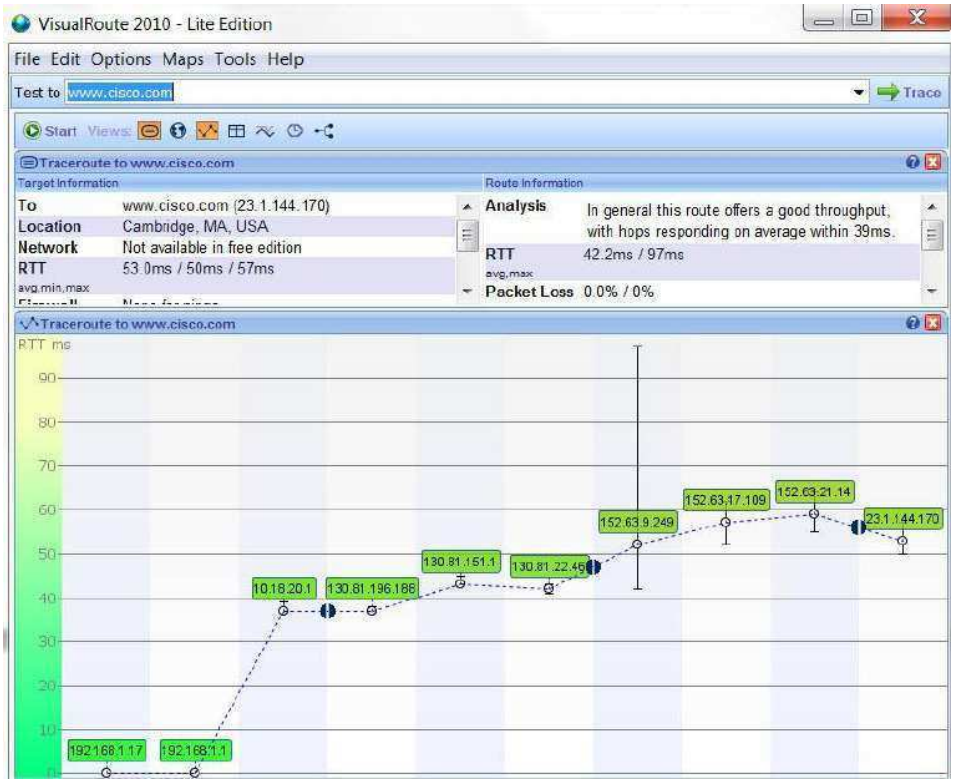
http://www.visualroute.com/download.html

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

Edition.

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

h. 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.

Практическое занятие №9

Настройка маршрутизатора включая динамический NAT

Цель: Настроить динамический NAT на маршрутезаторе в Cisco PT

Теория:

NAT (Network Address Translation) — технология трансляции сетевых адресов, т.е. подмены адресов в заголовке IP-пакета (иногда может еще и порт менять в заголовках TCP/UDP, но об этом позже).

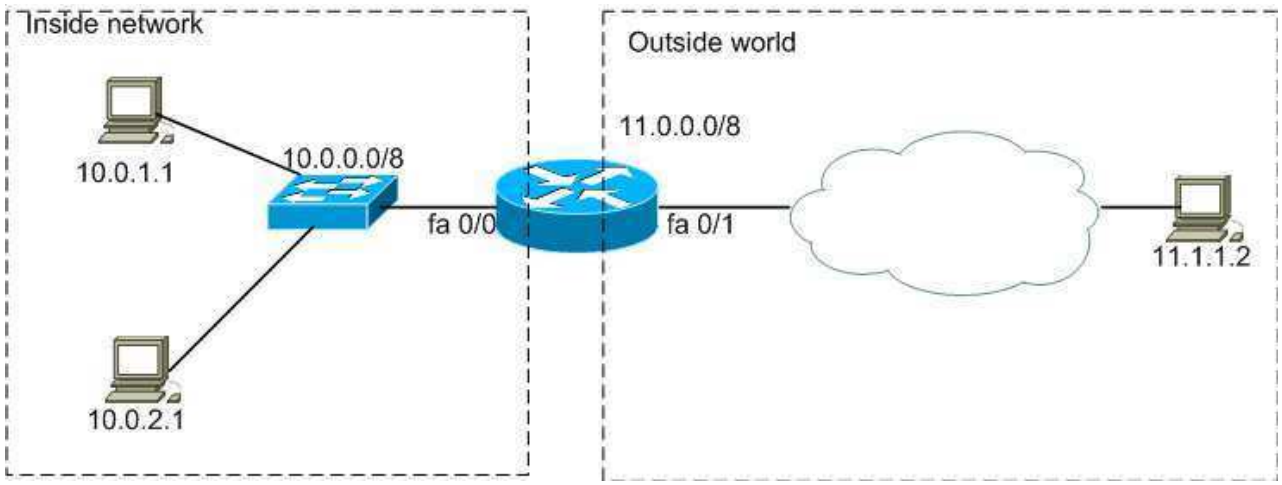
Другими словами, пакет, проходя через маршрутизатор, может поменять свой адрес источника и/или назначения.

Зачем это нужно?

1. Для обеспечения доступа из LAN, где чаще всего используются частные IP-адреса, в Internet, где маршрутизируются только глобальные IP-адреса.
2. (*в меньшей степени*) для сокрытия топологии сети и создания некоторого защитного барьера для проникновения внутрь сети (обсудим это позже на примере).

inside source NAT

Самый распространенный и достаточно простой вариант. Допустим у нас есть такая топология:



Другими словами,

а) подсеть внутренних адресов — 10.0.0.0/8

б) подсеть внешних адресов — 11.0.0.0/8

и мы хотим транслировать каким-то образом внутренние адреса во внешние при прохождении трафика через маршрутизатор.

Что для этого нужно?

1. Мы явно указываем, **что** мы хотим транслировать. Т.е. какой трафик и от каких хостов.
2. Мы явно указываем, **во что** мы хотим траслировать, т.е. пул внешних адресов (или единственный адрес для статической трансляции).
3. Помечаем внутренний и внешний интерфейс.
4. Включаем трансляцию.

Конфигурация inside source NAT

inside source dynamic NAT

1. Указываем, **что** транслировать. Для этого создаем access-list, перечисляющий трафик. Например, в нашем случае достаточно одной строчки:

(config)# access-list 100 permit ip 10.0.0.0 0.255.255.255 any

Замечание. В ACL могут встречаться строчки deny. Вопреки распространенному заблуждению, трафик удовлетворяющей данной строчке не дропается, а просто не подвергается трансляции. Так же, ACL может быть стандартным и расширенным, нумерованным и именованным.
2. Создаем пул из адресов, указывая стартовый и конечный адрес. Например так:

(config)# ip nat pool NAME_OF_POOL 11.1.1.10 11.1.1.20 netmask 255.255.255.0

Замечания.
1. Стартовый и конечный адрес в пуле могут совпадать, тогда трансляция будет в 1 адрес.
2. Опция netmask, хотя и является обязательной, по моему мнению — рудимент. Она позволяет вырезать из диапазона адресов в пуле те адреса, которые являются адресами подсети или бродкастными при данной маске.
3. Маркируем интерфейсы. В нашем случае достаточно

(config)# interface fa 0/0
(config-if)# ip nat inside

и

(config)# interface fa 0/1
(config-if)# ip nat outside

4. создаем собственно трансляцию:

ip nat inside source list 100 pool NAME_OF_POOL

вуаля :) Если мы теперь обратимся например с хоста 10.1.1.1 к хосту 11.1.1.2, то получим такую трансляцию:

Router#sh ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 11.1.1.10:55209 10.0.1.1:55209 11.1.1.2:23 11.1.1.2:23

Интересно, что хотя в таблице явно записаны source port и destination port, трансляция создается целиком для адреса. И на время ее жизни в таблице трансляция, пакеты снаружи могут проходить на внешний адрес (inside global) Например, пинг с некоторого адреса во внешней сети на наш inside global будет успешным (на время жизни трансляции):

R4#ping 11.1.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.1.1.10, timeout is 2 seconds:
!!!!!

Иными словами, открывается трансляция единожды и к некоторому хосту, после этого некоторое время действует для любого адреса извне.

Задание:

1. Ознакомится с примером приведенным в теории.
2. По примеру настроить NAT

Практическое занятие №9

Настройка маршрутизатора в качестве DHCP сервера

Цель: Насротить маршрутизатор в качестве DHCP сервера.

Задание:

Выполняем в Cisco PT

4. С помощью отрезка кроссоверного кабеля подключите компьютер к одному из Ethernet-портов маршрутизатора Cisco 1605 или другого, имеющегося в наличии.
5. Из конфигурационного режима создайте новый пул протокола DHCP с помощью команды **ip dhcp pool** ***name***, где ***name*** – имя вновь создаваемого пула.
6. В режиме конфигурации вновь созданного пула DHCP укажите с помощью команды **network** ***192.168.1.0 /24*** адреса, которые будут раздаваться клиентам.
7. Сконфигурируйте отдаваемые по DHCP адреса серверов DNS, для чего используйте команду **dns server** ***192.168.1.2 192.168.1.3***.
8. Аналогично предыдущему пункту сконфигурируйте адреса серверов WINS командой **netbios-name-server** ***192.168.1.4 192.168.1.5***.
9. Задайте IP-адрес шлюза по умолчанию для клиентов вызовом **default-router** ***192.168.1.1***.
10. Установите время аренды адреса клиентом, для чего выполните команду **lease** ***0 0 15***.
11. Выйдите из режима конфигурирования пула DHCP командой **exit**.
12. Настройте сетевую карту компьютера на автоматическое получение параметров IP.
13. Освободите полученный ранее адрес вызовом **ipconfig /release**.
14. Получите новые параметры с помощью **ipconfig /renew**.
15. Убедитесь в том, что вы получили конфигурацию протокола IP.
16. Просмотрите на маршрутизаторе таблицу выданных IP-адресов командой привилегированного режима командой **show ip dhcp binding**.
17. Исключите адреса *192.168.1.2* и *192.168.1.3* из пула выдаваемых адресов, для чего используйте команду режима конфигурации **ip dhcp excluded-address** ***192.168.1.2 192.168.1.3***. Если компьютеру был выдан какой-либо другой адрес, исключите и его из пула.
18. Откажитесь от используемого ранее адреса на лабораторном компьютере и запросите его вновь.
19. Убедитесь в том, что теперь сетевой карте компьютера присвоен другой адрес.
20. Сконфигурируйте статическую привязку MAC-адреса компьютера к выдаваемому сервером DHCP IP-адресу. Для этого создайте новый пул DHCP, внутри этого пула дайте команду **host** ***address mask***, где ***address*** и ***mask*** – IP-

адрес и сетевая маска конфигурируемого хоста. Выполните команду **client-identifier 01*aa.bbcc.ddee.ff***, где ***aabbccddeeff*** – MAC-адрес лабораторного компьютера, а **01** – указывает на тип среды Ethernet. Командой **client-name *test*** укажите имя настраиваемому клиенту.

21. Откажитесь на компьютере от текущего адреса и получите его вновь. Убедитесь в том, что полученный адрес – именно тот, который только что был жёстко сконфигурирован.

22. По подобию настроить в своей ранее разработанной сети DHCP-сервер на маршрутизаторе.

Практическое занятие № 10

Настройка соединения PPP между клиентом и поставщиком услуг интернета

Цель: Насторить соединение PPP.

Теория:

PPP позволяет использовать следующие параметры LCP.

- **Authentication (Аутентификация).**Соединённые маршрутизаторы обмениваются сообщениями проверки подлинности. Доступны два варианта аутентификации: на основе протокола PAP и на основе протокола CHAP.
- **Compression (Сжатие).** Эта функция повышает эффективную пропускную способность подключений PPP, уменьшая объём данных в кадре, передаваемом по каналу. Протокол распаковывает кадр в месте назначения. На маршрутизаторах Cisco доступно два протокола сжатия: Stacker и Predictor.
- **Error detection (Обнаружение ошибок)**. Эта функция определяет состояния сбоя. Параметры Quality и Magic Number способствуют обеспечению надёжного беспетлевого канала передачи данных. Поле Magic Number используется для обнаружения каналов, в которых возникла петля. До тех пор, пока не будет успешно завершено согласование параметра настройки Magic-Number, должно передаваться нулевое значение этого параметра. Значения параметра Magic-Number генерируются случайным образом на каждом конце подключения.
- **PPP Callback (Обратный вызов PPP)**. Обратный вызов PPP используется для повышения безопасности. При использовании этого параметра протокола LCP маршрутизатор Cisco может работать как клиент или сервер обратного вызова. Клиент выполняет начальный вызов, запрашивает у сервера обратный вызов и завершает начальный вызов. Маршрутизатор обратного вызова отвечает на начальный вызов и выполняет ответный вызов клиента на основе команд настройки. Используется команда **ppp callback** [**accept** | **request**].
- **Многоканальность**. Этот вариант обеспечивает распределение нагрузки между интерфейсами маршрутизатора, используемыми протоколом PPP. Протокол многоканального PPP, обозначаемый также MP, MPPP, MLP или Multilink, предоставляет метод распределения трафика между несколькими физическими каналами WAN, обеспечивая фрагментацию и повторную сборку пакетов, надлежащее упорядочивание, возможность использования оборудования различных поставщиков и балансировку нагрузки входящего и исходящего трафика.

Имя параметра	Тип параметра	Длина параметра	Описание
Протокол аутентификации	3	5 или 6	В этом поле указывается протокол аутентификации, PAP или CHAP.
Уплотнение протокола	7	2	Флаг, указывающий, что идентификатор протокола PPP должен быть сжат до одного октета, если двухбайтовый идентификатор протокола находится в диапазоне от 0x00-00 до 0x00-FF.
Уплотнение полей адреса и контроля	8	2	Флаг, указывающий, что поле PPP Address (всегда имеющее значение 0xFF) и поле PPP Control (всегда имеющее значение 0x03) должны быть удалены из заголовка PPP.
Magic Number (обнаружение ошибок)	5	6	Это произвольное число, выбранное для различения равноправных узлов и обнаружения каналов, в которых возникла петля.
Обратный вызов	13 или 0x0D	3	Индикатор длиной в 1 октет, указывающий способ определения обратного

-

Команды базовой настройки PPP

Запуск PPP на интерфейсе

Для настройки PPP в качестве метода инкапсуляции, используемого последовательным интерфейсом, служит команда настройки интерфейса**encapsulation ppp**.

В следующем примере активируется инкапсуляция PPP на интерфейсе serial 0/0/0.

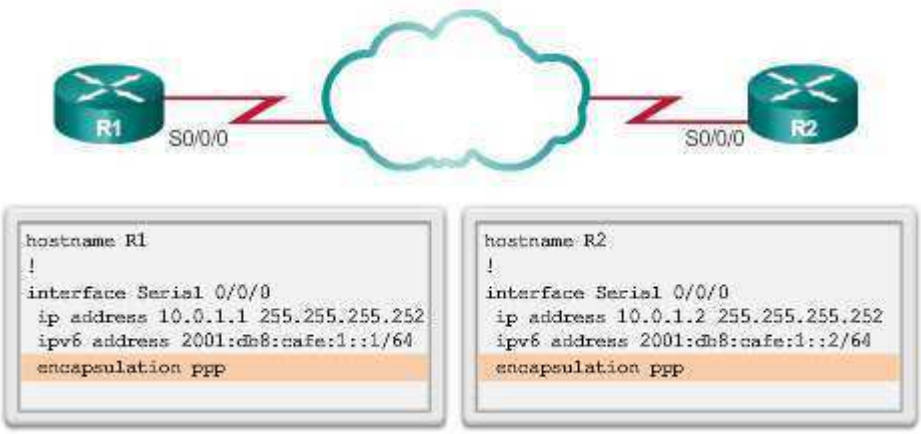
R3# ***configure terminal***

R3(config)# ***interface serial 0/0/0***

R3(config-if)# ***encapsulation ppp***

У команды **encapsulation ppp** нет аргументов. Помните, что если на маршрутизаторе Cisco не настроена инкапсуляция PPP, то по умолчанию для последовательных интерфейсов будет использоваться инкапсуляция HDLC.

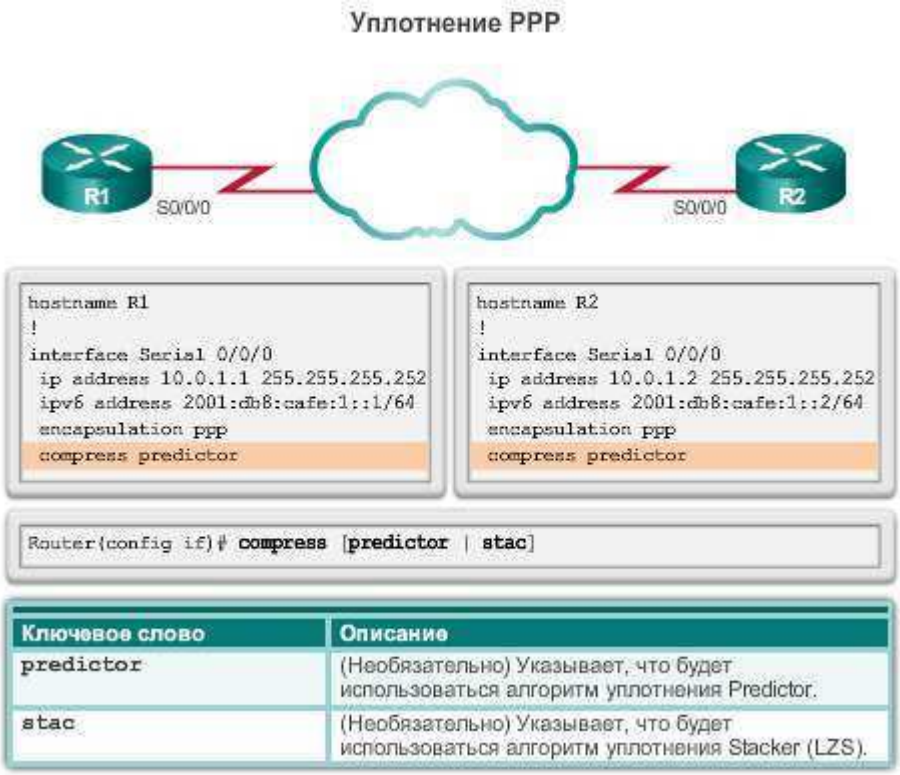
Базовая настройка PPP



На рисунке показаны маршрутизаторы R1 и R2, настроенные на использование на последовательных интерфейсах как адреса IPv4, так и адреса IPv6. PPP является инкапсуляцией уровня 2, поддерживающей различные протоколы уровня 3 протокола, включая IPv4 и IPv6.

Команды сжатия PPP

Настроить в протоколе «точка-точка» программное сжатие на последовательных интерфейсах можно после активирования инкапсуляции PPP. Поскольку в этом режиме вызывается процесс сжатия программным способом, он может повлиять на производительность системы. Если трафик уже состоит из сжатых файлов, таких как .zip, .tar или .mpeg, этой возможностью не следует пользоваться. На рисунке показан синтаксис команды**compress**.



Ключевое слово	Описание
predictor	(Необязательно) Указывает, что будет использоваться алгоритм уплотнения Predictor.
stac	(Необязательно) Указывает, что будет использоваться алгоритм уплотнения Stacker (LZS).

Для настройки сжатия при передаче по протоколу PPP введите следующие команды.

R3(config)# **interface serial 0/0/0**

R3(config-if)# **encapsulation ppp**

R3(config-if)# **compress** [**predictor** | **stac**]

Команда мониторинга качества канала PPP

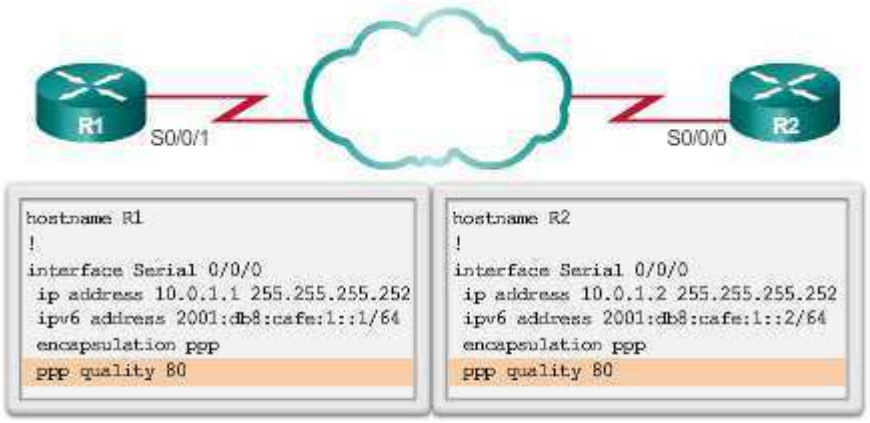
Помните, что LCP обеспечивает дополнительный этап определения качества канала. На этом этапе LCP проверяет канал, чтобы определить, является ли качество канала достаточным для использования протоколов уровня 3.

Команда **ppp quality** *percentage*обеспечивает соответствие канала установленному требованию к качеству; в противном случае канал закрывается.

Процентная величина рассчитывается как для входящего, так и для исходящего направления. Качество канала в исходящем направлении рассчитывается путем

сравнения общего числа отправленных пакетов и байтов с общим числом пакетов и байтов, полученных узлом назначения. Качество канала во входящем направлении рассчитывается путем сравнения общего числа полученных пакетов и байтов с общим числом пакетов и байтов, отправленных узлом назначения.
Если процентное выражение качества канала не поддерживается, то качество канала считается низким и канал отключается. В средстве наблюдения за качеством (LQM) реализован механизм задержки во времени, чтобы канал не подвергался последовательным активированиям и отключениям.

Мониторинг качества канала PPP




```
Router(config-if)# ppp quality percentage
```

Ключевое слово	Описание
percentage	Определяет пороговое значение для качества связи. Находится в диапазоне от 1 до 100.

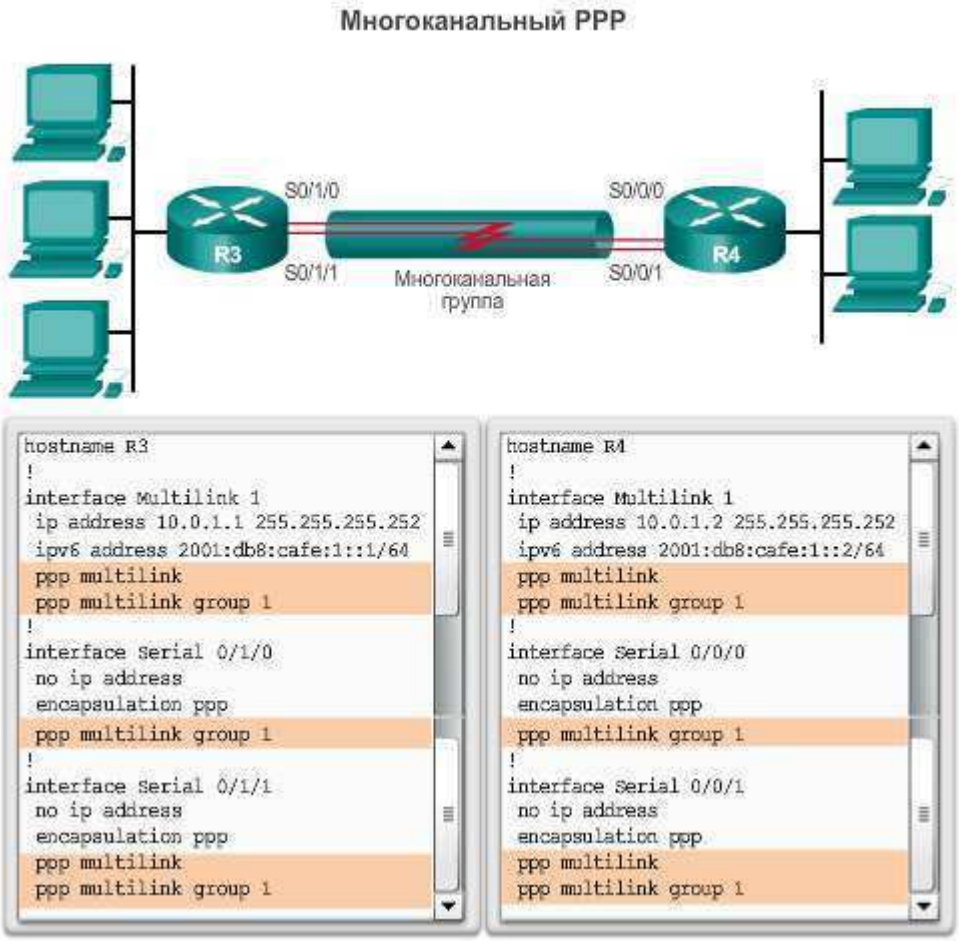
В следующем примере настройки осуществляется наблюдение за данными, переданными в канал, и обеспечивается предотвращение петель генерации кадров (см.рис).
R3(config)# **interface serial 0/0/0**
R3(config-if)# **encapsulation ppp**
R3(config-if)# **ppp quality 80**
Для отключения средства LQM используется команда **no ppp quality**.

Команды многоканального протокола PPP

Многоканальный протокол PPP (обозначается также MP, MPPP, MLP или Multilink) предоставляет метод распределения трафика между несколькими физическими каналами WAN. Многоканальный протокол PPP обеспечивает также фрагментацию и повторную сборку пакетов, надлежащее упорядочивание, возможность использования оборудования различных поставщиков и распределение нагрузки входящего и исходящего трафика.
MPPP позволяет фрагментировать пакеты и отправлять эти фрагменты одновременно по нескольким каналам «точка-точка» по одному и тому же удалённому адресу. В ответ на определённое пользователем пороговое значение

нагрузки открываются несколько физических каналов. MPPP может измерить нагрузку только во входящем трафике или только в исходящем трафике, но не общую нагрузку обоих трафиков.

Настройка MPPP выполняется в два шага (см. рисунок).



Шаг 1. Создание многоканальной группы.

- Многоканальный интерфейс создаётся командой **interface multilink** *number*.
- В режиме настройки интерфейса многоканальному интерфейсу назначается IP-адрес. В этом примере как адрес IPv4, так и адрес IPv6 настроены на маршрутизаторах R3 и R4.
- На интерфейсе запускается многоканальный PPP.
- Интерфейсу назначается номер многоканальной группы.

Шаг 2. Назначение интерфейсов многоканальной группе.

На каждом интерфейсе, входящем в многоканальную группу, выполняются следующие настройки.

- Активируется инкапсуляция PPP.
- Активируется многоканальный PPP.
- Производится привязка к группе посредством указания номера группы, настроенного в действии 1.

Для отключения многоканального PPP используется команда **no ppp multilink**.

Проверка настройки PPP

Для проверки правильности настройки инкапсуляции HDLC или PPP используется команда **show interfaces serial**. В выходных данных команды отображается настройка PPP (см. рис.).

```
R2# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.0.1.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, IPV6CP, CCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters 01:29:06
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
```

После настройки HDLC в выходных данных команды **show interfaces serial** должна отобразиться строкаencapsulation HDLC. Если настроен протокол PPP, должны отобразиться также состояния протоколов LCP и NCP. Обратите внимание, что протоколы управления сетью IPCP и IPV6CP открыты для IPv4 и IPv6, поскольку на маршрутизаторах R1 и R2 установлены и адреса IPv4, и адреса IPv6.

Проверка команд PPP

Команда	Описание
show interfaces	Отображает статистику для всех интерфейсов, настроенных на маршрутизаторе.
show interfaces serial	Отображает информацию о последовательном интерфейсе.
show ppp multilink	Отображает информацию о многоканальном интерфейсе PPP.

На рис. показан список команд для проверки PPP.

Команда **show ppp multilink**проверяет, активирован ли многоканальный протокол PPP на R3 (см. рис. 3).

```
R3# show ppp multilink

Multilink1
  Bundle name: R4
  Remote Endpoint Discriminator: [1] R4
  Local Endpoint Discriminator: [1] R3
  Bundle up for 00:01:20, total bandwidth 3088, load 1/255
  Receive buffer limit 24000 bytes, frag timeout 1000 ms
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x2 received sequence, 0x2 sent sequence
  Member links: 2 active, 0 inactive (max 255, min not set)
    Se0/1/1, since 00:01:20
    Se0/1/0, since 00:01:06
No inactive multilink interfaces
```

В выходных данных отражены интерфейс Multilink 1, имена узлов локальной и

удалённой оконечных точек и последовательные интерфейсы, включённые в многоканальную группу.

Задание:

1. Выполнить настройку PPP соединения.

Практическое занятие № 11

Настройка динамической маршрутизации. Протокол RIP. Проверка его работоспособности.

Цель : Формирование у студентов устойчивых навыков конфигурирования маршрутизаторов для работы с протоколом динамической маршрутизации RIP.

Ход работы

Для начала разберемся с тем, что же такое протокол динамической маршрутизации, какие особенности имеет протокол RIP и как он работает. Затем смоделируем сеть и настроим в ней протокол RIP. Наконец, посмотрим, с помощью каких команд проверяется работоспособность этого протокола.

Обзор протокола RIP

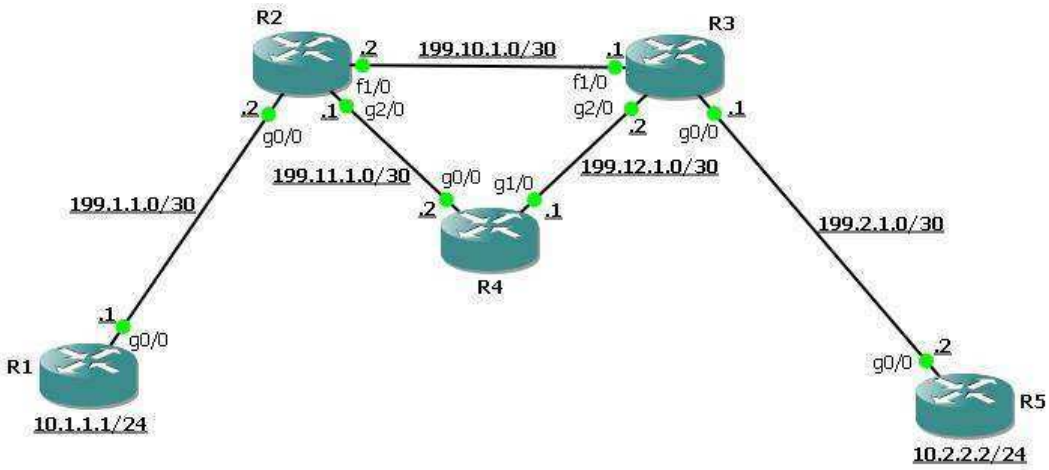
У всех протоколов динамической маршрутизации одна цель – строить оптимальную сетевую топологию без петель.

В данной лабораторной работе рассматривается RIPv2 (версии 2). RIP любой версии относится к протоколам маршрутизации внутреннего шлюза, является дистанционно-векторным протоколом и не учитывает состояния каналов. В качестве метрики в протоколе используется счетчик транзитных устройств, который учитывает, через сколько маршрутизаторов (или других L3-устройств) пролегает маршрут к сети. RIP осуществляет медленную конвергенцию[1] и по умолчанию имеет одну из наибольших стандартных административных дистанций[2] - 120. Кроме того, RIP не позволяет суммировать маршруты с маской короче классовой.

Для работы RIP использует четыре таймеры, перечисленные в таблице ниже.

Моделирование и настройка

Реализуем следующую сеть.



Для начала настроим все необходимые интерфейсы. На R1 это loopback, моделирующий сеть клиента, и интерфейс в сторону провайдера.

R1(config)# int lo1

R1(config-if)#ip addr 10.1.1.1 255.255.255.0

R1(config-if)# int g0/0

R1(config-if)#ip addr 199.1.1.1 255.255.255.252
R1(config-if)# no shutdown

Аналогично на R5.

R2(config)# int lo1

R2(config-if)#ip addr 10.2.2.2 255.255.255.0

R2(config-if)# int g0/0

R2(config-if)#ip addr 199.2.1.2 255.255.255.252
R2(config-if)# no shutdown

На R2 – интерфейсы GigabitEthernet и один интерфейс FastEthernet.

R2(config)# int g0/0

R2(config-if)#ip addr 199.1.1.2 255.255.255.252

R2(config-if)# no shutdown

R2(config-if)# int g2/0

R2(config-if)#ip addr 199.11.1.1 255.255.255.252
R2(config-if)# no shutdown

R2(config-if)# int f1/0

R2(config-if)#ip addr 199.10.1.2 255.255.255.252

R2(config-if)# no shutdown

Аналогично на R3 и на R4.

R3(config)# int g0/0

R3(config-if)#ip addr 199.2.1.1 255.255.255.252

R3(config-if)# no shutdown

R3(config-if)# int g2/0

R3(config-if)#ip addr 199.12.1.2 255.255.255.252

R3(config-if)# no shutdown

R3(config-if)# int f1/0

R3(config-if)#ip addr 199.10.1.1 255.255.255.252

R3(config-if)# no shutdown

R4(config)# int g0/0

R4(config-if)#ip addr 199.11.1.2 255.255.255.252

R4(config-if)# no shutdown

R4(config-if)# int g1/0

R4(config-if)#ip addr 199.12.1.1 255.255.255.252

R4(config-if)# no shutdown

В настоящий момент локальные сети клиента 10.1.1.1 и 10.2.2.2 не видят друг друга (отсутствует соответствующая маршрутная информация). Перейдём к настройке RIP. На каждом маршрутизаторе необходимо ввести следующие команды: в режиме глобальной конфигурации ***router rip***, чтобы перейти в режим

конфигурации протокола; ***network*** *адрес_сети*, чтобы включить протокол на нужных интерфейсах. Необходимо помнить, что в качестве адреса сети команды ***network*** нужно указывать только адрес классовой сети. Кроме того, введем команду ***no auto-summary*** для отключения суммирования сетей на границе маршрутизации.

Пример настройки маршрутизатора R1.

R1(config)# router rip

R1(config-router)# network 199.1.1.0

R1(config-router)# redistribute connected

R1(config-router)# no auto-summary

Замечание: если бы во второй строке мы указали в качестве сети адрес *10.1.1.0*, система не выдала бы никаких ошибок и предупреждений, тем не менее, протокол RIP включился бы на всех интерфейсах, подсети которых входили бы в сеть 10.0.0.0/8.

Важное замечание: с помощью команды ***redistribute connected*** мы добавили сети всех подключенных интерфейсов (в том числе и сеть интерфейса loopback) в базу данных протокола RIP – RIP DataBase (RDB), но не включили сам протокол на этих интерфейсах. Таким образом, информация об этой сети рассылается протоколом через все интерфейсы, на которых функционирует RIP (в нашем случае через gi0/0), но при этом остальные интерфейсы не рассылают RIP-пакеты и не слушают сеть на предмет входящих RIP-сообщений.

Пример настройки маршрутизатора R2.

R2(config)# router rip

R2(config-router)# network 199.10.1.0

R2(config-router)# network 199.1.1.0

R2(config-router)# network 199.11.1.0

R2(config-router)# no auto-summary

Настройка маршрутизатора R3.

R3(config)# router rip

R3(config-router)# network 199.10.1.0

R3(config-router)# network 199.2.1.0

R3(config-router)# network 199.12.1.0

R3(config-router)# no auto-summary

Настройка маршрутизатора R4.

R4(config)# router rip
R4(config-router)# network 199.12.1.0

R4(config-router)# network 199.11.1.0

R4(config-router)# no auto-summary

Настройка маршрутизатора R5.

R5(config)# router rip

R5(config-router)# network 199.2.1.0

R5(config-router)# redistribute connected
R5(config-router)# no auto-summary

Если на данном этапе настройки попытаться выполнить команду ***ping 10.2.2.2 source 10.1.1.1*** с R1, то маршрутизатор сообщит о недоступности узла с адресом 10.2.2.2. Дело в том, что по умолчанию запускается RIPv1, который поддерживает только с классовые сети. То есть в нашем случае в базу данных протокола будет добавлена только одна сеть вместо двух: 10.0.0.0/8 вместо 10.1.1.0/24 и 10.2.2.0/24, потому что RIPv1 не учитывает маски этих сетей.

Убедиться в этом можно путём просмотра таблицы маршрутизации и RDB на R2 и R3, которым маршрутизаторы R1 и R5 сообщают только о сети 10.0.0.0/8. Исправьте возникшую проблему, прописав команду ***version 2*** в режиме конфигурирования протокола маршрутизации на всех устройствах.

На этом настройка устройств завершена, перейдём непосредственно к тестированию.

Тестирование

1. С помощью команд ***ping 10.2.2.2 source 10.1.1.1*** и ***trace 10.2.2.2 source 10.1.1.1***, выполненных с маршрутизатора R1, убедитесь, что локальные сети клиента имеют доступ друг к другу.

2. Проанализируйте маршрут, которым следуют пакеты между двумя сетями, указанными в предыдущем пункте.

3. Отключите низкоскоростной канал между маршрутизаторами R2 и R3. Как изменится маршрут следования пакетов между сетями?

4. Используя команду ***show ip protocols***, проверьте настройки RIP на каждом маршрутизаторе.

5. Введите команду ***show ip route rip*** и проанализируйте её вывод.

6. Выполните перехват трафика между маршрутизаторами и проанализируйте сообщения RIP.

7. С помощью перехвата из предыдущего пункта продемонстрируйте работу метода расщепления горизонта в RIP.

«Плавающий» статический маршрут

В настроенной выше схеме трафик передаётся через канал FastEthernet, что может быть неэффективно из-за меньшей по сравнению с GigabitEthernet пропускной способностью. В этом пункте мы настроим так называемый «плавающий» маршрут, который поможет решить эту проблему.

Для начала необходимо отключить RIP на интерфейсах fa1/0 на R2 и R3.

R2(config)# router rip

R2(config-router)# no network 199.10.1.0

R3(config)# router
rip R3(config-
router)# no network
199.10.1.0

Теперь настроим статические маршруты в сторону сетей на интерфейсах loopback, но с административной дистанцией равно 130.

R2(config)# ip route 10.2.2.0 255.255.255.0 199.10.1.1 130

R3(config)# ip route 10.1.1.0 255.255.255.0 199.10.1.2 130

Добавим эти маршруты в RIP[3].

R2(config)# router rip

R2(config-router)# redistribute static

R3(config)# router rip

R3(config-router)# redistribute static

С помощью команды ***trace 10.2.2.2 source 10.1.1.1***, выполненной с маршрутизатора R1, убедимся, что пакеты идут через R4. Кроме того, посмотрим таблицу маршрутизации на R2 с помощью команды ***show ip route*** и убедимся, что статического маршрута в ней нет.

Теперь выключим интерфейсы в сторону R4.

R2(config)# int g2/0

R2(config-if)# shutdown

R3(config)# int g2/0

R3(config-if)# shutdown

Снова посмотрим таблицу маршрутизации и убедимся, что статический маршрут появился в таблице маршрутизации. Повторим с помощью команды trace 10.2.2.2 source 10.1.1.1 с R1, что связность сети не нарушена.

Практическое занятие № 12

Администрирование серверов и рабочих станций

Цель работы:

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

Теоретический материал

Введение в Windows Server 2003

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

Версии Windows Server 2003

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

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

- Windows Server 2003, Enterprise Edition, расширяет возможности Windows Server 2003, Standard Edition, обеспечивая поддержку служб кластеров, служб метакаталогов и служб для Macintosh. В ней также поддержи каются 64-разрядные процессоры Intel Itanium, оперативная память с возможностью ≪горячей≫ замены и неоднородный доступ к памяти (nonuniform memory access, NUMA). Эта версия поддерживает до 32 Гбайт оперативной памяти на процессорах x86, до 64 Гбайт оперативной памяти на процессорах Itanium и до 8 центральных процессоров.

- Windows Server 2003, Datacenter Edition, — самый надежный Windows-сервер. Эта версия поддерживает более сложную кластеризацию и способна работать с большими объемами оперативной памяти — до 64 Гбайт на процессорах x86 и до 128 Гбайт на процессорах Itanium. Минимальное количество процессоров для работы Datacenter Edition — 8, максимальное — 32.

- Windows Server 2003, Web Edition, предназначена для запуска служб Web при развертывании Web-узлов и Web-приложений. Для решения этих задач в данную версиювключены Microsoft .NET Framework, Microsoft Internet Information Sendees (IIS), AS P.NET и функции для равномерного распределения нагрузки на сеть, Многие другие функции, в частности Active Directory, в ней отсутствуют. Строго говоря, из стандартных компонентой Windows в этой версии предусмотрены лишь распределенная файловая система DFS, шифрованная файловая система EFS и удаленный рабочий стол. Версия Windows Server 2003, Web Edition, поддерживает до 2 Гбайт оперативной памяти и до двух центральных процессоров.

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

Различия в администрировании

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

- Рабочие группы — это свободные объединения компьютеров, в которых каждый компьютер управляется независимо.

- Домены — это объединения компьютеров, коллективно управляемых с помощью контроллеров домена, т. е. систем Windows Server 2003, регулирующих доступ к сети, базе данных каталога и общим ресурсам.

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

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

Домены, деревья и леса

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

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

Групповая политика

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

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

Любой сервер может поддерживать одну или более следующих ролей.

- Контроллер домена (Domain controller) — сервер, на котором работают службы каталогов и располагается хранилище данных каталога. Контроллеры домена также отвечают за вход в сеть и поиск в каталоге. При выборе этой роли на сервере будут установлены DNS и Active Directory. Почтовый сервер (POPS, SMTP) [Mail server (POP3, SMTP)] - сервер, на котором работают основные почтовые службы POP3 (Post Office Protocol 3) и SMTP (Simple Mail Transfer Protocol), благодаря чему почтовые POP3-клиенты домена могут отправлять и получать электронную почту. Выбрав эту роль, вы определяете домен по умолчанию для обмена почтой и создаете почтовые ящики. Эти службы удобны в небольших компаниях или при удаленном соединении, когда электронная почта необходима, но вполне может обойтись без функциональности Microsoft Exchange Server.

- Сервер печати (Print, server) — сервер, организующий доступ к сетевым принтерам и управляющий очередями печати и драйверами принтеров. Выбор этой роли позволит вам быстро настроить параметры принтеров и драйверов.

- Сервер потоков мультимедиа (Streaming media server) — сервер, предоставляющий мультимедийные потоки другим системам сети или Интернета. Выбор этой роли приводит к установке служб Windows Media. Эта роль поддерживается только в версиях Standard Edition и Enterprise Edition.

- Сервер приложений (Application server) — сервер, на котором выполняются Web-службы XML, Web-приложения и распределенные приложения. При назначении серверу этой роли на нем автоматически устанавливаются IIS, COM+ и Microsoft .NET Framework. При желании вы можете добавить к ним серверные расширения Microsoft FrontPage, а также включить или выключить ASP.NET.

- Сервер терминалов (Terminal Server) — сервер, выполняющий задачи для клиентских компьютеров, которые работают в режиме терминальной службы. Выбор этой роли приводит к установке Terminal Server. Для удаленного управления сервером устанавливать Terminal Server не нужно. Необходимый для этого удаленный рабочий стол (Remote Desktop) устанавливается автоматически вместе с ОС.

- Сервер удаленного доступа или VPN-сервер (Remote access/VPN server) — сервер, осуществляющий маршрутизацию сетевого трафика и управляющий телефонными соединениями и соединениями через виртуальные частные сети (virtual private network, VPN). Выбрав эту роль, вы запустите Мастер настройки сервера маршрутизации и удаленного доступа (Routing and Remote Access Server Setup Wizard). С помощью параметров маршрутизации и удаленного доступа вы можете разрешить только исходящие подключения, входящие и исходящие подключения или полностью запретить доступ извне.

- Узел кластера серверов (Server cluster node) — сервер, действующий в составе группы серверов, объединенных в кластер. Выбор этой роли приводит к запуску Мастера создания кластера (New Server Cluster Wizard), позволяющего создать новую кластерную группу, или Мастера добавления узлов (Add Nodes Wizard), который поможет добавить сервер к существующему кластеру. Эта роль поддерживается только в версиях Enterprise Edition и Datacenter Edition.

- Файл-сервер (File server) — сервер, предоставляющий доступ к файлам и управляющий им. Выбор этой роли позволит вам быстро настроить параметры квотирования и индексирования. Вы также можете установить Web-приложен и для администрирования файлов. В этом случае будет установлен IIS и включены страницы ASP (Active Server Pages).

- DHCP-сервер (DHCP Server) — сервер, на котором запущен DHCP (Dynamic Hose Configuration Protocol), позволяющий автоматизировать назначение IP-адресов клиентам сети. При выборе этой роли на сервере будет установлен DHCP и запущен Мастер создания области (New Scope Wizard).

- DNS-сервер (DNS Server) — сервер, на котором запущена служба DNS, разрешающая имена компьютеров в IP-адреса и наоборот. При выборе этой роли на сервере будет установлена DNS и запущен Мастер настройки DNS-сервера (Configure DNS Server Wizard).

- WINS-сервер (WINS server) — сервер, на котором запущена служба WINS (Windows Internet Name Service), разрешающая имена NetBIOS в IP-адреса и наоборот. Выбор этой роли приводит к установкеWINS.

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

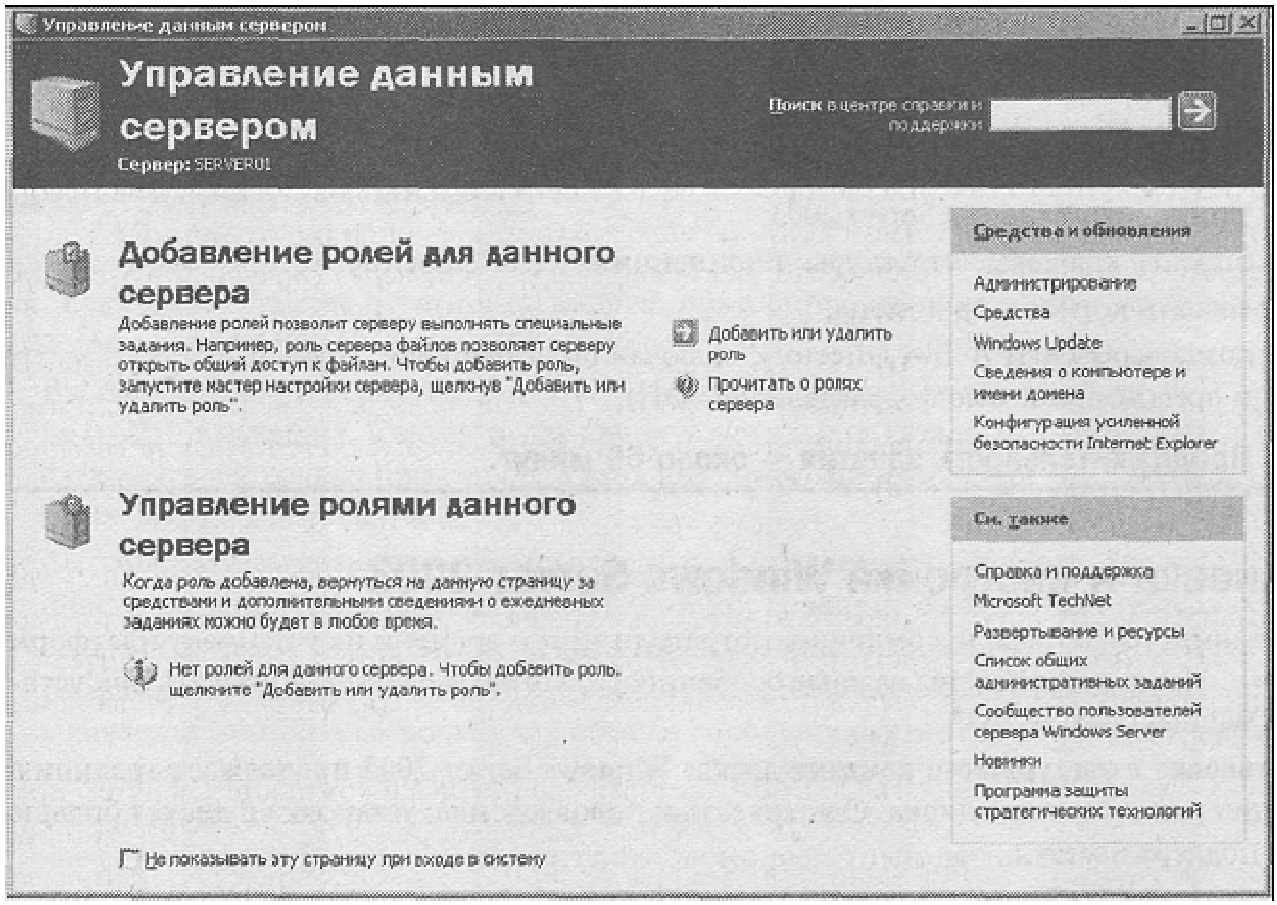


Рисунок 1. Страница Управление данным сервером

Таблица 1. Краткий справочник основных средств администрирования Windows Server 2003

Средство администрирования	**Назначение**
Active Directory — домены и доверие (Active Directory Domains and Trusts)	Управление доверительными отношениями между доменами
Active Directory — пользователи и компьютеры (Active Directory Users and Computers)	Управление пользователями, группами, компьютерами и другими объектами Active Directory
Active Directory — сайты и службы (Active Directory Sites and Service)	Создание сайтов для управления репликацией Active Directory
DHCP	Конфигурация и управление службой DHCP
DNS	Управление службой системы доменных имен (DNS)

WINS	Управление службой WINS, преобразующей имена NetBIOS в IP-адреса
Администратор кластеров (Cluster Administrator)	Управление службой Cluster
Администратор серверных расширений (Server Extensions Administrator)	Управление серверными расширениями, например FrontPage
Внешнее хранилище (Remote Storage)	Управление службой Remote Storage
Диспетчер служб Интернета (Internet Information Services Manager)	Управление Web-, FTP- и SMTP-серверами
Диспетчер служб терминалов (Terminal Services Manager)	Управление и МОЕНПЧЛШНГ пользователей, сеансов и процессов Terminal Service
Источники данных (ODBC) [Data Sources (ODBC)]	Добавление, удаление и настройка источников данных и драйверов ODBC (Open Database Connectivity)
Контроль допуска QpS (QoS Admission Control)	Управление службой Quality of Service (QpS) Admissions Control для регулировки пропускной способности сети
Лицензирование (Licensing)	Управление лицензированием доступа клиентов к серверным продуктам
Маршрутизация и удаленный доступ к сети (Routing and Remote Access)	Конфигурация и управление службой Routing and Remote Access, контролирующей интерфейсы маршрутизации, динамическую IP-маршрутизацию и удаленный доступ
Настройка сервера (Configure Your Server)	Добавление, удаление и конфигурация служб Windows для сети
Настройка служб терминалов	Управление настройкой протокола Terminal Service и параметрами

(Terminal Services Configuration)	сервера
Пакет администрирования диспетчера подключений (Connection Manager Administration Kit)	Конфигурирование и настройка диспетчера подключений
Политика безопасности домена (Domain Security Policy)	Просмотр и редактирование политики безопасности в домене
Политика безопасности контроллера домена (Domain Controller Security Policy)	Просмотр и редактирование политики безопасности для организационного полразделения контроллера домена
Производительность (Performance)	Отображение графиков производительности системы и настройка журналов и сигналов оповещения
Просмотр событий (Event Viewer)	Управление событиями и журналами
Распределенная файловая система DIFS (Distributed File System)	Создание и управление распределенными файловыми системами, объединяющими общие папки из разных компьютеров
Сетевой монитор (Microsoft Network Monitor)	Мониторинг сетевого трафика и устранение неисправностей в сети
Службы (Services)	Управление запуском и настройка служб Windows
Службы компонентов (Component Services)	Конфигурация и управление приложениями COM-, управление событиями и службами
Удаленные рабочие столы (Remote Desktop)	Настройка удаленных подключений и просмотр сеансов удаленных подключений
Управление компьютером(Computer Management)	Запуск и остановка служб, управление дисками и доступ к другим средствами управления системой

Центр сертификации (Certification Authority)	Управление сертификационными службами

Регистрация пользователя в системе

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

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

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

Рисунок 2. Диалоговое окно "Операционная система Windows"

Рисунок 3. Диалоговое окно "Вход в Windows"

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

Таблица 2. Параметры диалогового окна "Вход в Windows"

Параметры	**Описание**
User Name (Имя)	Введите уникальную учетную запись пользователя, присвоенную Вам администратором. Эта учетная запись должна присутствовать в базе данных каталогов на контроллерах домена, чтобы обеспечивать регистрацию в домене, и в базе данных каталогов локального компьютера — для регистрации на локальном компьютере
Password (Пароль)	Введите пароль, присвоенный указанному Вами имени пользователя, учитывая регистр символов. Чтобы пароль не стал достоянием посторонних, при его вводе символы на экране заменяются звездочками (*)

Domain (Домен)	Чтобы зарегистрироваться в домене, укажите его имя. При попытке регистрации пользователя в домене база данных контроллера домена проверяется на наличие соответствующего элемента. Регистрация по указанной учетной записи разрешается, если введенное имя пользователя, пароль и имя домена соответствуют данным в базе данных контроллера домена. Чтобы зарегистрироваться на локальном компьютере, укажите его имя. Локальный компьютер проверит наличие информации о Вас в локальной базе данных каталогов. Регистрация по указанной учетной записи разрешается, если введенное имя пользователя, пароль и имя компьютера соответствуют данным в локальной базе данных каталогов. Пользователь может зарегистрироваться на локальном компьютере, только указав имя пользователя, имеющееся в локальной базе данных каталогов. Серверы и компьютеры под управлением Windows 2003 содержат встроенные локальные учетные записи *Administrator* (Администратор) и *Guest* (Гость).

Проверка глобальной учетной записи

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

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

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

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

Проверка локальной учетной записи

Когда пользователь щелкает кнопку **ОК,** компьютер сначала проверяет указанное имя компьютера, а затем ищет имя пользователя и пароль в локальной

базе данных каталогов. Если имена совпадают, регистрация разрешается и пользователь получает доступ к локальным ресурсам. Если же нет, пользователь не получает доступ к компьютеру.

Функции администратора Windows 2003

Администрирование Windows NT подразумевает выполнение как специальных операций после установки системы, так и рутинных каждодневных действий.

Функции администратора можно разделить на пять категорий.

Таблица 3. Функции администратора

Категория	**Характерные задачи**
Администрирование учетных записей пользователей и групп	Планирование, создание и ведение учетных записей пользователей и групп для обеспечения каждому пользователю возможности регистрации в сети и доступа к необходимым ресурсам
Администрирование защиты	Планирование и реализация стратегии безопасности для защиты данных и общих сетевых ресурсов, в том числе папок, файлов и принтеров
Администрирование принтеров	Настройка локальных и сетевых принтеров для обеспечения пользователям доступа к ресурсам печати. Устранение обычных проблем печати
Мониторинг событий и ресурсов сети	Планирование и реализация стратегии аудита событий в сети с целью обнаружения нарушений защиты. Управление ресурсами и контроль их использования
Резервное копирование и восстановление данных	Планирование и выполнение регулярных операций резервного копирования для обеспечения быстрого восстановления важных данных

Средства администратора Windows 2003

Средства администрирования входят в состав Windows 2003 и могут применяться или для администрирования любого компьютера домена, или для администрирования локального компьютера.

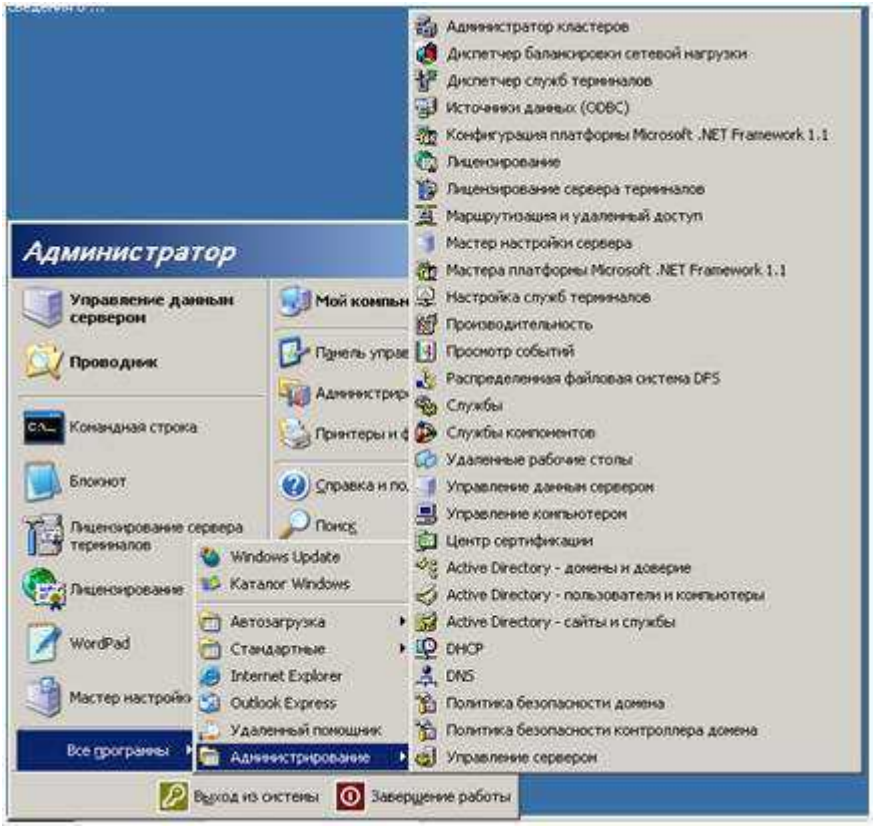


Рисунок 4. Средства администрирования

Таблица 4. Средства администрирования

Средство	**Назначение**
Администратор кластеров	Администратор кластеров - это основное средство администрирования и конфигурирования объектов кластера серверов, таких как узлы, группы и другие ресурсы. Это позволяет вам управлять кластером серверов без необходимости физического присутствия в одном из узлов.
Диспетчер балансировки сетевой нагрузки	Обеспечивает балансирование IP-трафика между несколькими серверами. Не обеспечивает переход по отказу (failover) для приложений и данных.
Диспетчер служб терминалов	Позволяет управлять конфигурацией сервера служб терминалов

Конфигурация платформы Microsoft .NET Framework 1.1	Позволяет настраивать среду .NET Framework
Лицензирование	Утилита, позволяющая управлять клиентскими лицензиями в масштабах предприятия
Лицензирование сервера терминалов	Утилита, позволяющая управлять клиентскими лицензиями для служб терминалов (Terminal Services), работающих в режиме выполнения приложений
Маршрутизация и удалённый доступ	Служит для управления маршрутизацией и удаленным доступом
Мастер настройки сервера	Мастер, позволяющий администратору настроить сервер в соответствии с выбранными ролями (файловый сервер, сервер служб Интернета и т. д.)
Производительность	Каждый компьютер с Windows Server 2003 содержит компоненты, мониторинг которых можно выполнять с помощью оснастки Performance (Производительность). Это могут быть аппаратные или программные компоненты, которые выполняют задачи или поддерживают рабочую нагрузку. Многие из этих компонентов имеют показатели, отражающие определенные аспекты их функционирования, которые можно точно измерить как скорость выполнения задач.
Просмотр событий	Служит для просмотра и управления системным журналом, журналами безопасности и приложений
Распределенная файловая система DFS	Создает и управляет распределенными файловыми системами, объединяющими совместно используемые папки на различных компьютерах
Службы	Запускает, останавливает и конфигурирует службы (сервисы) Windows

Службы компонентов	Конфигурирует и управляет службами компонентов COM+
Удалённые рабочие столы	Позволяет управлять многочисленными сессиями терминального доступа к удаленным компьютерам
Управление данным сервером	Мастер, представляющий собой информационный центр для управления различными ролями сервера, обращения к службам поддержки и вспомогательным инструментам, а также позволяющий быстро находить информацию об обновлениях, способах решения проблем и т. п.
Управление компьютером	Предоставляет функции администрирования системы. Содержит в своем составе ряд изолированных оснасток и оснасток расширения
Центр сертификации	Позволяет работать с центрами сертификации, развернутыми в корпоративной сети
Active Directory - домены и доверие	Служит для управления доменами и доверительными отношениями
Active Directory — сайты и службы	Определяет топологию и расписание репликации Active Directory. Обеспечивает изменение служб корпоративного уровня
Политика безопасности домена	Служит для управления параметрами безопасности (представленными в узле Security Settings объекта групповой политики, привязанного к объекту домена) для всего домена
Политика безопасности контроллера домена	Служит для управления параметрами безопасности (представленными в узле Security Settingsобъекта групповой политики, привязанного к подразделению Domain Controllers) на контроллерах домена

Мониторинг ресурсов

Сведения о системе

Утилита System Information (Сведения о системе) (Winmsd.exe) представляет исчерпывающую информацию об аппаратном обеспечении компьютера, системных компонентах и программной среде. Системная информация разделена на категории, которым в окне структуры соответствуют следующие узлы (Рисунок 5): **System Summary** (Сведения о системе),**Hardware Resources** (Ресурсы аппаратуры), **Components** (Компоненты), **Software Environment** (Программная среда) и **Internet Settings** (Параметры Интернета).

- Узел **System Summary** отображает общую информацию о компьютере и операционной системе: версию ОС и номер сборки, тип процессора, объем ОЗУ, версию BIOS, региональные установки, а также информацию об объеме физической и виртуальной памяти на компьютере.

- Узел **Hardware Resources** отображает информацию об аппаратных установках, таких как каналы DMA, номера прерываний (IRQ), адреса ввода/вывода (I/O) и адреса памяти. Узел **Conflicts/Sharing** (Конфликты/ Совместное использование) идентифицирует устройства, которые совместно используют ресурсы или конфликтуют с другими ресурсами. Такая информация помогает выявлять проблемы, возникающие с аппаратными устройствами.

- Узел **Components** отображает информацию о конфигурации Windows и используется для определения статуса драйверов устройств, сетевых устройств и программного обеспечения мультимедийных устройств. Кроме того, данный узел содержит обширную информацию об истории драйверов с записью всех изменений, которые производились с компонентами.

- Узел **Software Environment** отображает "снимок" программного обеспечения, загруженного в память компьютера. Данная информация может быть использована для просмотра списка выполняющихся задач или для выяснения номера версии продукта.

- Узел **Internet Settings** содержит, в частности, информацию о настройках программы Internet Explorer.

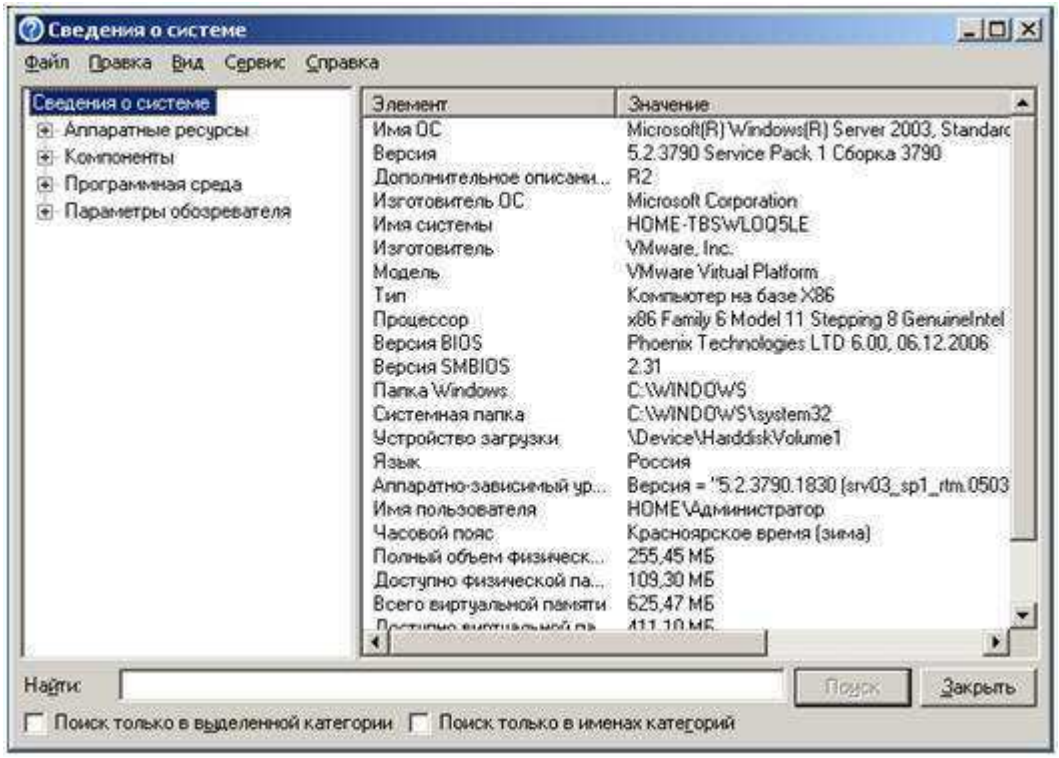


Рисунок 5. Внешний вид утилиты "Сведения о системе"

Составление и печать сводки

- Информация, предоставляемая программой System Information (Сведения о системе), нужна не только организации, осуществляющей поддержку, — напечатанная сводка может пригодиться службе инвентаризации. Из сводки можно быстро узнать объем оперативной памяти и дискового пространства на конкретном компьютере, а также, какие устройства на нем установлены.

- Распечатать постранично или всё целиком можно из меню **Файл->Печать.** Сохранить общий отчёт можно из меню **Файл->Экспорт**.

Управление компьютером

Инструмент (и одноименная оснастка) Computer Management (**Управление компьютером**) (Рисунок 6) является одним из основных средств системного администратора для конфигурирования компьютера. Данную оснастку можно использовать для администрирования, как локальной системы, так и удаленных компьютеров (в том числе систем Windows 2000 и — с некоторыми ограничениями — компьютеров с Windows NT 4.0). Это позволяет администратору со своего рабочего места устранять проблемы и конфигурировать любой компьютер в сети, на котором установлена Windows Server 2003.

Для запуска оснастки Computer Management можно пользоваться двумя способами: выбрать соответствующую команду в меню Start | Administrative

Tools или щелкнуть правой кнопкой мыши на команде My Computer(Мой компьютер) в меню Startи выбрать в контекстном меню пункт Manage(Управление).

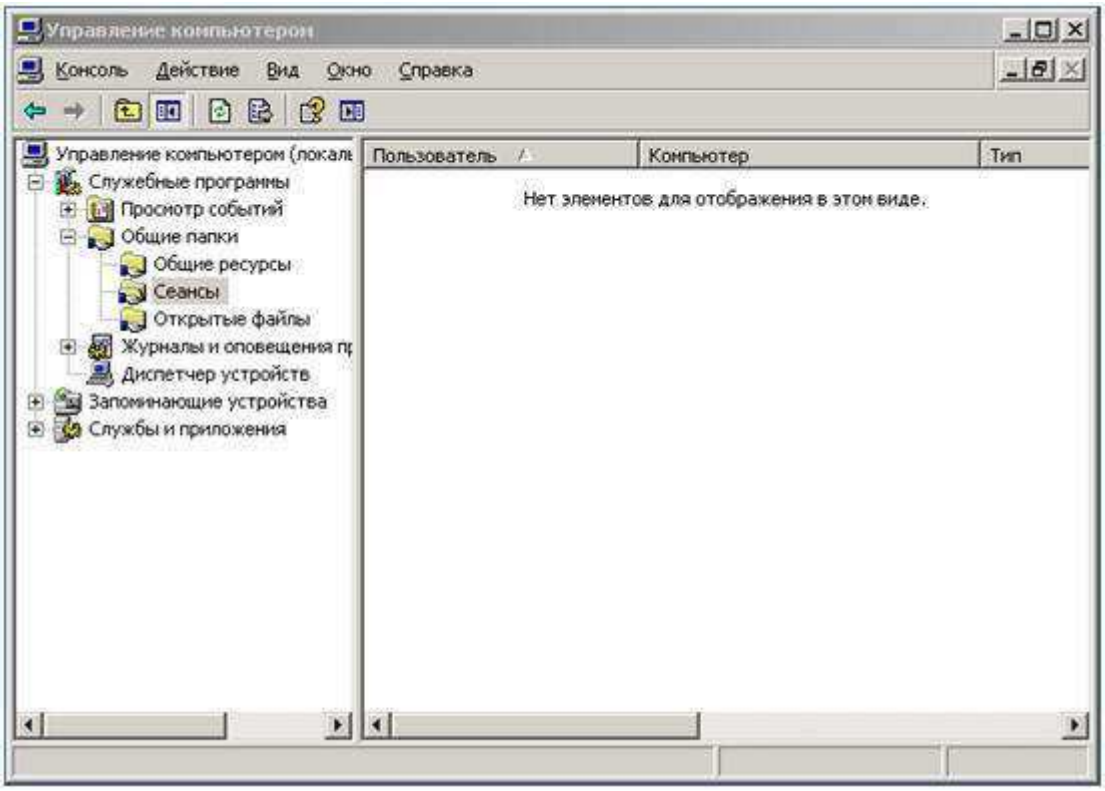


Рисунок 6. Оснастка "Управление компьютером"

Просмотр пользовательских сеансов

Оснастка **Shared Folders**(Общие папки) позволяет просматривать информацию о соединениях и использовании ресурсов локального или удаленного компьютеров. Данная оснастка используется вместо программы Server в Control Panel системы Windows NT 4.0.
Оснастка **Shared Folders** содержит три узла: **Shares** (Ресурсы), **Sessions** (Сеансы) и **Open Files** (Открытые файлы). При выборе данных узлов в панели результатов отображается содержание соответствующего узла.

С помощью оснастки можно выполнять следующие задачи:

- создавать, просматривать, изменять свойства и удалять общие ресурсы на локальном или удаленном компьютерах (Windows NT 4.0/2000/XP и Windows Server 2003) и устанавливать разрешения на доступ к ним. Кроме того, можно управлять режимом кэширования общих папок (в случае их использования в качестве изолированных папок). В системах Windows XP и Windows Server 2003 появилась очень удобная новая возможность управления процессом публикации общей папки в каталоге Active Directory (рис. 6.12) — можно сразу после создания общей папки опубликовать ее в каталоге, не прибегая к помощи

оснастки Active Directory Users and Computers. Все необходимые действия достаточно очевидны из содержания приведенного примера: в данном случае публикуется общая папка службы факсов, содержащая клиентское программное обеспечение для систем, не имеющих его (например, Windows 9x);

- просматривать список удаленных пользователей, подключенных к компьютеру, и отключать их;

- просматривать список файлов, открытых удаленными пользователями, и закрывать открытые файлы.

Windows 2003 Backup

Регулярное резервное копирование информации с серверов и локальных жестких дисков предотвращает утрату и повреждение данных из-за поломки жесткого диска, отключения питания, воздействия вирусов и т.д. Резервное копирование при грамотном планировании и наличии надежного оборудования позволяет безболезненно справиться с последствиями катастрофы.

Графическое инструментальное средство Windows 2003 Backup предназначено для автоматического и ручного резервного копирования и восстановления файлов, расположенных на разделах файловых систем FAT и NTFS.

Выбор стратегии резервного копирования

Перед тем как приступать к резервному копированию файлов, нужно разработать стратегию, отвечающую потребностям Вашей организации и гарантирующую восстановление утраченных данных. Эффективное архивирование и восстановление информации — одна из самых важных задач администратора.

Отбор файлов для резервного копирования

По степени важности (а следовательно, и по частоте создания резервных копий) папки и файлы можно разделить на три категории:

- важные — их резервные копии создаются всегда;

- полезные — их резервные копии создаются изредка;

- малозначимые — их резервные копии не создаются никогда.

Отбирая файлы для резервного копирования, учитывайте следующие правила:

- всегда создавайте резервные копии

o файлов, жизненно важных для работы Вашей организации;

o реестров всех главных и резервных контроллеров домена (каждый контроллер домена имеет свою копию базы данных каталогов; резервное копирование реестра контроллера домена предотвращает потерю информации об учетных записях пользователей и защите).

- резервные копии файлов, изменяемых редко или не представляющих особой ценности, следует создавать лишь время от времени.

- не сохраняйте временные файлы, так как они постоянно изменяются, и вряд ли могут быть использованы для восстановления данных.

Выбор типа резервного копирования

Windows 2003 Программа архивации (Backup Utility) предлагает пять вариантов резервного копирования: *обычное* (normal), *копирующее* (copy), *инкрементальное* (incremental), *разностное* (differential) и *ежедневное* (daily). Выбор стратегии резервного копирования определяется тем, сколько времени отводится на сохранение данных и каковы требования к скоростям поиска резервных копий и восстановления файлов.

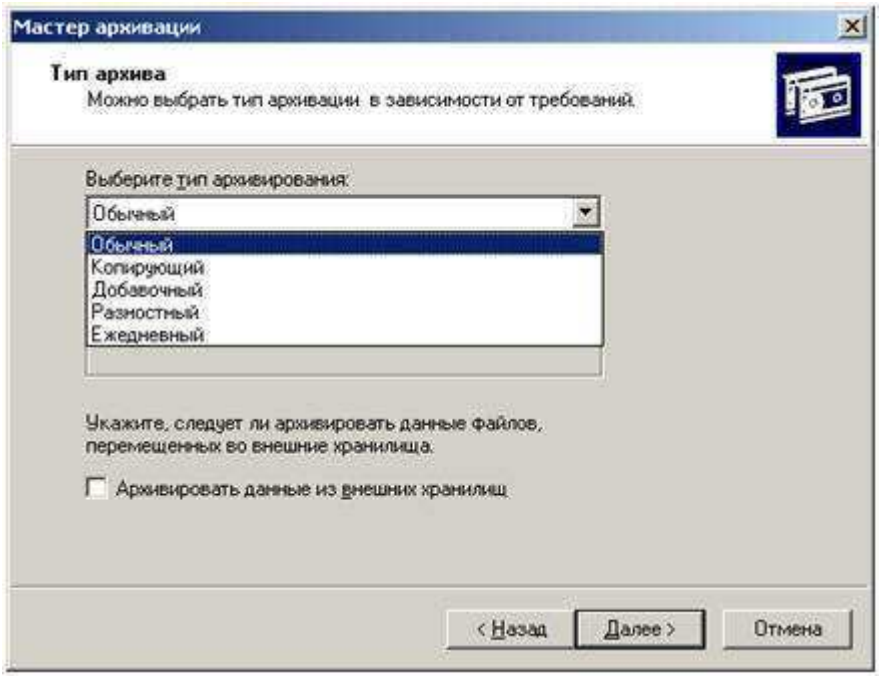


Рисунок 7. Выбор типа архивации

Краткая характеристика перечисленных выше типов резервного копирования приведена в таблице.

Таблица 5. Варианты резервного копирования

Варианты резервного копирования	**Характеристика**
Обычное или полное	Архивирует выбранные файлы и помечает их как сохраненные. Обычное резервное копирование позволяет быстро восстанавливать файлы, так как наиболее свежие файлы находятся на последней ленте. Для создания первой резервной копии всегда следует применять обычное резервное копирование всех файлов
Инкрементальное или добавочное	Архивирует только файлы, созданные или измененные с момента выполнения последнего обычного или инкрементального резервного копирования. Эти файлы помечаются флажком архивации. Если Вы сочетаете обычное и инкрементальное резервное копирование, то воссоздание информации начинается с восстановления последней обычной резервной копии, а затем последовательно восстанавливаются файлы инкрементальных копий
Разностное	Архивирует файлы, созданные или измененные со времени последнего обычного (или инкрементального) резервного копирования. Файлы при этом не помечаются флажком архивации. При комбинации обычного и разностного резервного копирования для восстановления данных требуются лишь 2 ленты: с последней обычной и с последней разностной копиями
Копирующее	Архивирует выбранные файлы, не помечая их флажком архивации. Тем самым не оказывает влияния на операции обычного и инкрементального резервного копирования и может применяться для промежуточного сохранения данных
Ежедневное копирование	Архивирует выбранные, файлы, которые были изменены во время ежедневного копирования.

	Файлы не помечаются флажком архивации. Эта операция полезна, например, когда Вы берете работу на дом и хотите быстро выбрать файлы, над которыми сегодня работали

Журналы резервного копирования

Журнал резервного копирования (backup log) — это текстовый файл, в котором регистрируются операции резервного копирования (рис. 8). Он полезен при восстановлении данных. Его можно либо распечатать, либо посмотреть в любом текстовом редакторе. Журнал хранится на диске, поэтому в случае повреждения каталога архива на ленте обратитесь к нему, чтобы найти нужный файл.

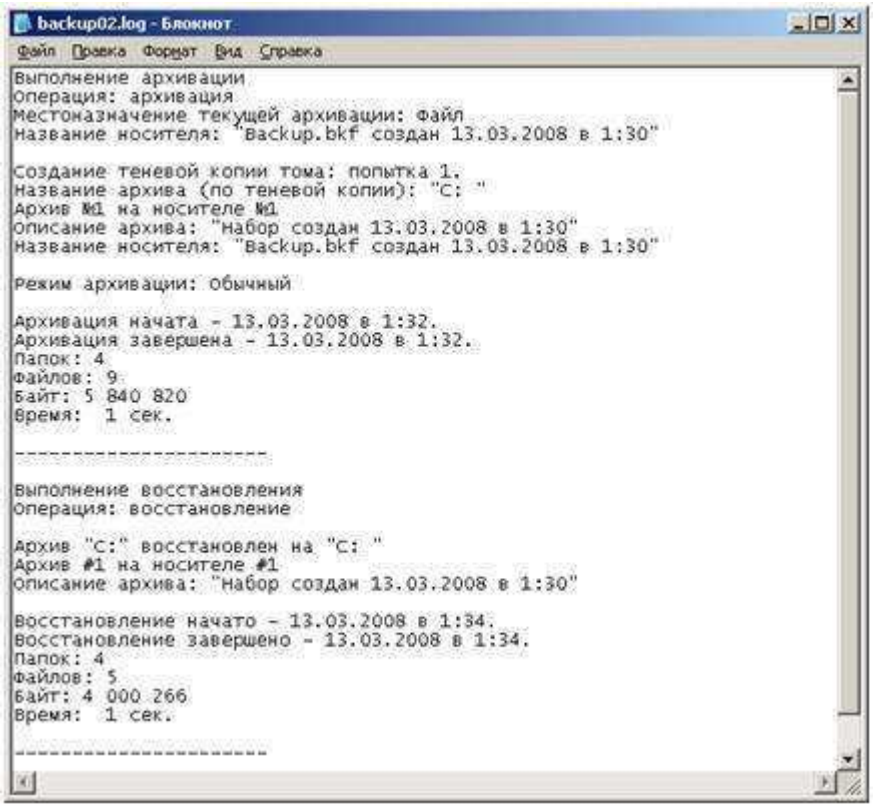


Рисунок 8. Журнал резервного копирования

Журнал резервного копирования содержит следующую информацию:

- дату создания архива;
- название варианта резервного копирования;

местонахождение накопителя.

Шаблон плана резервного копирования

Местонахождение накопителя __ Местонахождение лент_____

Путь к архивируемым файлам и папкам	**Ежедневное резервное копирование**	**Еженедельное резервное копирование (укажите день)**

Недельное расписание резервного копирования

Понедельник	**Вторник**	**Среда**	**Четверг**	**Пятница**
Тип копирования	**Тип копирования**	**Тип копирования**	**Тип копирования**	**Тип копирования**
Лента	**Лента**	**Лента**	**Лента**	**Лента**
Архив: Да Нет	**Архив: Да Нет**	**Архив: Да Нет**	**Архив: Да Нет**	**Архив: Да Нет**

Типы резервного копирования:

О = Обычное, Д = Инкрементальное, Р = Разностное, К = Копирующее, ЕК = Ежедневное копирование

Резервное копирование файлов

Программа резервного копирования Windows 2003 выглядит следующим образом. (рис. 9)

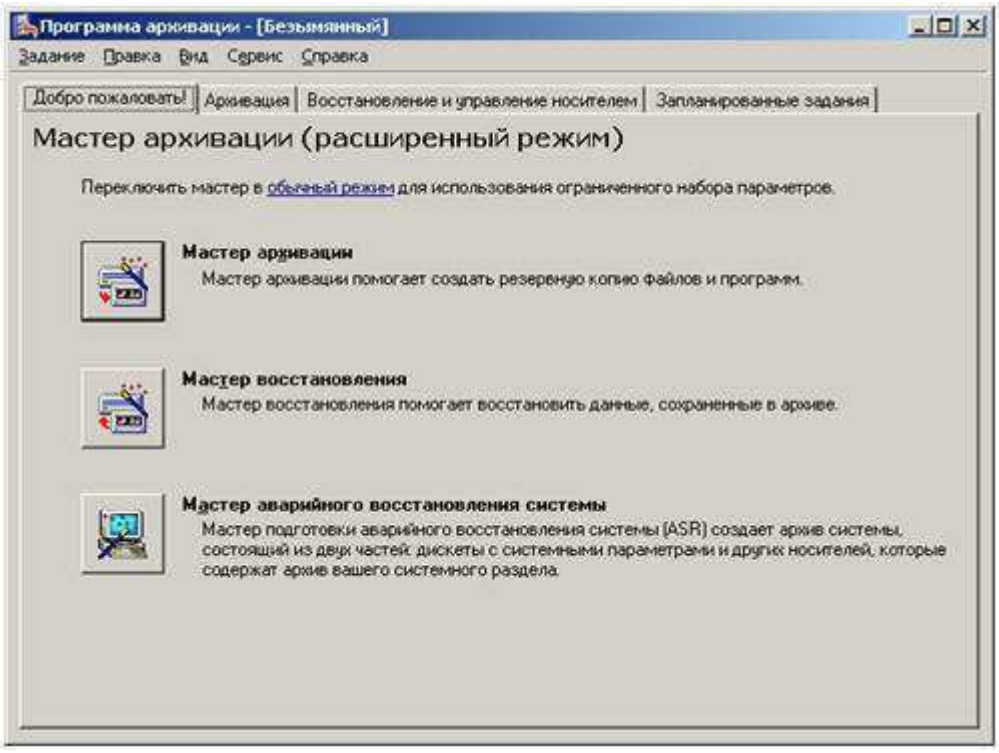


Рисунок 9. Окно мастеров архивации

Чтобы запустить программу, в меню **Start** (Пуск) выберите пункты **Programs** (Программы), **Accessories** (Стандартные), **System Tools** (Служебные), **Backup** (Архивация данных).

На рис. 10 представлены мастера архивации. Здесь можно выбрать 3 мастера: мастер архивации, мастер восстановления и мастер аварийного восстановления системы.

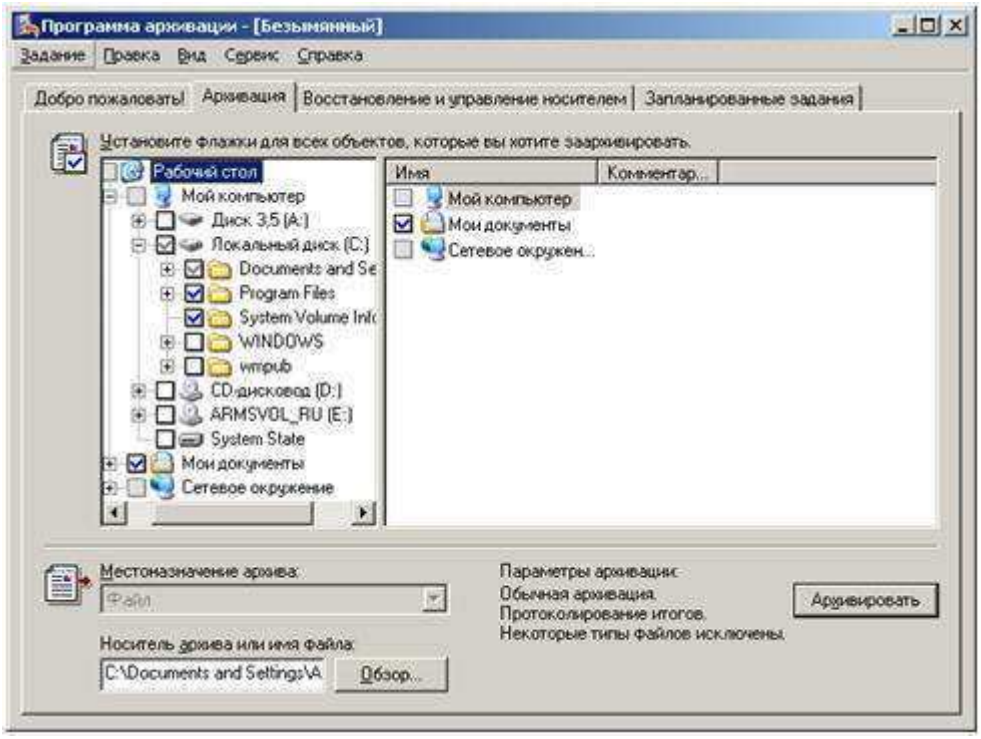


Рисунок 10. Окно "Архивация"

На рисунке 10 представлено окно архивации. Здесь можно выбрать параметры архивации: объекты архивации и назначение архивации. Можно также выбрать дополнительные параметры архивации (рисунок 11).

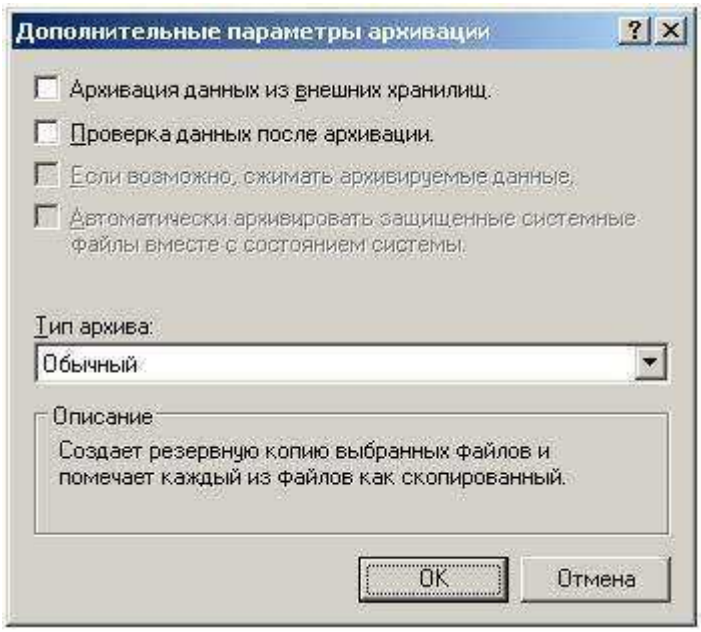


Рисунок 11. Окно "Дополнительные параметры архивации"

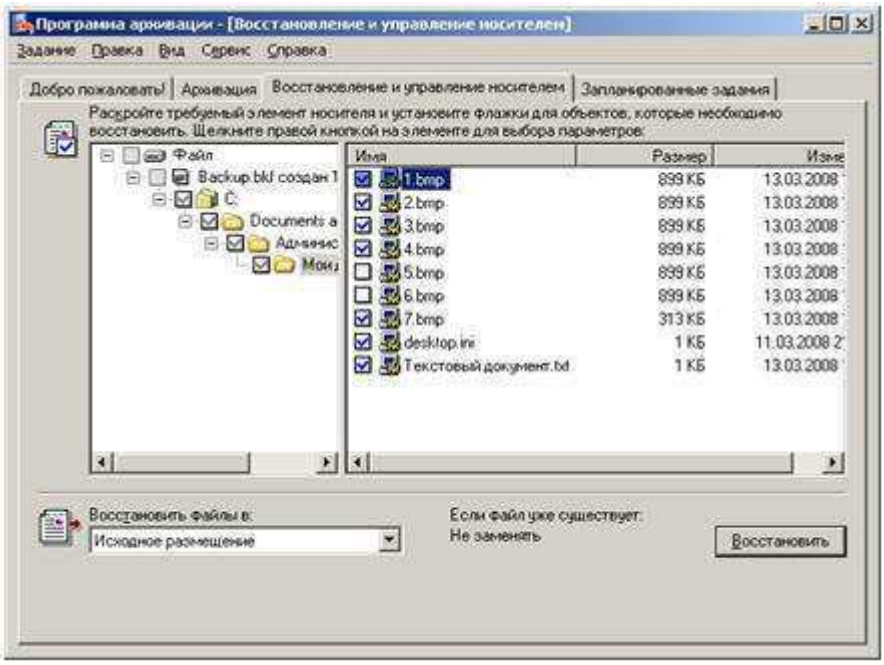


Рисунок 12. Окно "Восстановление и удаление носителем"

На рисунок 12 представлено окно восстановления управления носителем. Здесь можно выбрать необходимые для восстановления объекты.

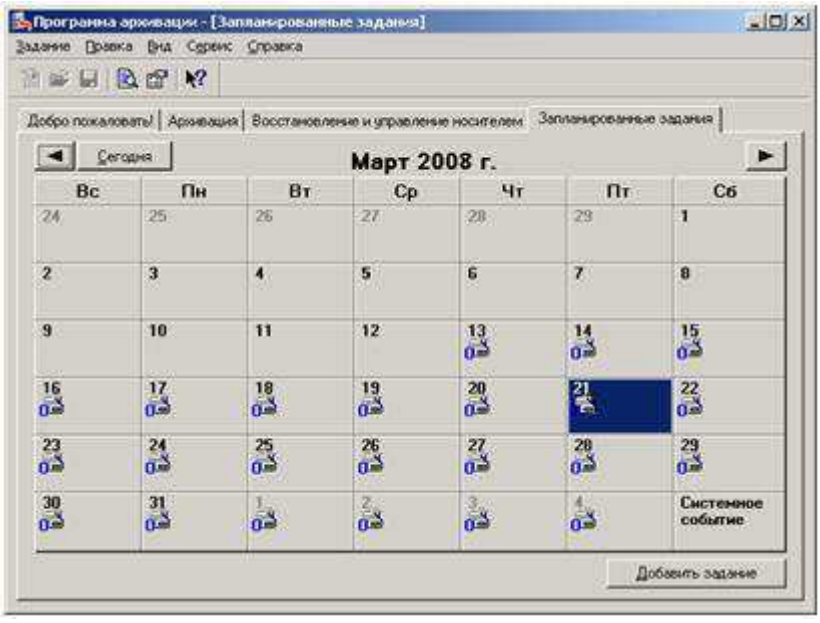


Рисунок 13. Окно "Запланированные задания"

На рисунок 13 представлено окно планировщика заданий. Здесь можно создать задание архивации, путем вызова мастера архивации (рисунок 14).

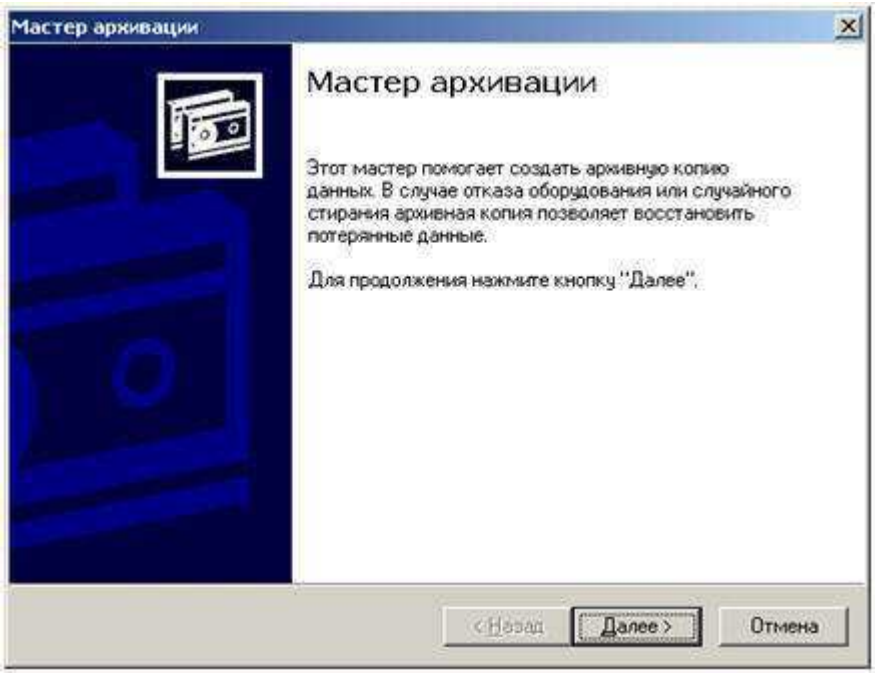


Рисунок 14. Мастер архивации

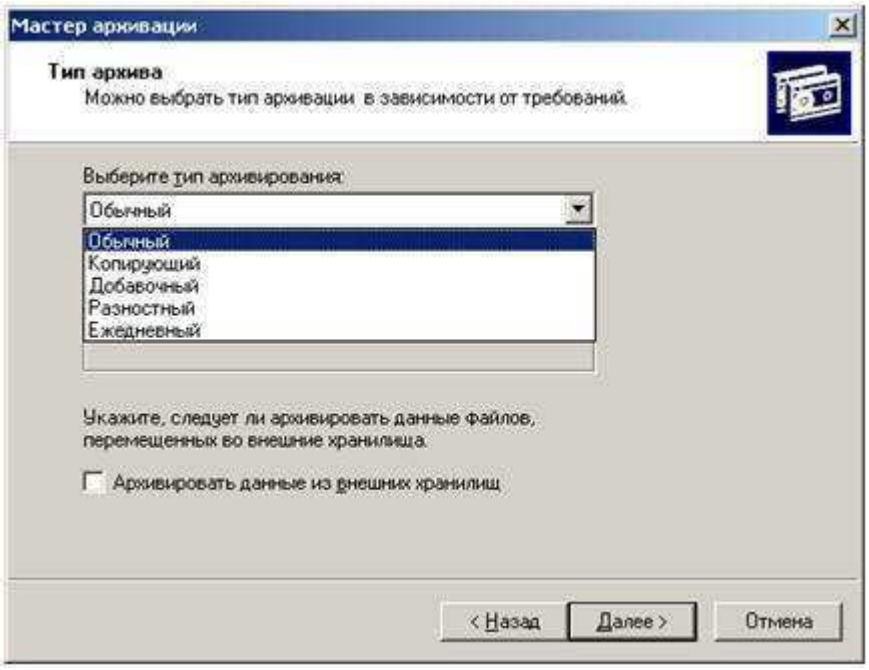


Рисунок 15. Окно "Мастер архивации". Выбор типа архивации.

На рисунок 15 представлены типы архивации: обычный, копирующий, добавочный, разностный, ежедневный. Далее предлагается выбрать время выполнения задания (рисунок 16) и параметры задания (рисунок 17).

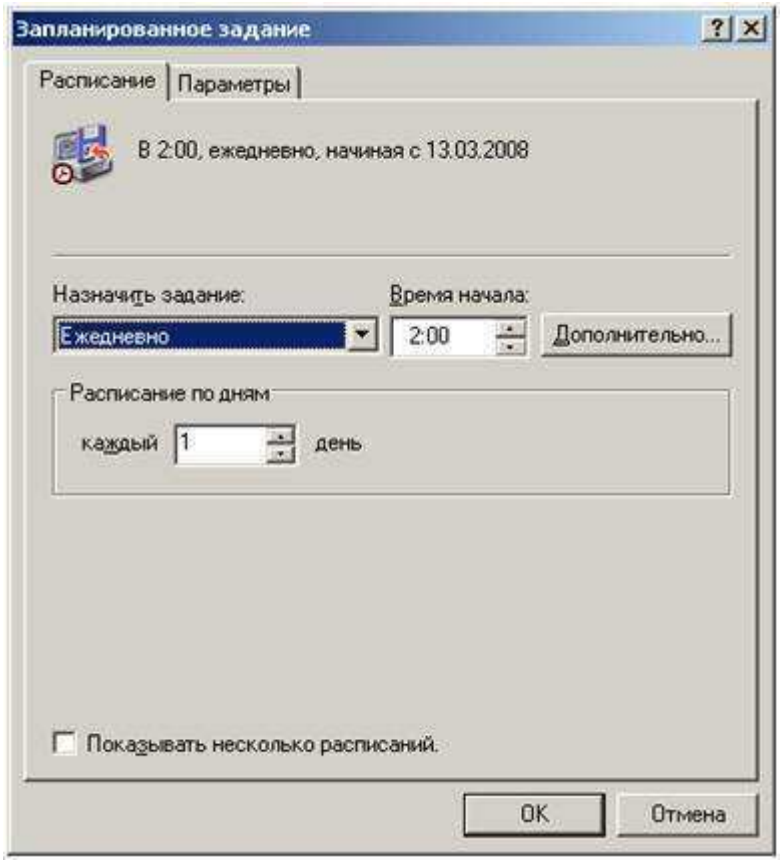


Рисунок 16. Окно "Расписание"

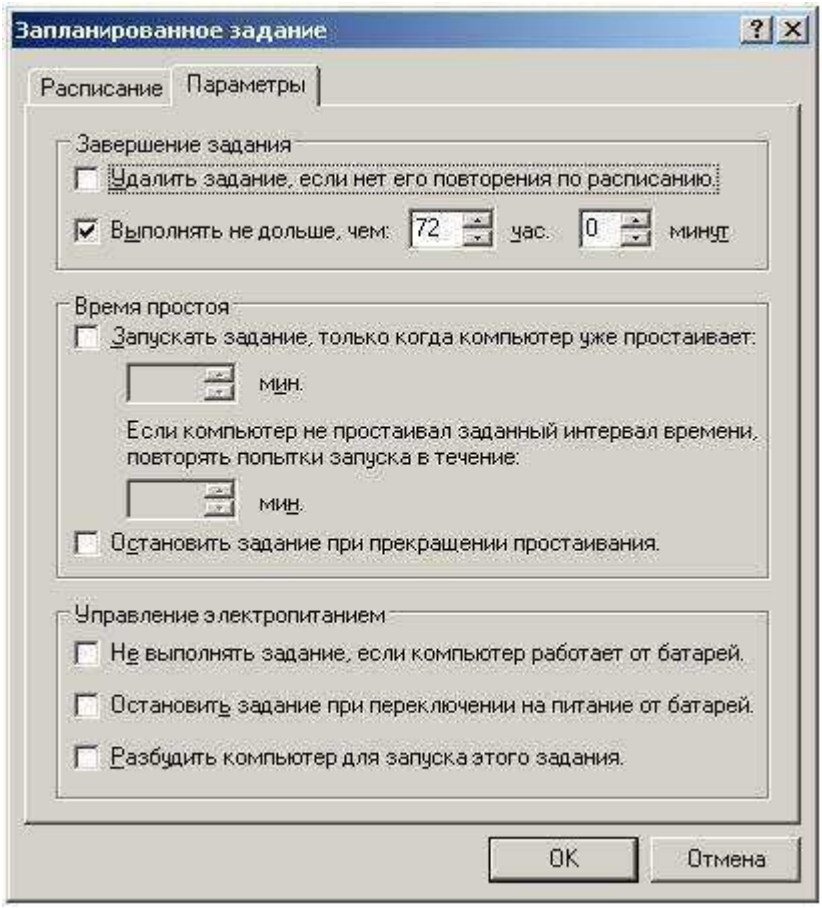


Рисунок 17. Окно "Параметры архивации"

4. Порядок выполнения работы

1. Изучить предлагаемый теоретический материал.

2. Получить следующую информацию с помощью утилиты System Information (Сведения о системе):

- свойства компьютера
- пользовательские сеансы
- список ресурсов, открытых на сервере

4. Построить отчет с максимальным объемом данных о компьютере (системе).

5. Создать план резервного копирования

6. Выполнить резервное копирование различного типа с помощью программы Backup Utility (**Start** (Пуск) - **Programs** (Программы) - **Accessories** (Стандартные) - **System Tools** (Служебные) - **Backup** (Архивация данных)):

- Полное
- Инкрементное
- Ежедневное

7. Проанализировать журнал резервного копирования. Сделать выводы на основании анализа.

Практическое занятие № 13

Организация доступа к локальным сетям и Интернету

Цель: Рассмотреть различные варианты подключения к сети Интернет локальной сети, использующие различные программные средства.

Краткие теоретические сведенья:

Имеются три основных варианта подключения локальной сети к Интернет:

1. «прямое» IP-подключение,
2. подключение через NAT,
3. подключение через прокси-сервер.

Рассмотрим преимущества, недостатки и область применения каждого метода, а также некоторые возникающие нюансы. Выбор конкретного способа подключения зависит от потребностей пользователей, цели подключения и, в некоторой степени, финансовых возможностей.

Итак, компьютер *Workstantion 1*. У него есть доступ, как к Интернету, так и к локальной сети. Наша задача - дать компьютерам локальной сети доступ к Интернет через подключенный к нему компьютер. Далее этот компьютер мы будем называть шлюзом или маршрутизатором.

Рассмотрение способов мы начнем с наименее часто использующегося, наиболее дорогого, но также наиболее «правильного» и естественного способа, дающего наибольшие по сравнению с другими способами возможности.

«Прямое» IP-подключение к Internet. Для того, чтобы Ваша локальная сеть была полноценно подключена к Интернету, должны соблюдаться, как минимум, три условия:

1. Каждая машина в локальной сети должна иметь "реальный", интернетовский IP-адрес;
2. Эти адреса должны быть не любыми, а выделенными Вашим провайдером для Вашей локальной сети (скорее всего, это будет подсеть класса C);
3. На компьютере-шлюзе, подключенном к двум сетям - локальной сети и сети провайдера, должна быть организована IP-маршрутизация, т.е. передача пакетов из одной сети в другую.

В этом случае Ваша локальная сеть становится как бы частью Интернета. Собственно, это тот способ подключения, которым подключены к Интернету сами Интернет-провайдеры и хостинг-провайдеры.

В отличие от обычного подключения, рассчитанного на один компьютер, при таком подключении "под клиента"
выделяется не один IP-адрес, а несколько, так называемая "IP-подсеть".
При таком способе подключения Вы можете организовать в своей сети сервисы, доступные из Интернета - ведь при
данном подключении не только Интернет полностью доступен из Вашей сети, но и Ваша сеть - из Интернета, т.к.
является его частью.
Однако такая "прозрачность" Вашей сети резко снижает ее защищенность - ведь любые сервисы в локальной сети,
даже предназначенные для "внутреннего" использования, станут доступными извне через Интернет. Чтобы это не
имело места, доступ в локальную сеть извне несколько ограничивают. Обычно это делается установкой на шлюзе
программы-firewall. Это своеобразный фильтр пакетов, проходящих из одной сети в другую. Путем его настройки
можно запретить вход-выход из локальной сети пакетов, соответствующих определенным критериям - типу IP-
пакета, IP-адресу назначения, TCP/UDP-порту и т.п.
Firewall решает такие задачи, как:
· блокировку доступа извне к определенным TCP/IP-сервисам локальной сети.
· блокировку доступа к определенным компьютерам локальной сети. Таким образом, можно
запретить доступ извне ко всем машинам, кроме определенных серверов, предназначенных для
доступа из Интернет.
· защиту от троянских программ на сетевом уровне.
Несмотря на универсальность такого метода подключения локальной сети к Интернет, этот метод имеет
недостатки. Благодаря им, его реально и используют только лишь те организации, которым надо сделать свои
сервера доступными из Интернет - в основном, те же интернет-провайдеры и хостинг-провайдеры, а также
информационные службы. Самый главный недостаток заключается в дороговизне выделения IP-адресов и уж тем
более IP-подсетей, к тому же эту плату надо вносить периодически.
Поэтому на практике рассмотрим другие, описанные далее способы, не требующие больших затрат и, что самое
главное, позволяющие подключить локальную сеть через обычное подключение с одним внешним IP-адресом.

Подключение через NAT (IP-маскарадинг)

Технология Network Address Translation (NAT) - "трансляция сетевых адресов" позволяет нескольким машинам
локальной сети иметь доступ к Интернет через одно подключение и один реальный внешний IP-адрес.

Для того, чтобы компьютера локальной сети могли устанавливать соединения с серверами сети Интернет, нужно,
чтобы:

· IP-пакеты, адресованные серверу в Интернет, смогли его достигнуть;

· ответные IP-пакеты, идущие от сервера Интернет на машину в локальной сети, также смогли ее
достигнуть.

С первым условием проблем не возникает, а как быть со вторым? Ведь компьютера локальной сети не имеют
своего "реального" интернетовского IP-адреса! Как же они могут получать IP-пакеты из Интернет?!

А работает это следующим образом - на компьютере-шлюзе стоит программа NAT-сервера. Компьютер-шлюз
прописан на машинах локальной сети как "основной шлюз", и на него поступают все пакеты, идущие в Интернет (не
адресованные самой локальной сети). Перед передачей этих IP-пакетов в Интернет NAT-сервер заменяет в них IP-
адрес отправителя на свой, одновременно запоминая у себя, с какой машины локальной сети пришел этот IP-пакет.

Когда приходит ответный пакет (на адрес шлюза, конечно), NAT определяет, на какую машину локальной сети его
надо направить. Затем в полученном пакете меняется адрес получателя на адрес нужной машины, и пакет
доставляется этой машине через локальную сеть.

Как видим, работа NAT-сервера прозрачна для машин локальной сети (как и работа обычного IP-маршрутизатора).

Единственным принципиальным ограничением этого метода подключения локальной сети к Internet является
невозможность установить _входящее_ TCP-соединение из Интернет на машину локальной сети. Однако для
"клиентских" сетей этот недостаток превращается в достоинство, резко увеличивающее (по сравнению с первым
методом подключения) их защищенность и безопасность. Администраторы некоторых провайдеров даже
употребляют слова NAT и Firewall как синонимы.

Подключение через прокси-сервер
Это самый простой тип подключения. При этом никакой маршрутизации IP-пакетов между локальной сетью и сетью
Интернет не происходит. Машины локальной сети работают с Интернет через программу-посредник, так
называемый прокси-сервер, установленный на компьютере-шлюзе.
Основной особенностью этого метода является его "непрозрачность". Если, скажем, в случае NAT программа-
клиент просто обращается к Интернет-серверу, не "задумываясь", в какой сети и через какую маршрутизацию она работает, то в случае работы через прокси-сервер программа должна явно обращаться к прокси-серверу. Мало
того, клиентская программа должна уметь работать через прокси-сервер. Однако проблем с этим не возникает -
все современные и не очень броузеры умеют работать через прокси-сервера.
Другой особенностью является то, что прокси-сервер работает на более высоком уровне, чем, скажем, NAT. Здесь
уже обмен с Internet идет не на уровне маршрутизации пакетов, а на уровне работы по конктретным прикладным
протоколам (HTTP, FTP, POP3...). Соответственно для каждого протокола, по которым должны "уметь" работать
машины локальной сети, на шлюзе должен работать свой прокси-сервер.
Эта "протокольная зависимость" и есть основной недостаток этого метода подключения как самостоятельного.
Однако, с другой стороны, "маршрутизация" на таком высоком уровне может дать и немалые преимущества.
Почти каждый интернет-провайдер имеет один или несколько прокси- серверов, через которые рекомендует
работать своим клиентам. Несмотря на то, что это совершенно необязательно (как правило, клиент провайдера
может обращаться к Интернет напрямую), это дает выигрыш в производительности, а при повременной оплате,
соответственно, экономить время он-лайн. Это происходит потому, что прокси-сервера способны кэшировать
(запоминать) запрашиваемые пользователем документы, и при следующих к ним обращениях выдавать копию из
кэша, что быстрее, чем повторно запрашивать с интернет-сервера. Кроме того, прокси-сервера могут быть
настроены так, что будут блокировать загрузку баннеров наиболее распространенных баннерных служб, тем
самым также (порой значительно) ускоряя загрузку веб-страниц.

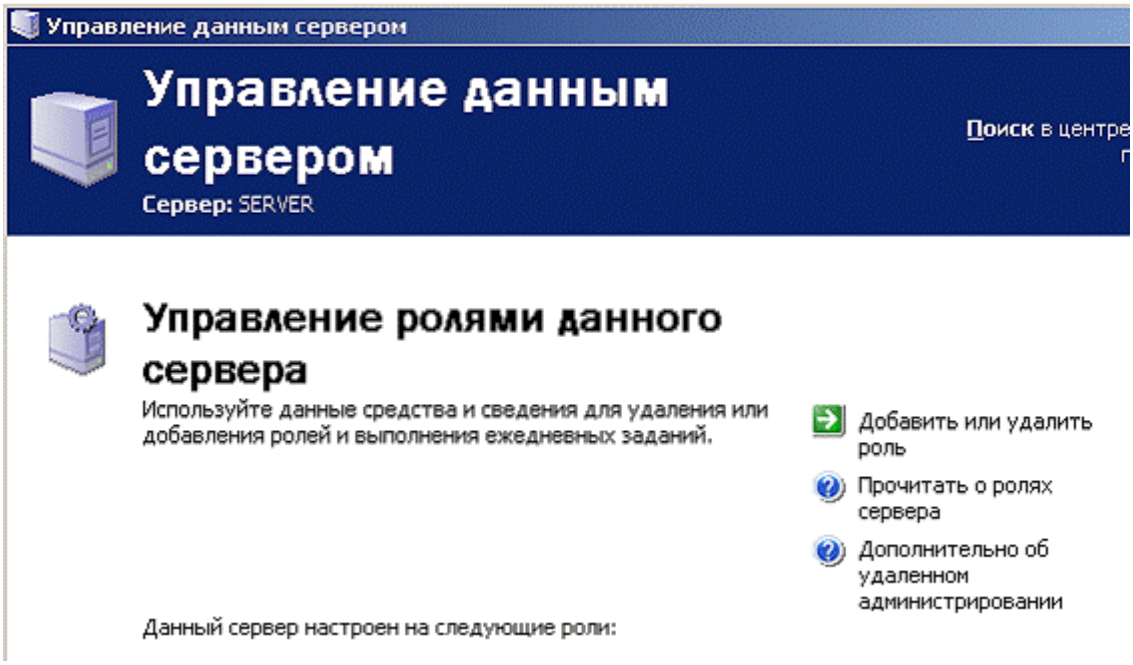
При установке HTTP прокси сервера в локальной сети и работе через него за счет кэширования экономится не
только время, но и трафик - потому, что кэширование происходит в самой локальной сети, "до" канала с
провайдером, в котором считается трафик (при оплате за объем перекачанной информации).

Ход работы:

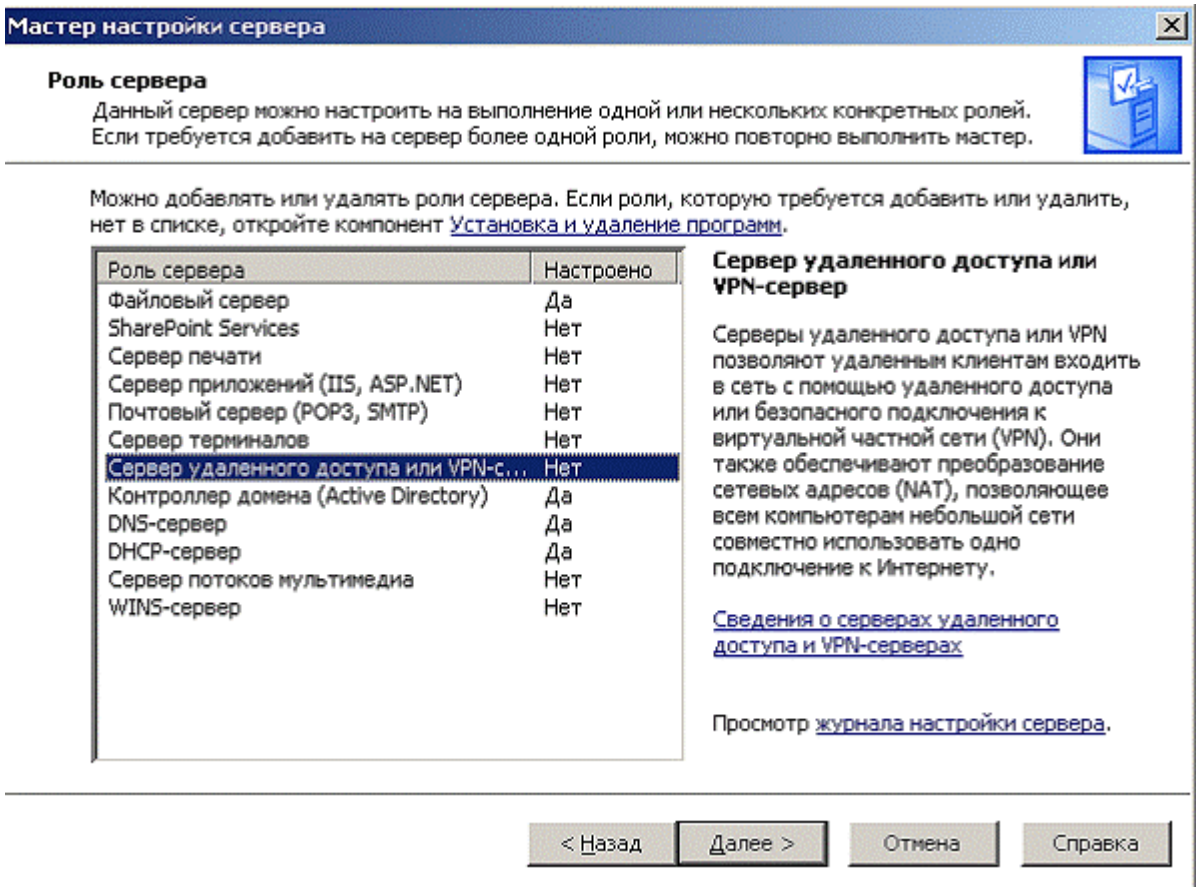
Настройка подключения через Win2003 Server. NAT

Для создания условий, заданных в лабораторной работе, необходимо выполнить ряд действий:

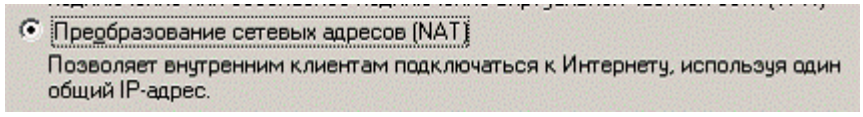
1. Выключаем виртуальную машину с Linux. Удаляем ее из нашей группы.
2. Добавляем Win2003 Server и добавляем сетевой адаптер, который подключаем по схеме
«NAT». Второй подключаем к «LAN1»
3. После загрузки Win2003 Server настраиваем новый сетевой адаптер на автоматическое
получение IP- адреса.
4. Проверяем доступ к Интернет.
5. Запустите режим управления сервером.



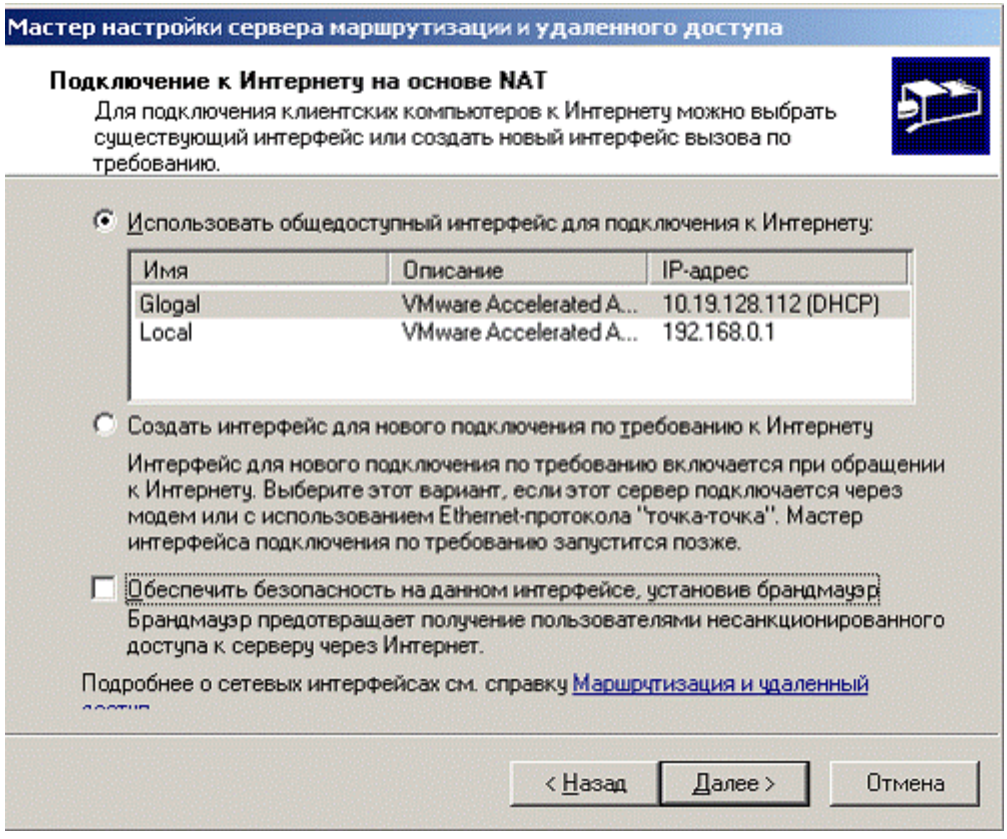
6. Выберите добавить новую роль.
7. В списке ролей выберите следующий пункт.



8. Выберите вариант «NAT»

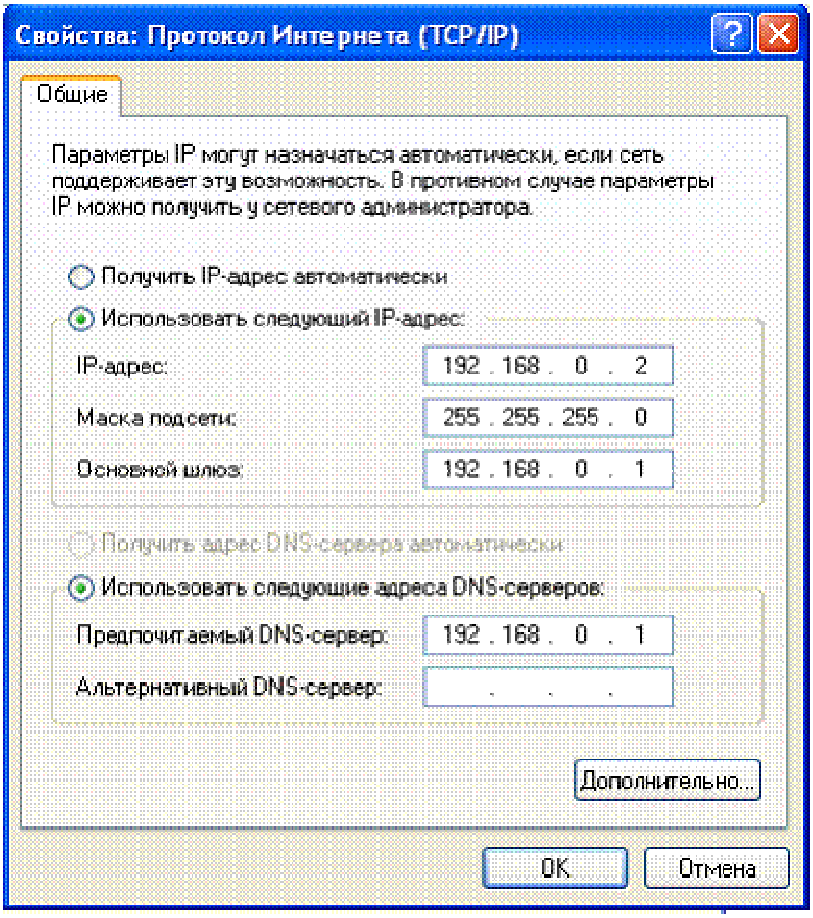


9. Выберите интерфейс подключенный к Интернет



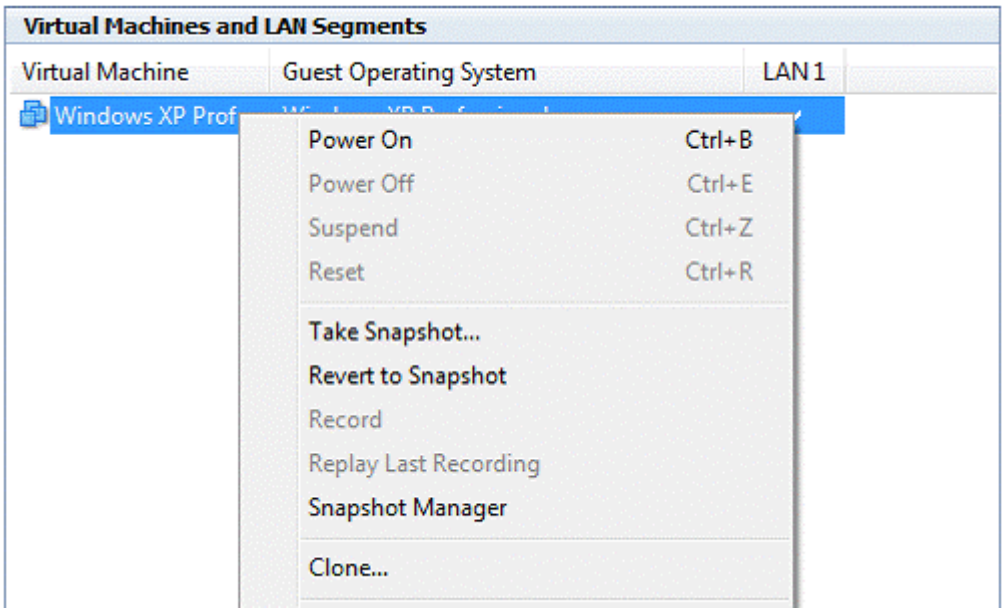
10. Отключите брандмауэр

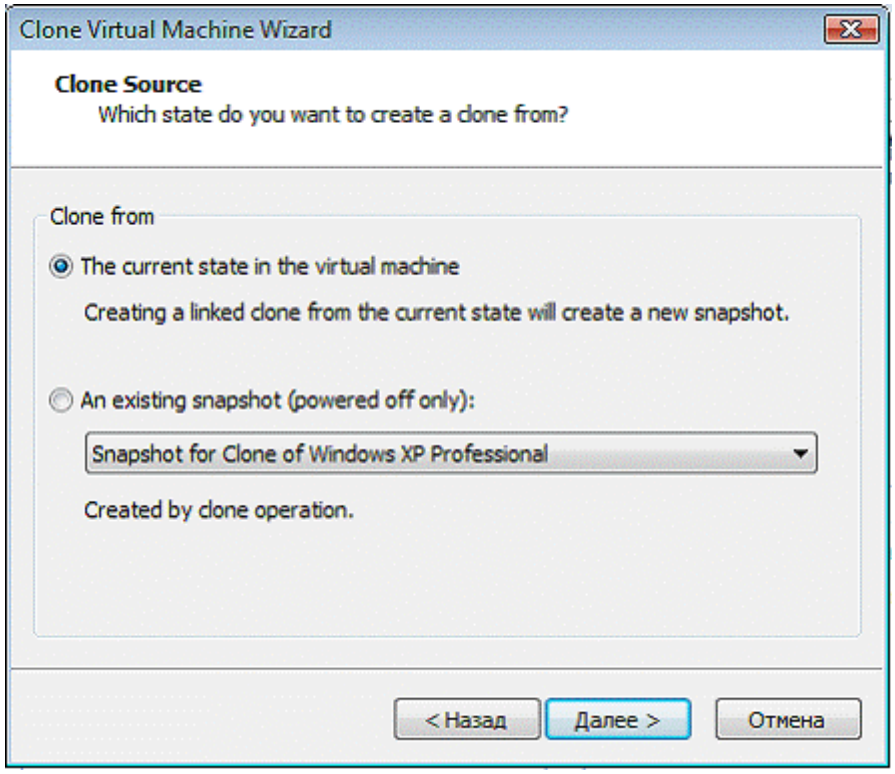
11. Введите следующие параметры на клиентской машине

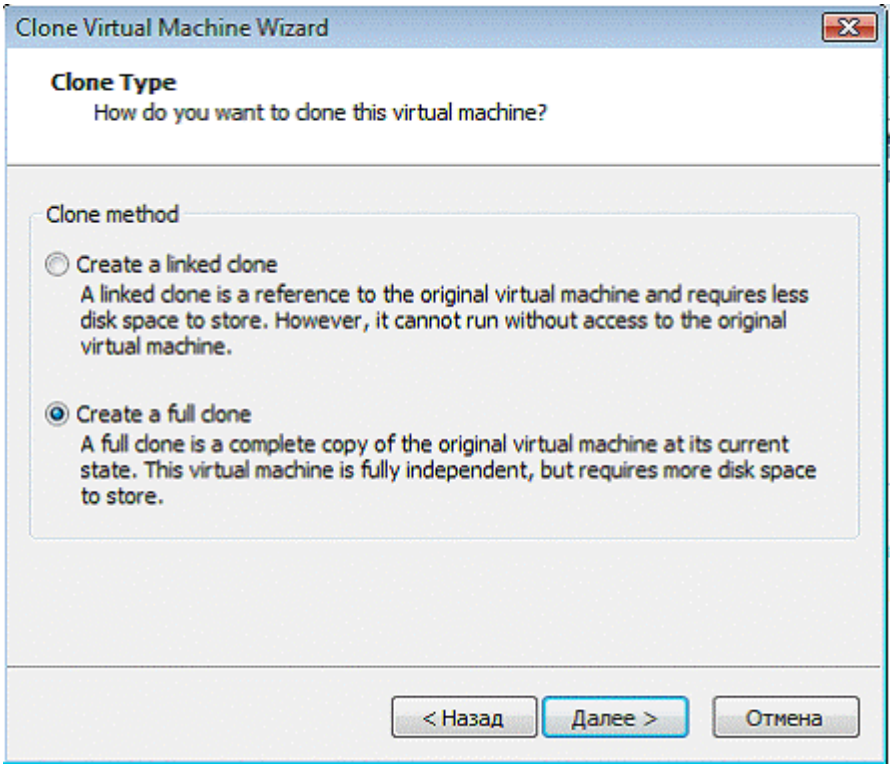


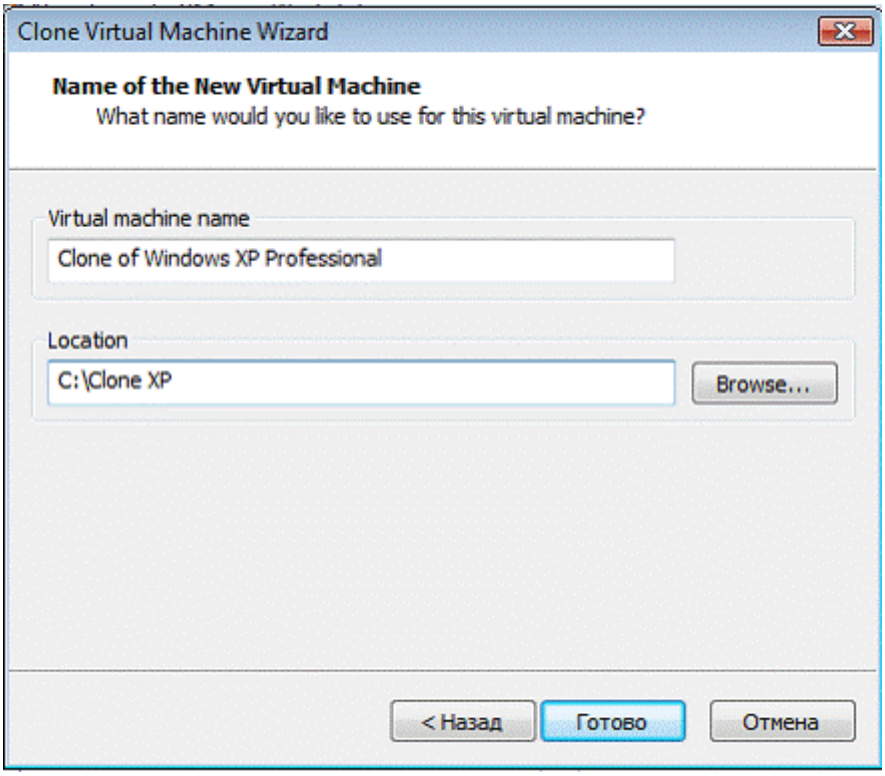
Проверьте работоспособность NAT при помощи команд (с клиентской машины):
ping 192.168.0.1
ping [адрес адаптера сервера, подключенного к Интернет]
Настройка подключения через WinXP. Internet Connection Sharing.
Для выполнения следующих двух этапов необходимо проделать следующие действия:
Выключите Win2003 Server и удалите его из Вашей группы.
Создайте клон WinXP.

Выполняйте действия согласно рисункам



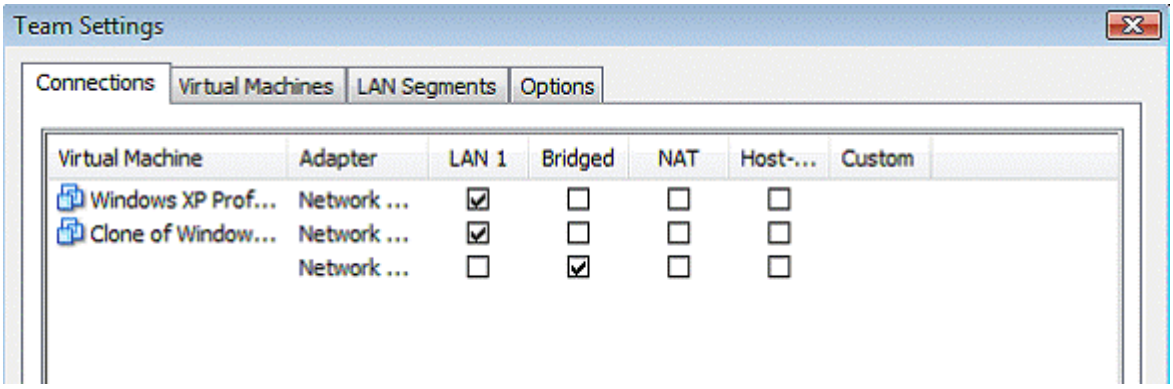






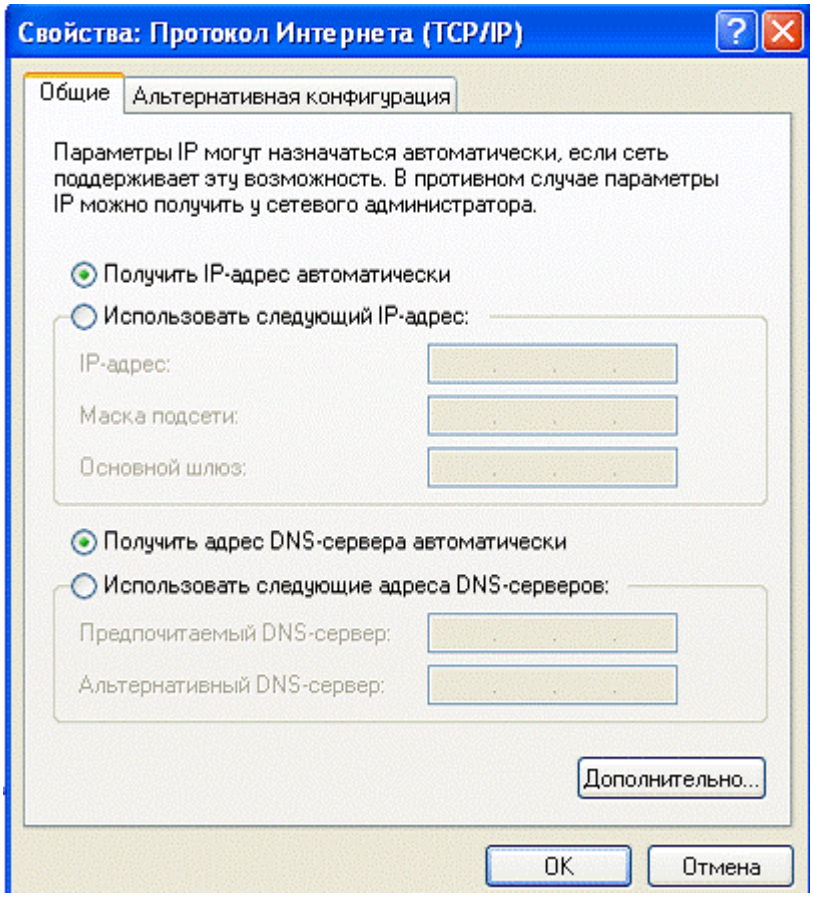
Добавьте новую ОС в группу

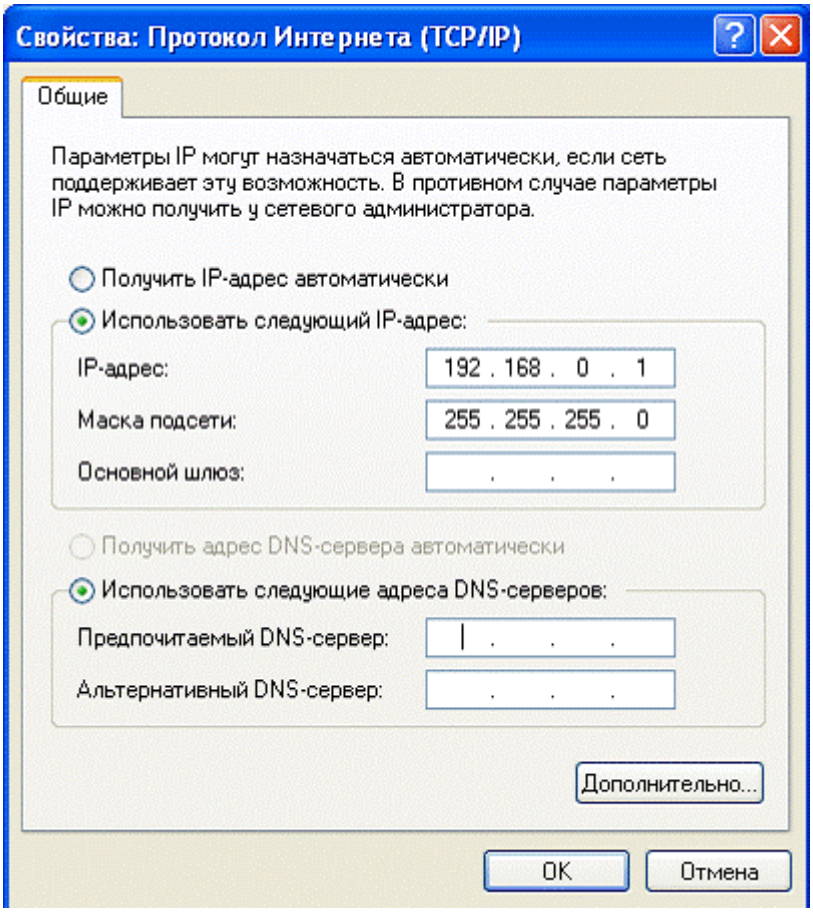
Добавить сетевой адаптер, как показано на рисунке



Запустить виртуальные машины

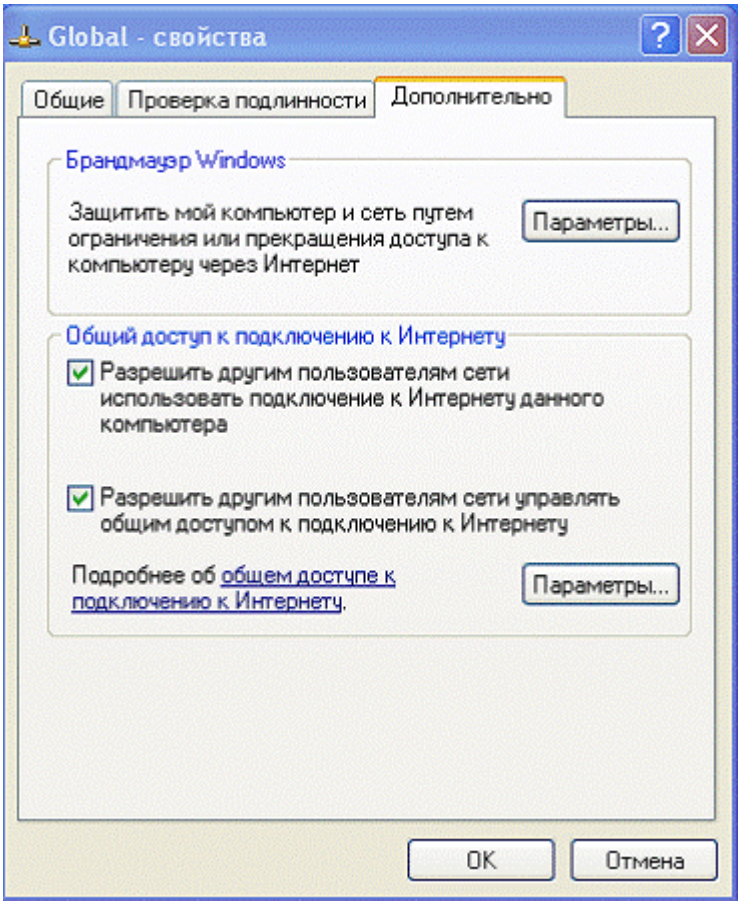
Настройте на шлюзе адаптеры, как показано на рисунке



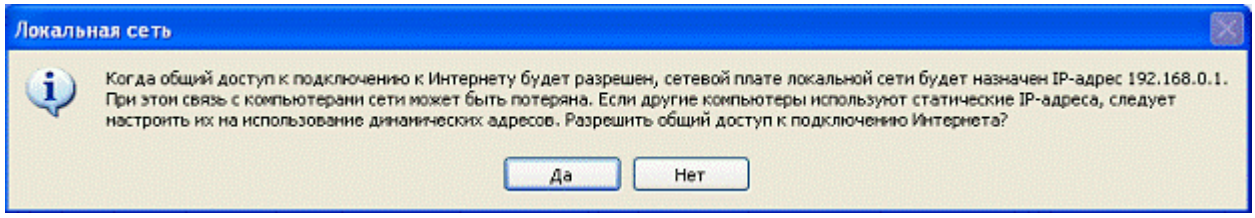


Для удобства переименуйте их

На шлюзе, открываем *Панель управления > Сеть и удаленный доступ к сети (Control Panel > Network Connections)*,
выберите ваше подключение правой кнопкой и нажмите *Свойства (Properties)*.
В закладке *Дополнительно*
(Advanced) отметьте флажок *Общий доступ в моей сети для этого подключения (Allow Other Network Users To*
Connect Thought This Computer's Internet Connection).



ICS жестко сконфигурирован и назначает компьютеру, обеспечивающему доступ, статический внутренний
адрес 192.168.0.1. Все клиенты размещаются в одной физической подсети, получают адреса из диапазона
192.168.0.0/24 (/24 означает первые 24 единицы в маске сети, представленной в двоичной форме, т.е. это маска
255.255.255.0) и используют для разрешения имен только DNS-сервер, размещенный на этом же компьютере.



На клиентских машинах устанавливаем Автоматическое получение IP-адреса.
Настройка подключения через WinXP. Прокси-сервер
На первом этапе необходимо установить прокси сервер на компьютере подключенном к сети Интернет.
Используйт флешку для переноса программы.

Практическое занятие № 14

Установка и сопровождение сетевых сервисов

Цель: изучить особенности настройки различных сетевых служб, облегчающих администрирование ЛВС, а так же возможности управления доступом к внешним сетевым ресурсам на примере программного комплекса Winroute.

DNS-сервер

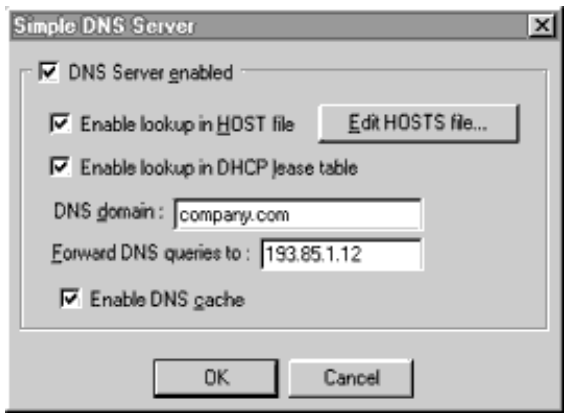
Каждый компьютер, подключенный к Интернет, идентифицируется уникальным числовым IP-адресом. Для установки соединения между двумя компьютерами через Интернет, первый должен знать IP-адрес второго. Поскольку IP–адреса неудобны для запоминания, была создана Служба доменных Имен (Domain Name Service — DNS). 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 ниже:



- "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.

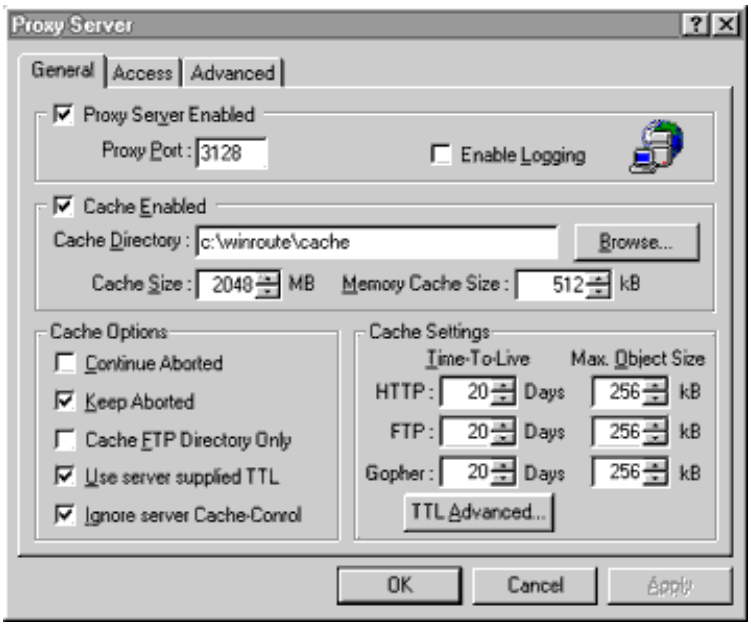
Управление доступом

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)



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.

Время жизни

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)

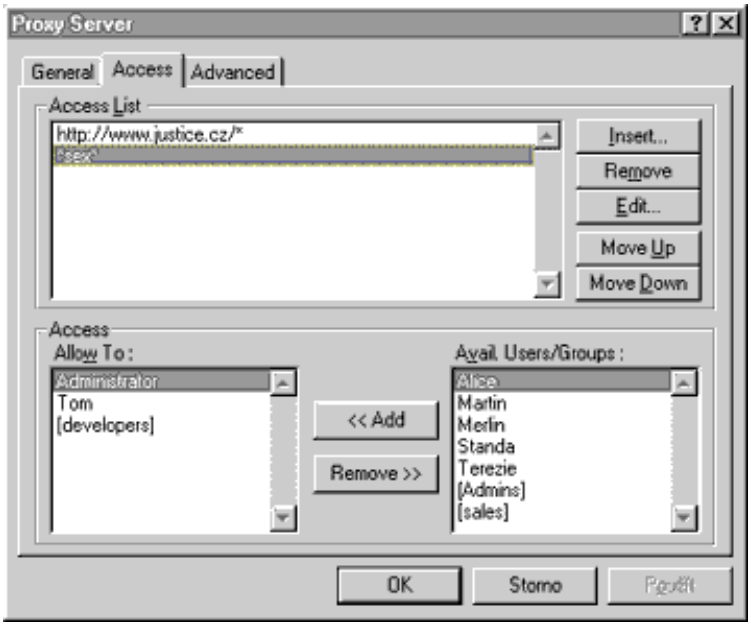
Вы можете установить время жизни объекта, исходя из его URL. Определения URL могут включать умолчания (*).

Примеры: *www*, ftp://*.zip

Максимальный размер объекта

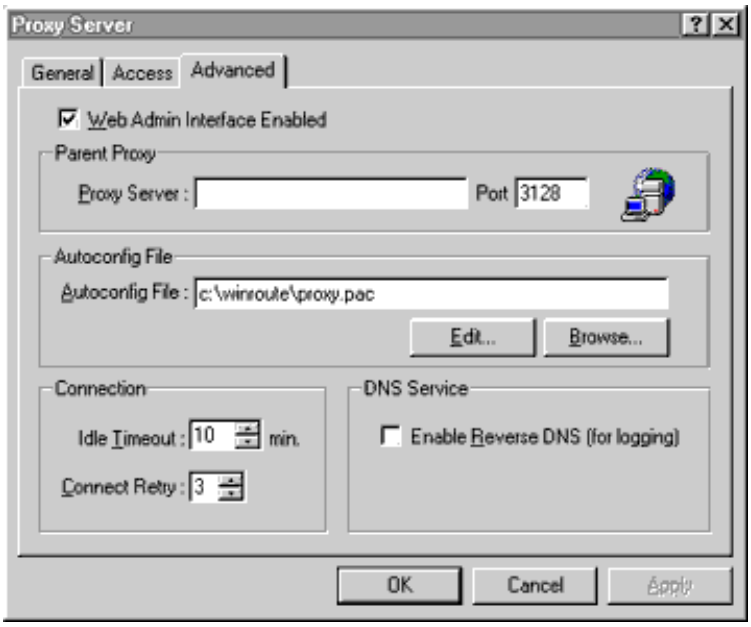
Все объекты, размер которых превосходит это значение, не будут записываться в кэш.

Доступ



Закладка "Доступ" описывается в пункте Access Control (Управление доступом)

Сложные настройки



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 на иллюстрации:

Access List	**users/groups**
*	boss
./	[users]
./	[users]

2. Чтобы полностью закрыть доступ к домену **:**

Access List	**users/groups**
./	

Примечание: невозможно заблокировать доступ членам группы **[Admins]** куда-либо.

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 Интернет 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:

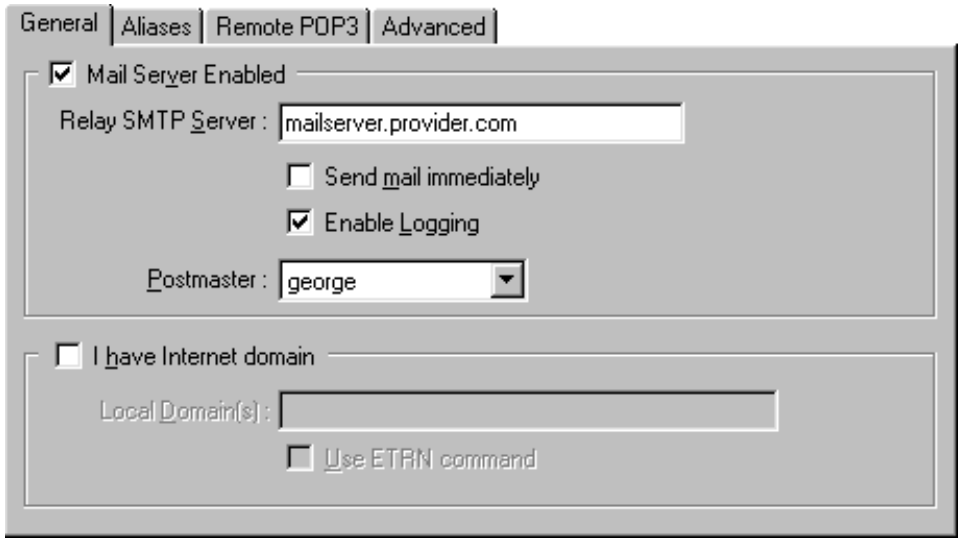
- почта получена из Интернет через SNTP (от пользовательского почтового клиента или из Интернет)
- перед загрузкой в почтовый ящик почты с удаленного ящика POP3

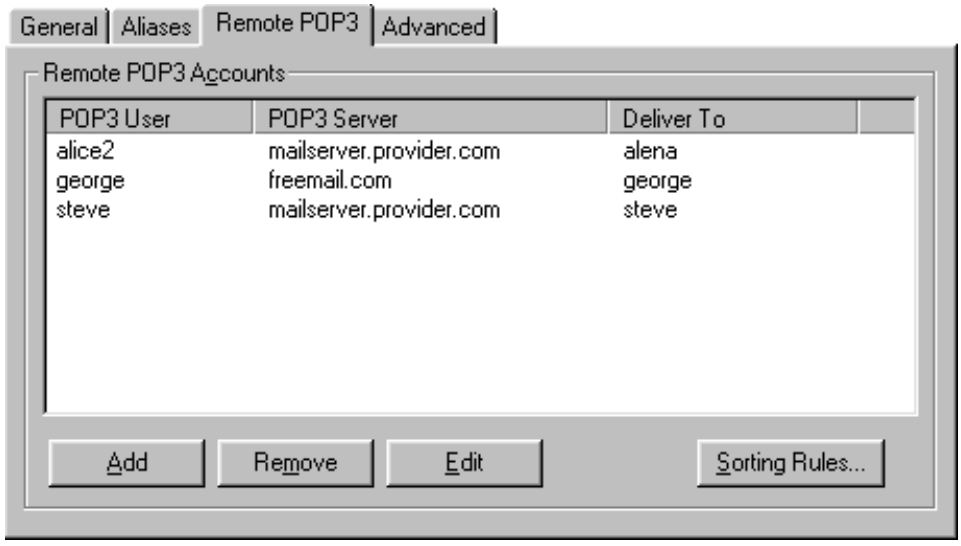
Алиасы устанавливаются в закладке "Aliases".

Почтовый сервер (Примеры)

Получение почты с удаленного почтового ящика POP3

Каждый пользователь имеет эккаунт у провайдера. Для исходящей почты используется почтовый сервер провайдера .





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.

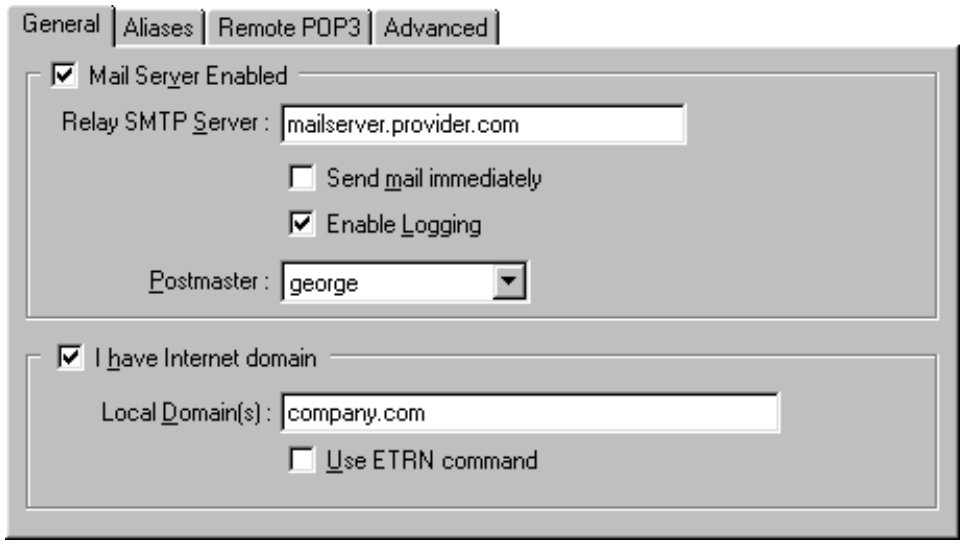
Получение почты из почтового ящика домена

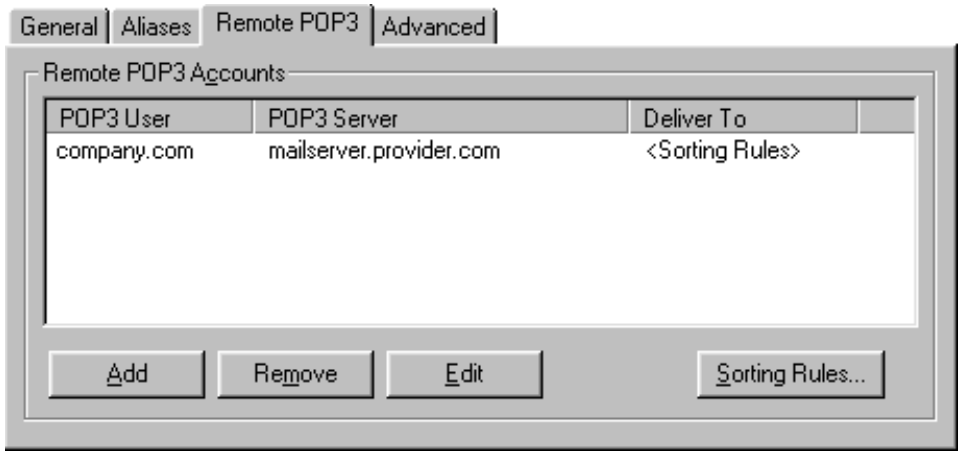
Рассмотрим случай с компанией, в которой 5 работников. У каждого есть учетная запись в WinRoute. Записи следующие: alice, george, jane, martin и tom.

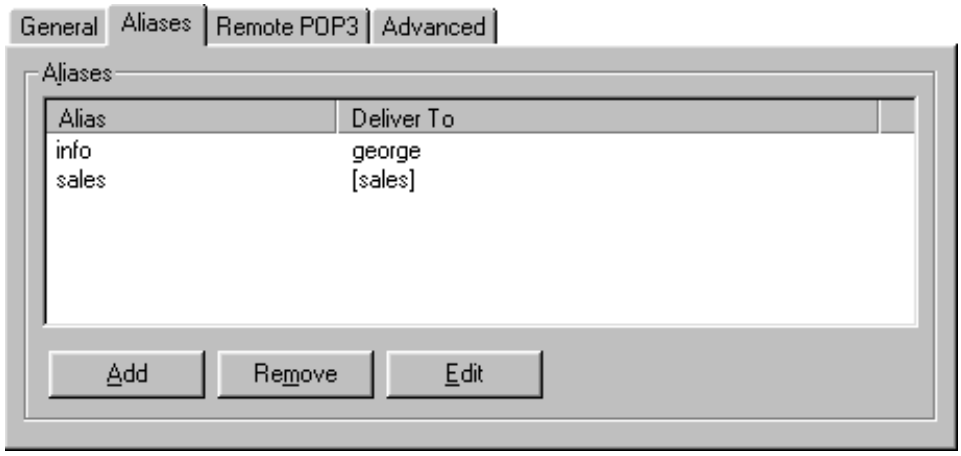
Компания имеет домен и провайдер всю почту для этого домена хранит в ящике company на свем почтовом сервере . Для исходящей почты используется тот же сервер.

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 .







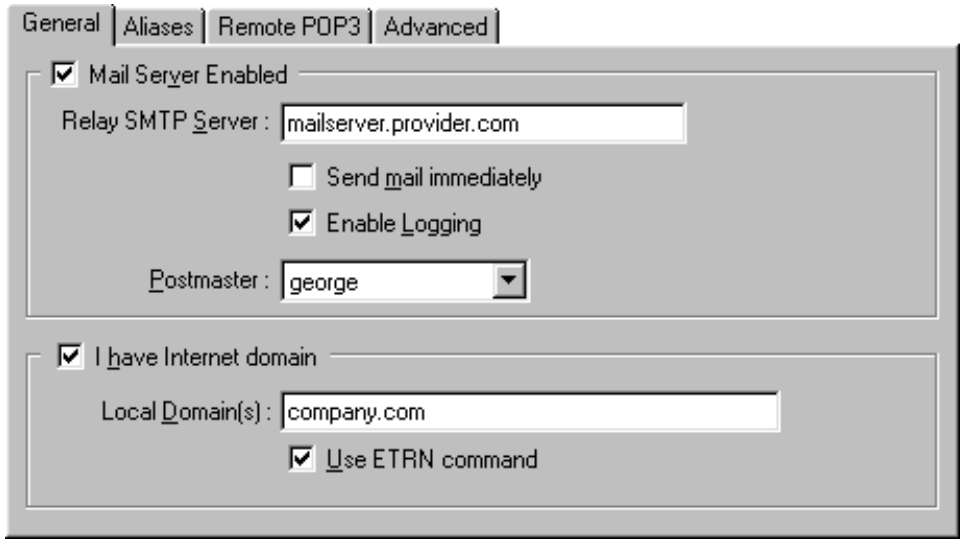
Доменная почтовая служба SMTP

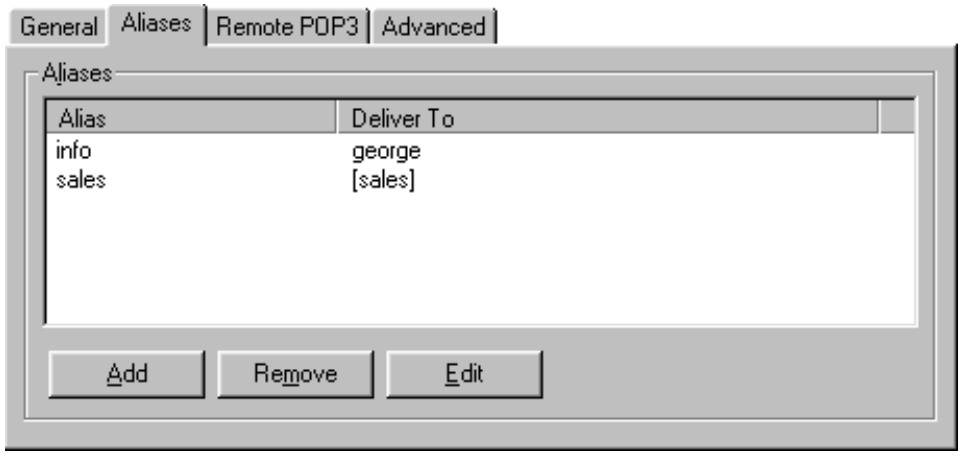
Случай с той же компанией: 5 пользователей, у каждого есть учетная запись WinRoute. Записи следующие: alice, george, jane, martin и tom.

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).





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.

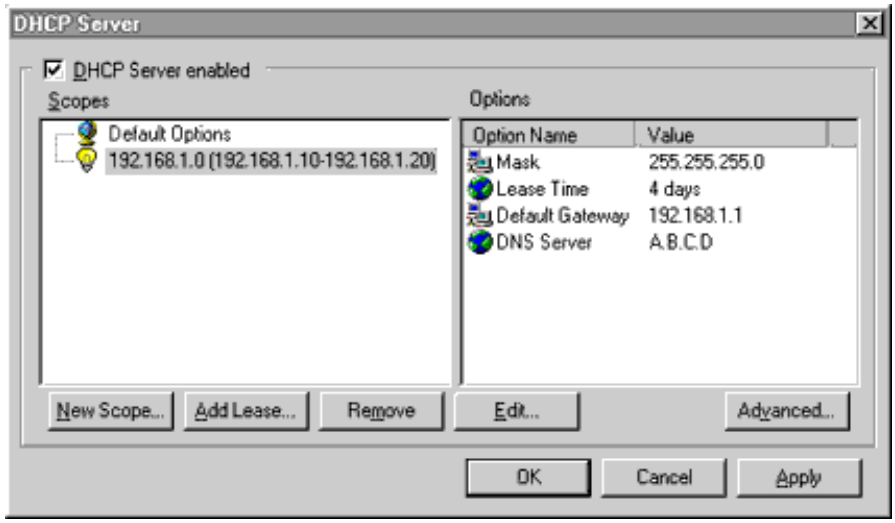
Настройка DHCP-сервера

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.



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:

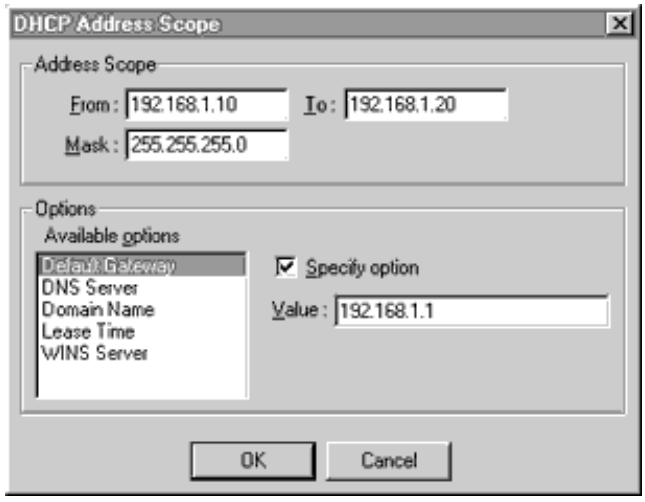
– для интервала определен параметры

– 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:



"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:

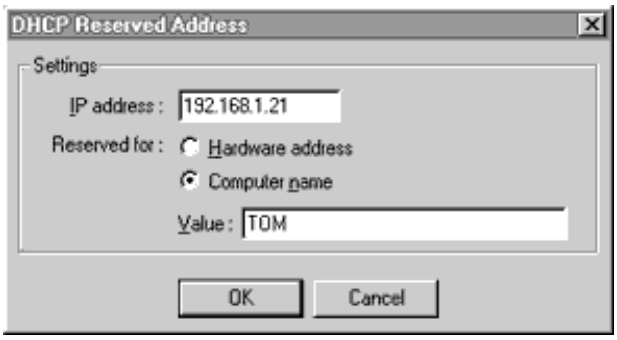
- "Default Gateway" Адрес шлюза по умолчанию. Шлюз обслуживает коммуникацию со станциями в других подсетях.
- "DNS Server" IP-адрес DNS-сервера.

- "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:



- "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

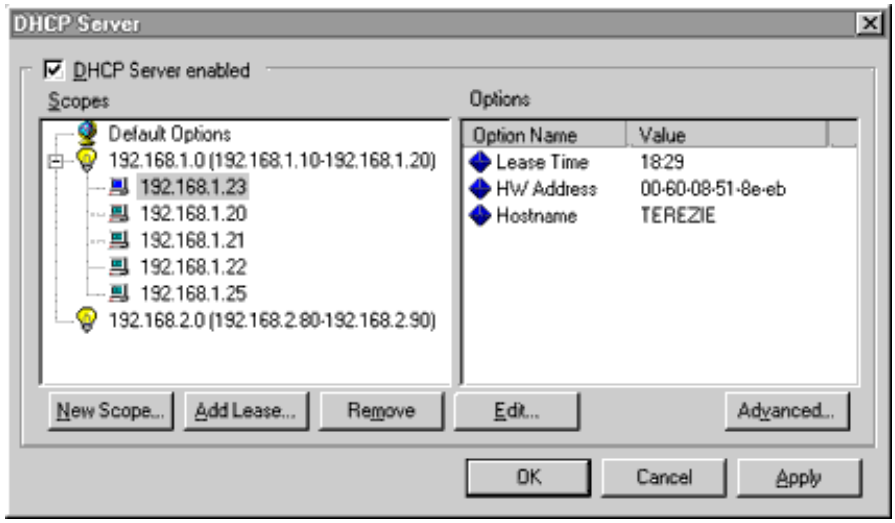
Чтобы использовать сервер DHCP в сети с несколькими сегментами, вам нужно настроить шлюзы в вашей сети так, чтобы они пересылали запросы DHCP на сегмент, к которому подключен DHCP-сервер. Примеры настроек для некоторых типов роутеров показаны ниже:

- 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:



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)

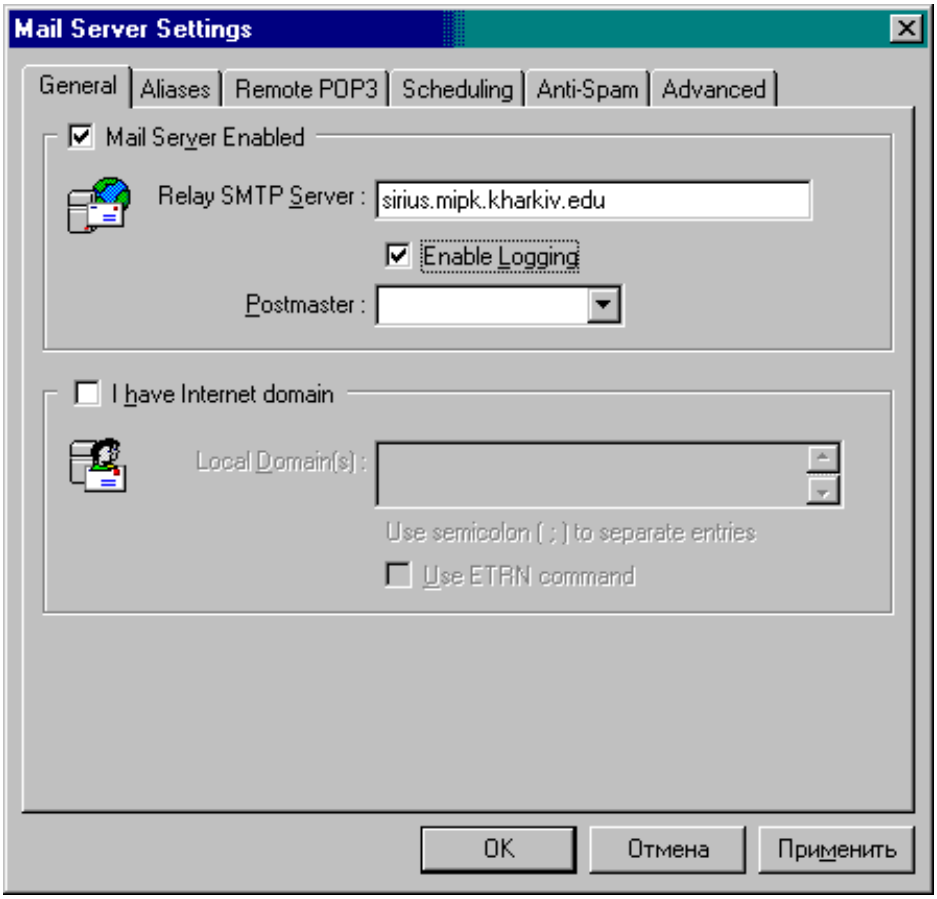
4.4. Выполнить п.4.2. предварительно проверив корректность настроек Proxy в броузерах на других машинах сети (обратить внимание на закладку “Дополнительно”). При корректной настройке фильтрация запросов будет происходить последовательно — Winroute Proxy, внешний Proxy–сервер, о чем можно судить по автоматически 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,

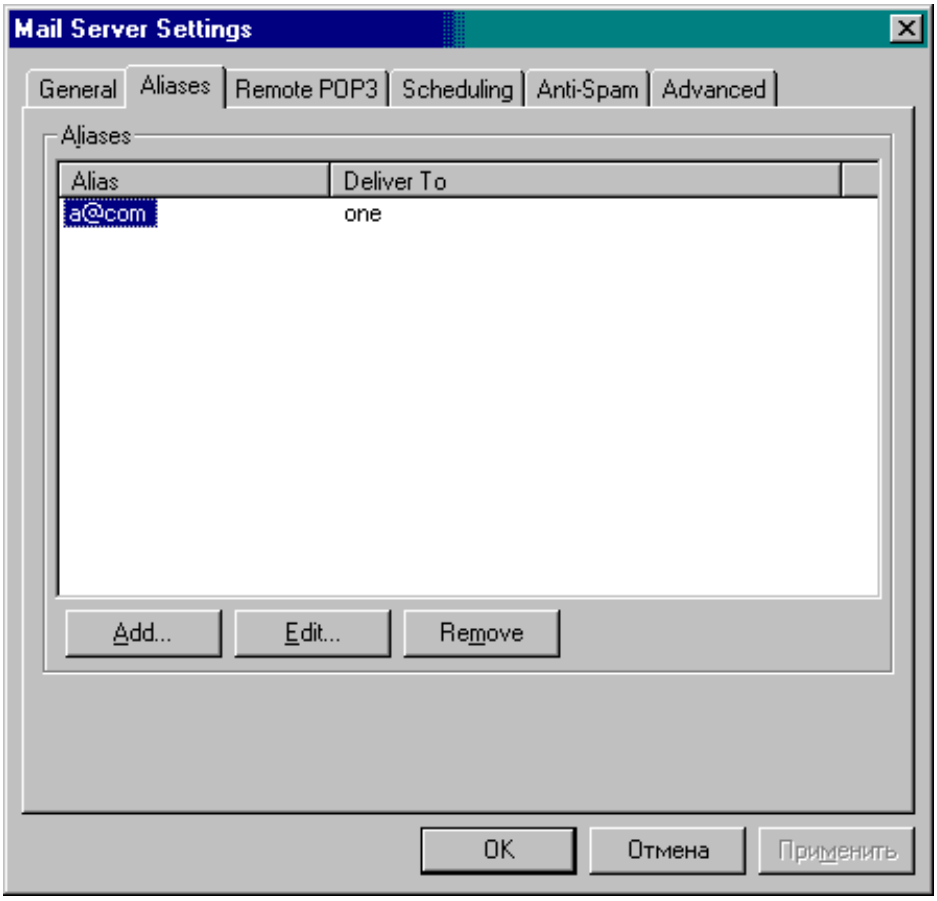
несмотря на то что в настройках прокси набираемый адрес добавлен в список разрешенных.

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)

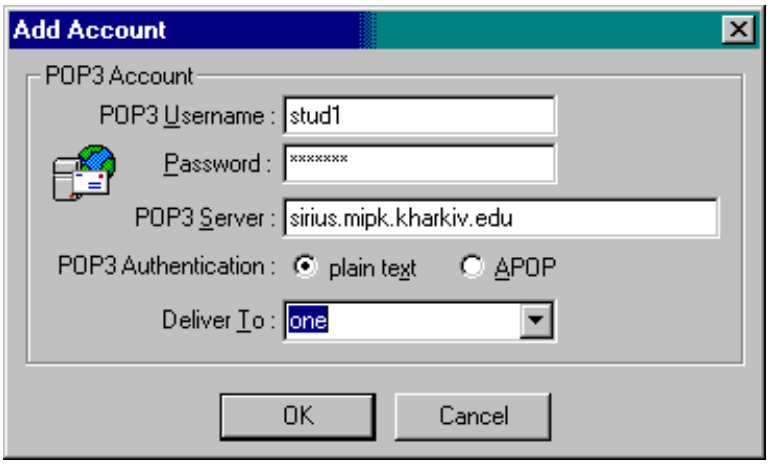
5.1. Указать внешний SMTP server



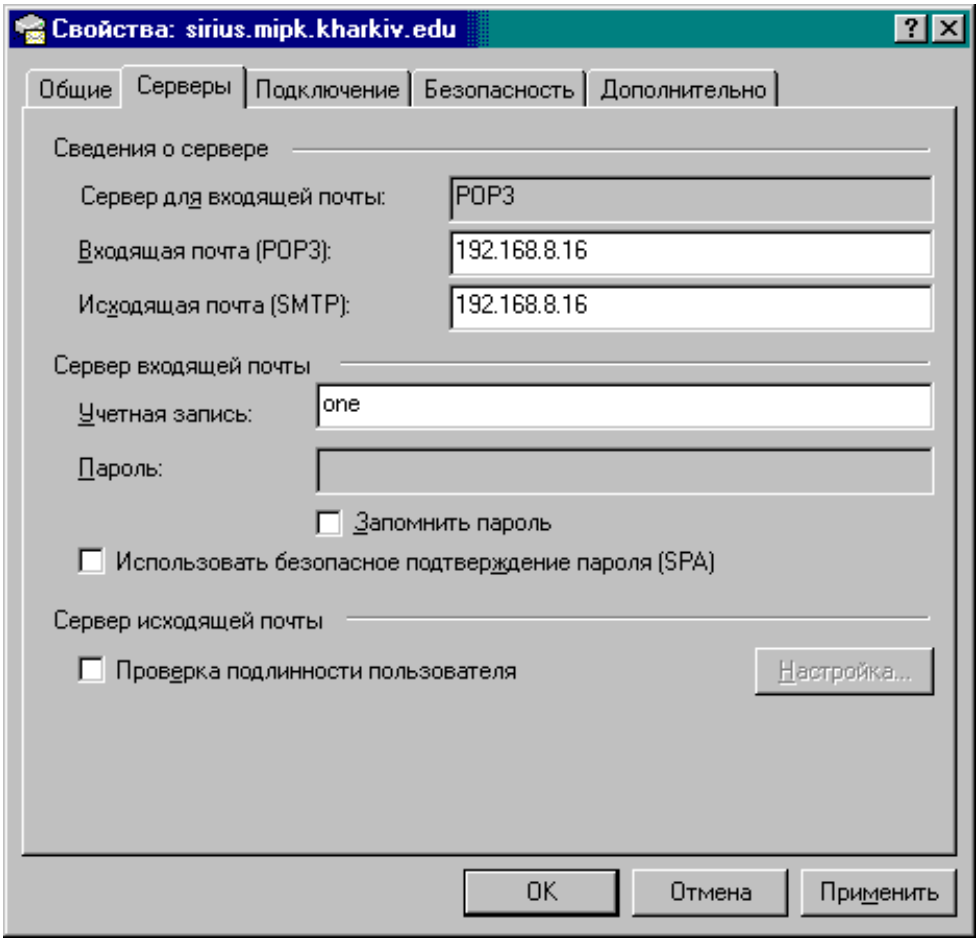
5.2. Добавить алиасы



5.3. Настроить удаленный POP3 сервер



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



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.

Практическое занятие № 15

Планирование решения резервного копирования

Цель: изучить возможности программного обеспечения резервного копирования.

1. При подготовке к выполнению лабораторной работы:
   создать на одном из дисков папку (каталог) d:\backups
2. Создать образ системы средствами Архивации и восстановления ОС Windows 7.
   1. Создать папку (подкаталог) d:\backups\ms;
   2. Запустить средство Архивации и Восстановления
   3. Создаем образ системы в папке (подкаталоге) d:\backups\ms
   4. Отказываемся от создания Диска восстановления.
3. Знакомимся с командой robocopy. Запустить интерпретатор командной строки cmd.
   1. В режиме командной строки создать папку (подкаталог) d:\backups\rc;
   2. Сделать в созданной папке зеркальную копию папки %Homepath%\Documents
   3. Создать командный (.cmd / .bat) файл для создания копии папки %Homepath%\Documents, при этом
      1. копировать только файлы с атрибутом "Архивный" и сбрасывать атрибут;
      2. указать 10 повторных попыток;
      3. указать подробный вывод в журнал с указанием пропущенных файлов;
      4. Перейти в панель управления — администрирование — запустить планировщик задач и создать новую задачу. Присвоить ей имя, установить в триггерах "время" интервал запуска задачи; в "действиях" указать запуск нашего файла xxxxxx.bat или xxxxxx.cmd
      5. вставить скриншоты
      6. вставить содержимое командного файла
4. Загрузить из сети Интернет любую программу резервного копирования, способную работать в режиме portable. Если не подобрали программу - установить Cobian Backup 11 Gravity в режиме приложения (без автозапуска).
   1. Создать папку (подкаталог) d:\backups\any;

2. Установить программу
3. В оконном режиме ознакомиться с функциями и опциями указанной программы
    1. Сделать в созданной папке полную копию папки %Homepath%\Documents
    2. указать действия или кнопки создания копии
    3. (вставить скриншоты)
5. Удалить ранее установленные программы. Удалить папку d:\backups

Практическое занятие

Анализ неполадок среды передачи данных

Цель: Ознакомится с процедурами поиска и устранения неполадок среды передачи данных.

Процедура поиска и устранения неполадок

Процесс поиска и устранения неполадок занимает значительное время в работе сетевых администраторов и технического персонала. Благодаря применению эффективных методов устранения неполадок общую длительность данного процесса удаётся сократить (если работы выполняются в производственной среде). Процесс поиска и устранения неполадок можно разбить на три основных этапа:

Этап 1. Сбор информации о симптомах — процесс поиска и устранения неполадок начинается со сбора данных и документирования симптомов, информация о которых поступает из сети, оконечных систем и от пользователей. Кроме того, сетевой администратор определяет, какие сетевые устройства были затронуты и как функционирование сети изменилось по сравнению с базовыми показателями. Симптомы могут отображаться в разном виде (предупреждения из системы управления сетями, консольные сообщения и жалобы пользователей). В ходе сбора данных о симптомах важно, чтобы сетевой администратор задавал вопросы и расследовал проблему с целью локализации проблемы до более узкого круга возможных причин её появления. Например, распространяется ли проблема на одно устройство, группу устройств, подсеть или всю сеть устройств?

Этап 2. Изоляция проблемы — изоляция представляет собой процесс исключения переменных до тех пор, пока в качестве причины не будет определена одиночная проблема или набор связанных проблем. Для этого администратор сети проверяет характеристики проблем на логических уровнях сети, чтобы выбрать наиболее вероятную причину. На этом этапе сетевой администратор может собирать информацию и документировать дополнительные симптомы в зависимости от определённых характеристик проблем.

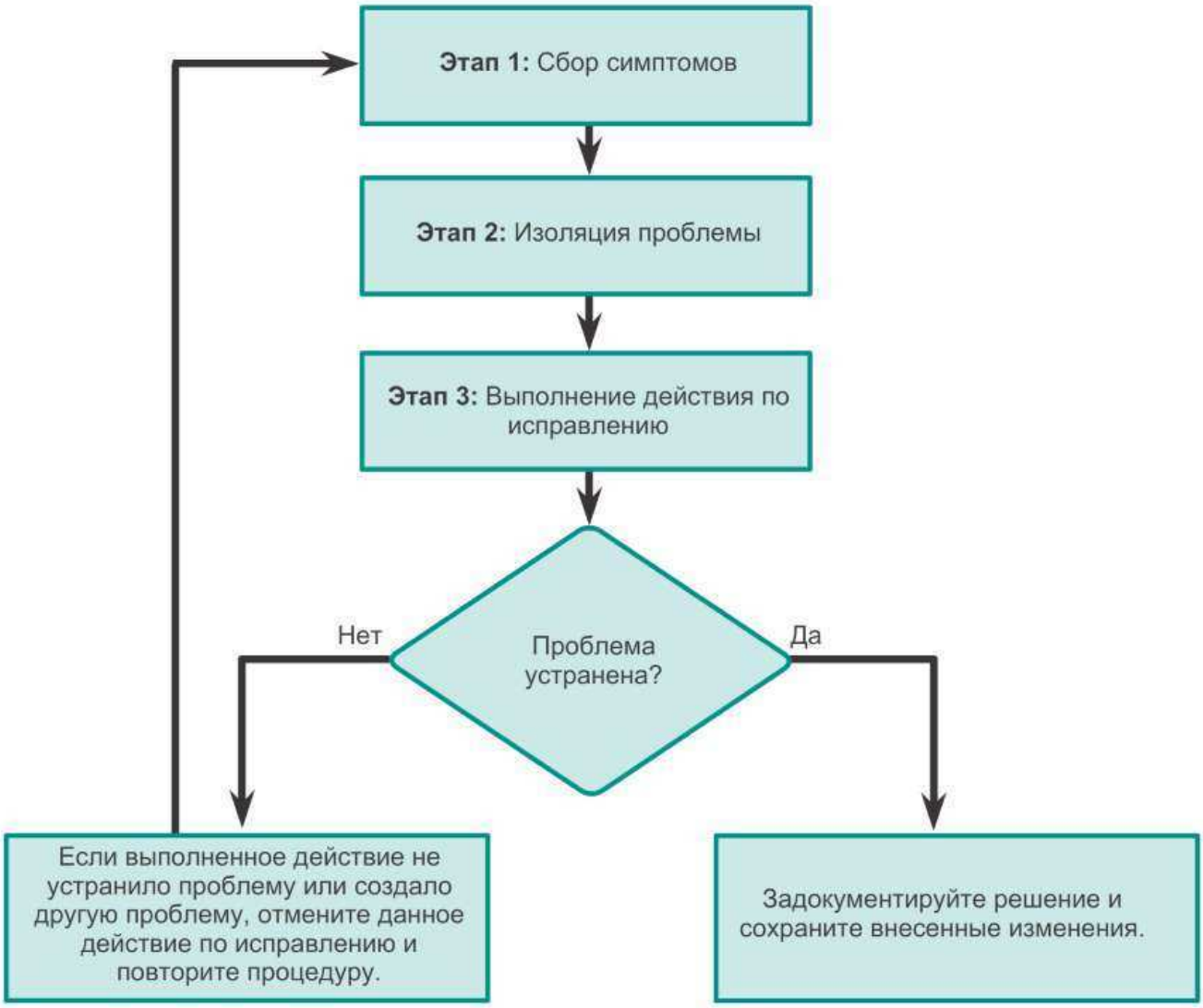
Этап 3. Выполнение исправляющего действия — после определения причины проблемы сетевой администратор пытается её устранить путём исполнения, тестирования и документирования возможных решений. После обнаружения проблемы и определения требуемого решения администратору может понадобиться решить, можно ли немедленно реализовать решение или реализацию следует отложить. Это зависит от степени влияния изменений на

пользователей и сеть. Уровень серьёзности проблемы всегда следует соотносить со степенью влияния решения. Например, если критически важный сервер или маршрутизатор необходимо выключить на длительное время, то реализацию исправления лучше отложить на конец рабочего дня. В ряде случаев до разрешения фактической проблемы можно применить обходное или временное решение. Обычно это относится к процедурам контроля изменений в сети.

Если действие по исправлению создаёт другую проблему или не устраняет существующую, то попытка решения документируется, внесенные изменения удаляются, а сетевой администратор возвращается к процедуре сбора данных о симптомах и изоляции проблемы.

Эти этапы не являются взаимоисключающими. На любом этапе процесса может возникнуть необходимость вернуться к предыдущим этапам. Например, при изоляции проблемы администратору может потребоваться сбор дополнительных симптомов. Кроме того, при попытке исправления проблемы существует риск создания другой проблемы. В этом случае следует удалить внесенные изменения и снова начать процедуру поиска и устранения неполадок.

Для каждого этапа должна быть сформирована политика устранения неполадок, включая процедуры контроля изменений. Политика позволяет организовать согласованный метод работы для каждого этапа. Среди прочего, в политике должна содержаться процедура документирования каждой важной порции информации.



Примечание. Для устранения проблем следует общаться с пользователями и любыми сотрудниками, принимающими участие в процессе поиска и устранения неполадок. Информацию о разрабатываемом решении должны получить другие сотрудники отдела ИТ. Наличие соответствующим образом оформленной документации о причине проблемы и способе её устранения позволит другим техническим специалистам предотвращать либо устранять похожие проблемы в будущем.

При сборе данных о симптомах важно, чтобы администратор собирал фактическую информацию и доказательства наличия проблем. Это позволит последовательно устранять возможные причины проблем и, в конечном счёте, определять первопричину самих проблем. Путём анализа информации администратор сети формулирует гипотезу, чтобы предложить возможные причины и решения и одновременно исключить появление других проблем.

Процесс сбора информации состоит из следующих пяти шагов.

Шаг 1. Сбор информации — получение информации из заявок на устранение отказов, от пользователей или из оконечных систем, на которые воздействует проблема, с целью формирования определения данной проблемы.

Шаг 2. Определение ответственности— если проблема относится к области контроля организации, перейдите к следующему этапу. Если проблема выходит за границы области контроля организации (например потеря связи через Интернет за пределами автономной системы), обратитесь к администратору внешней системы до сбора информации о других симптомах.

Шаг 3. Уточнение (сужение) области — определите, на каком уровне сети существует проблема: на уровне ядра, распределения или доступа. На идентифицированном уровне проанализируйте существующие симптомы и используйте топологию сети, чтобы определить, какое оборудование является наиболее вероятной причиной проблемы.

Шаг 4. Сбор данных о симптомах из предположительно неисправных устройств — соберите информацию о симптомах аппаратных и программных ошибок из предположительно неисправных устройств с помощью многоуровневого подхода по поиску и устранению неполадок. Начните с наиболее вероятного неисправного элемента и, используя весь свой опыт и знания, попытайтесь определить источник неполадки — отказ оборудования или ошибка в настройке программного обеспечения.

Шаг 5. Документирование симптомов— иногда проблему можно устранить с помощью задокументированной информации о симптомах. Если это невозможно, перейдите к этапу изоляции в рамках общего процесса поиска и устранения неполадок.

Для сбора данных о симптомах сетевых проблем используйте следующие команды ОС IOS Cisco и другие средства, например:

- **команды ping** , **traceroute** и**telnet**;
- **команды show** и **debug**;
- перехваченные пакеты;
- журналы устройств.

В таблице на рисунке указаны наиболее распространенные команды ОС IOS Cisco, используемые для сбора данных о симптомах сетевых проблем.

Команды для сбора данных о симптомах

Команда	Описание
ping *{host|ip-address}*	Позволяет послать пакет эхо-запроса по адресу и ожидать ответ. Переменная *host | ip-address* - это IP-псевдоним или IP-адрес целевой системы.
traceroute *{destination}*	Позволяет определить путь передачи пакета по сетям. Переменная destination — это имя компьютера или IP-адрес целевой системы.
telnet *{host|ip-address}*	Позволяет подключиться к IP-адресу с помощью приложения Telnet.
show ip interface brief **show ipv6 interface brief**	Позволяет отобразить сводку состояний всех интерфейсов на устройстве.
show ip route **show ipv6 route**	Позволяет отобразить текущие таблицы маршрутизации IPv4 и IPv6, в которых указаны маршруты ко всем известным сетевым пунктам назначения.
show running-config	Позволяет отобразить содержимое файла текущей конфигурации.
[no] debug ?	Позволяет отобразить список параметров для включения или отключения событий отладки на устройстве.
show protocols	Позволяет отобразить настроенные протоколы, а также глобальное и поинтерфейсное состояние всех настроенных протоколов уровня 3.

Примечание. Несмотря на то, что команда **debug** является важным средством сбора данных о симптомах, она создаёт объёмный трафик консольных сообщений, и она может существенно уменьшить уровень производительности сетевого устройства. Если команду **debug**необходимо выполнить в обычное рабочее время, предупредите пользователей сети о планируемых процедурах по поиску и устранению неполадок, а также о возможном ухудшении уровня производительности сети. По окончании процедуры не забудьте отключить режим отладки.

Во многих случаях о проблеме сообщает конечный пользователь. Зачастую информация может быть очень общей или неопределённой, например, «Сеть не работает» или «Я не могу пользоваться электронной почтой». В таких случаях необходимо точнее определить проблему. При этом может потребоваться задать несколько вопросов конечным пользователям.

Опрос конечных пользователей

Рекомендации	Примеры вопросов конечному пользователю
Задавайте вопросы, прямо относящиеся к проблеме.	Что не работает?
Используйте каждый вопрос в качестве средства исключения или обнаружения возможных проблем.	Связаны ли друг с другом работающие и неработающие ресурсы?
Говорите с пользователем на том техническом языке, который ему понятен.	Работал ли когда-либо раньше не работающий сейчас ресурс?
Спросите у пользователя, когда впервые была обнаружена проблема.	Когда впервые была обнаружена проблема?
Происходило ли что-либо необычное с тех пор, когда всё ещё нормально работало?	Что изменилось с тех пор, когда всё ещё нормально работало?
Попросите пользователя воспроизвести проблему, если это возможно.	Можете ли вы воспроизвести проблему?
Определите последовательность событий, произошедших перед появлением проблемы.	Когда именно возникает проблема?

При опросе конечных пользователей о сетевой проблеме, с которой они могли столкнуться, задавайте правильные и точные вопросы. Это поможет вам получить информацию, необходимую для документирования симптомов проблемы. В таблице на рисунке приведены несколько рекомендаций, а также примеры вопросов для конечных пользователей.

Задание:

1. Ознакомится с теоретическим материалом.
2. Исправить проблему в задании, выданном преподавателем в Cisco PT.
3. Описать каждый этап по поиску и устранению проблемы.

Практическое занятие

Определение ошибок, связанных с кабелями и передающей средой

Цель: Определить возможные ошибками на физическом уровне модели OSI

Симптомы и причины отладки сети на физическом уровне

Физический уровень обеспечивает передачу битов между компьютерами и регулирует процесс передачи потока битов по физической среде. Физический уровень представляет собой единственный уровень, имеющий дело с физическими компонентами, например проводами, платами и антеннами.

Во многих случаях проблемы в сети проявляются как проблемы с производительностью. Проблемы с производительностью означают, что имеется разница между ожидаемым и наблюдаемым режимом работы и что система не функционирует должным образом. Отказы и неоптимальные состояния на физическом уровне не только создают неудобства пользователям, но и могут отрицательно влиять на уровень производительности всей компании. Сети, где возникают подобные ситуации, обычно перестают работать. Так как верхние уровни модели OSI зависят от функционирования физического уровня, то администратор сети должен иметь возможность эффективно изолировать и устранять проблемы на этом уровне.

К общим симптомам сетевых проблем на физическом уровне относятся следующие:

- **Уровень производительности ниже базового** — наиболее распространенными причинами медленного или плохого функционирования являются перегрузка или недостаточная вычислительная мощность серверов, ненадлежащая настройка коммутаторов или маршрутизаторов, затор трафика в канале с низкой пропускной способностью и постоянная потеря кадров.
- **Потеря связи** — если кабель или устройство выходит из строя; наиболее очевидным симптомом является потеря связи между устройствами, которые обмениваются данными по данному каналу с неисправным устройством либо интерфейсом. Такую ситуацию можно обнаружить путём отправки обычного эхо-запроса (ping). Неустойчивая связь может указывать на плохой электрический контакт или окислившиеся контактные поверхности.
- **Узкое место или затор в сети** — если маршрутизатор, интерфейс или кабель выходит из строя, то протоколы маршрутизации могут перенаправить трафик на другие маршруты, которые не рассчитаны на обработку дополнительного трафика. Это может привести к затору или появлению «узких мест» в таких зонах сети.
- **Высокая интенсивность использования ЦП** — высокая интенсивность использования ЦП говорит о том, что устройство, например маршрутизатор, коммутатор или сервер, работает на пределе своей расчётной производительности или превышает его. Если данную проблему быстро не устранить, то перегрузка ЦП может привести к выключению или отказу устройства.
- **Консольные сообщения об ошибках** — сообщениях об ошибках, выводимые на консоли устройства, указывают на проблему на физическом уровне.

К общим сетевым проблемам на физическом уровне относятся следующие:

- **Проблемы, связанные с электропитанием** — такие проблемы являются одной из основных причин сетевых проблем. Также необходимо проверить режим работы вентиляторов и убедиться, что впускные и вытяжные вентиляционные каналы шасси не загрязнены. Если на другие расположенные поблизости устройства также не поступает электропитание, то предположительно неисправен основной источник питания.
- **Отказы оборудования** — неисправные платы сетевых интерфейсов (NIC) могут быть причиной ошибок при передаче данных в сети

вследствие коллизий, коротких кадров и некорректных сигналов. Некорректный сигнал (Jabber) часто определяется как состояние, при котором сетевое устройство непрерывно передаёт беспорядочные и бессмысленные данные в сеть. Другими вероятными причинами таких сигналов являются поврежденные файлы драйверов сетевых карт, плохие кабельные соединения или проблемы с заземлением.

- **Проблемы с кабелями** — многие проблемы можно устранить путём повторного подключения кабелей, которые были частично отсоединены. При выполнении физического контроля обращайте внимание на поврежденные кабели, неправильные типы кабелей и дефектные разъёмы RJ-45. Предположительно неисправные кабели следует проверить и заменить исправными.

- **Затухание** — затухание может происходить в тех случаях, если длина кабеля превышает расчётный предел для среды передачи данных, или при наличии некачественного подключения вследствие применения некачественного кабеля, либо загрязнённых или окисленных контактов. Если уровень затухания является высоким, то принимающее устройство не всегда сможет успешно отличать друг от друга битовые компоненты в потоке.

- **Шум** — обычно шумом называются локальные электромагнитные помехи (EMI). Шум могут создавать разные источники, такие как радиостанции, полицейские системы радиосвязи, системы обеспечения безопасности в зданиях, авиационные системы для автоматической посадки, перекрёстные помехи (шум, наводимый другими кабелями в том же кабельном канале, или соседними кабелями), расположенные поблизости электрические кабели, устройства с крупными электродвигателями или любое оборудование, содержащее радиопередатчик, более мощный, чем мобильный телефон.

- **Ошибки настройки интерфейса** — на интерфейсе многие параметры могут оказаться неправильно настроенными, что может приводить к неработоспособности интерфейса, например неправильная тактовая частота, неправильный источник синхронизации, а также состояние, когда интерфейс не включен. Это приводит к потере связи с подключенными сегментами сети.

- **Превышение расчётных пределов**— компонент может работать некорректно на физическом уровне, так как он используется с большей нагрузкой, чем та, на которую он был рассчитан. При

устранении проблем такого типа становится очевидно, что ресурсы для устройства работают на максимальном пределе или почти на максимальном уровне, что приводит к увеличению количества ошибок интерфейса.

- **Перегрузка ЦП** — к симптомам данного состояния относятся процессы с высоким коэффициентом использования ЦП, нестабильная работа входных очередей, низкий уровень производительности, отсутствие или замедление отклика на запросы маршрутизатора, например Telnet и ping, или отсутствие обновлений маршрутизации. Одной из причин перегрузки ЦП в маршрутизаторе является интенсивный трафик. Если какие-то интерфейсы постоянно оказываются в состоянии перегрузки по трафику, то рекомендуется рассмотреть возможность перепроектирования потоков трафика в сети или модернизации оборудования.

Процесс поиска и устранения неполадок на уровне 2 может быть довольно сложным. Настройка и функционирование этих протоколов являются крайне важными аспектами для создания функциональной, хорошо настроенной сети. Проблемы на уровне 2 имеют отличительные признаки, которые в случае их обнаружения позволят оперативно выявить проблему.

Задание:

1. Ознакомится с теорией.
2. Определить возможные ошибки в задании выданном преподавателем.

Практическое занятие

Настройка коммутируемой сети, поиск и устранение неисправностей в ней

Цель: Найти и устранить неисправности в сети, смоделированной в Cisco PT

Поиск неисправностей в сети.

Поиск неисправностей в сети - это сочетание анализа (измерения, диагностика и локализация ошибок) и синтеза (принятие решения о том, какие изменения надо внести в работу сети, чтобы исправить ее работу).

Анализ - определение значения критерия эффективности (или, что одно и то же, критерия оптимизации) системы для данного сочетания параметров сети.

Из этого этапа выделяется подэтап мониторинга, на котором выполняется более простая процедура - процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т.п. Далее выполняется этап собственно анализа, под которым в этом случае понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Задача мониторинга решается программными и аппаратными измерителями, тестерами, сетевыми анализаторами и встроенными средствами мониторинга систем управления сетями и системами.

Задача анализа требует более активного участия человека, а также использования таких сложных средств как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

Синтез - выбор значений варьируемых параметров, при которых показатель эффективности имеет наилучшее значение. Если задано пороговое значение показателя эффективности, то результатом синтеза должен быть один из вариантов сети, превосходящий заданный порог.

Приведение сети в работоспособное состояние - это также синтез, при котором находится любой вариант сети, для которого значение показателя эффективности отличается от состояния "не работает". Синтез рационального варианта сети - процедура чаще всего неформальная, так как она связана с

выбором слишком большого и очень разнородного множества параметров сети - типов применяемого коммуникационного оборудования, моделей этого оборудования, числа серверов, типов компьютеров, используемых в качестве серверов, типов операционных систем, параметров этих операционных систем, стеков коммуникационных протоколов, их параметров и т.д. и т.п. Очень часто мотивы, влияющие на выбор "в целом", то есть выбор типа или модели оборудования, стека протоколов или операционной системы, не носят технического характера, а принимаются из других соображений - коммерческих, "политических" и т.п. Поэтому формализовать постановку задачи оптимизации в таких случаях просто невозможно. В данной книге основное внимание уделяется этапам мониторинга и анализа сети, как более формальным и автоматизируемым процедурам. В тех случаях, когда это возможно, в книге даются рекомендации по выполнению некоторых последовательностей действий по нахождению рационального варианта сети или приводятся соображения, облегчающие его поиск.

Обнаружение проблем в сетевом окружении.

Основные проблемы, которые могут возникать в сетевом окружении:

- потеря или невозможность соединения компьютеров в подсети и/или в домене,
- уменьшение скорости обмена данными,
- невозможность получить доступ к общим ресурсам сети - папкам, каталогам, принтерам и т.д,
- невозможность получения IP-адреса от сервиса DHCP,
- невозможность установления связи с компьютерами других доменов,
- нарушение функционирования сетевого взаимодействия с использованием безопасности IP,
- недоступность со стороны компьютера-клиента серверных компонентов.

Проверить наличие или отсутствие соединений с другими компьютерами в сети можно в папке **Сетевое окружение**, открыв папку **Вся сеть** (дважды щелкнув соответствующий значок). В папке **Вся сеть** доступна сеть **Microsoft Windows Network**. Открыв ее, можно увидеть значки с именами доступных доменов подсетей, и далее, значки компьютеров входящих в эти подсети. Отсутствие

значков уже говорит об отсутствии соединений. Но если соединение с каким-либо компьютером внезапно пропадет, то попытка открыть этот компьютер вызовет задержку в работе проводника на период срабатывания тайм-аута и система выведет сообщение об отсутствии в сети ресурса. Аналогично обстоит дело с доступом к каталогу **Active Directory**, значок которого Каталог находится там же, в папке **Вся сеть**.

Поиск неисправностей в сети. Утилиты TCP/IP.

Windows XP предоставляет в ваше распоряжение широкий набор утилит для управления, конфигурирования и выявления неисправностей среды TCP/IP.

Ping - диагностическая утилита, которая проверяет возможность соединения с удаленным компьютером.

Pathping - усовершенствованная утилита ping, которая также отражает маршрут прохождения и предоставляет статистику потери пакетов на промежуточных маршрутизаторах.

Route - показывает и позволяет изменять конфигурацию локальной таблицу маршрутизации.

Tracert - отслеживает маршрут, по которому пакеты перемещаются на пути к пункту назначения.

Netstat - показывает текущую информацию сетевого соединения TCP/IP. Например, информацию о подключенном хосте и номера используемых портов.

Ipconfig - показывает текущую конфигурацию TCP/IP на локальном компьютере.

Hostname - показывает локально настроенное имя узла TCP/IP ..

Arp - показывает и позволяет изменять кэш протокола ARP (Address Resolution Protocol), где хранится информация о соответствии IP - адресов - MAC - адресам локальных узлов.

Nslookup - утилита командной строки - распознаватель для запросов DNS сервера.

Утилиты выполняются из командной строки.

Чтобы открыть окно командной строки нажмите кнопку Пуск и выберите последовательно команды Все программы -> Стандартные -> Командная строка.

Если не удается подключиться к другому компьютеру, могут иметь место неполадки с подключением или неполадки с именами.

Применение утилит ping и ipconfig.

Чтобы определить причину неполадок, попытайтесь выполнить обмен пакетами (утилита ping) с IP-адресом другого компьютера. Таким компьютером может быть компьютер, с которым вы пытаетесь соединиться, или основной шлюз.

Чтобы определить IP-адрес основного шлюза: наберите в командной строке ipconfig и нажмите клавишу ENTER. Если требуемая информация уходит с экрана, то для просмотра экранов по очереди введите ipconfig | more и нажмите клавишу ENTER. В отображаемых результатах найдите строку Основной шлюз и запишите соответствующий IP-адрес.

Чтобы выполнить обмен пакетами (ping) с другим компьютером: наберите в командной строке: ping адрес, где адрес представляет IP-адрес другого компьютера, и нажмите клавишу ENTER.

Если обмен пакетами выполнен успешно, появляется отклик, аналогичный следующему:

Ответ от <адрес> число байт=32:
Ответ от <адрес>: число байт=32 время=75мс TTL=28
Ответ от <адрес>: число байт=32 время=87мс TTL=28

Если обмен пакетами выполнить не удается, появляется отклик, аналогичный следующему:

Ответ от <адрес> число байт=32:
Превышен интервал ожидания.
Превышен интервал ожидания.

Утилита **Ipconfig** показывает текущую конфигурацию TCP/IP на локальном

компьютере.
Ключи утилиты:

/release - освобождает полученный от DHCP IP - адрес.
/renew - получает от DHCP новый IP - адрес.
/all - показывает всю информацию о TCP/IP конфигурации.
/flushdns - очищает кэш локального распознавателя DNS.
/regsiterdns - обновляет адрес в DHCP и перерегистрирует его в DNS.
/displaydns - показывает содержание кэша распознавателя DNS.

Задание:

1. Ознакомиться с теорией.
2. Найти и устранить неисправности в задании выданном преподавателем.

Практическое занятие

Поиск и устранение неисправностей соединений LAN

Цель: Получение практических навыков по поиску и устранению неисправностей соединений LAN

Теория:

Рассмотрим некоторые неполадки, причины их возникновения и пути разрешения.

1. Клиенты входящих подключений не могут видеть ресурсы вне компьютера, принимающего входящие подключения.

Причина. Если адреса, назначаемые клиентам входящих подключений, не принадлежат сети, к которой подключен компьютер, принимающий входящие подключения, то для этих клиентов необходимо создать маршрут к компьютерам интрасети.

Решение. Измените диапазон IP-адресов, выделяемых клиентам входящих подключений, чтобы он был подмножеством адресов сети, к которой подключен компьютер, принимающий входящие подключения. Если сделать это нельзя, то задайте для узлов интрасети в качестве адреса основного шлюза IP-адрес компьютера, принимающего входящие подключения.

- Если узлы интрасети настроены на автоматическое получение IP-адреса и в интрасети работает сервер DHCP, то его можно настроить на автоматическое назначение основного шлюза компьютерам.
- Если узлы интрасети настроены на автоматическое получение IP-адреса, а сервер DHCP в интрасети отсутствует (т.е. используется средство автоматического назначения частных IP-адресов), то нужно будет на каждом узле интрасети вручную задать IP-адрес, маску подсети и адрес основного шлюза.

Причина. Вычисленный диапазон адресов, выделяемых клиентам входящих подключений, шире диапазона, указанного пользователем.

Решение. В большинстве сетей TCP/IP для более эффективного управления IP-адресами используются подсети. Для диапазона адресов, заданного в полях **С** и **По**, вычисляется ближайшая подходящая подсеть. Диапазон адресов в такой подсети может оказаться шире диапазона, указанного при настройке. Так происходит в случае, если адреса в полях **С** и **По** не являются границами подсети. Во избежание проблем укажите диапазон, границы которого совпадают

с границами подсети. Например, если используется интрасеть с идентификатором частной сети 10.0.0.0, то примером диапазона, границы которого попадают точно на границы подсети, является диапазон 10.0.1.168 — 10.0.1.175. Для интрасети с идентификатором 192.168.0.0 можно задать диапазон 192.168.1.0 — 192.168.1.255.

2. При использовании подключения по локальной сети отсутствует ответ.

Причина. Возможно, неполадки связаны с сетевым адаптером.

Решение. Выполните следующие действия.

- Посмотрите на значок подключения по локальной сети. В зависимости от состояния подключения по локальной сети значок в папке «Сетевые подключения» может выглядеть по-разному. Кроме того, при отключении адаптера от среды передачи (например, при отсоединении кабеля) в области уведомлений появляется значок состояния. Дополнительные сведения см. в разделе Подключения по локальной сети.
- Проверьте правильность работы сетевого адаптера с помощью Диспетчера устройств.

Причина. Возможно, кабель локальной сети отсоединен от сетевого адаптера.

Решение. Убедитесь, что кабель локальной сети подключен к сетевому адаптеру.

3. Конфликты между последовательными портами вызывают неполадки с подключением.

Причина. Конфликты между последовательными портами.

Это правило действует и при использовании мыши совместно с программами последовательной связи, такими как компонент «Сетевые подключения» или программа терминала. Данное правило не распространяется на случай, когда используется интеллектуальный последовательный адаптер, такой как DigiBoard.

4. При попытке подключения возвращается сообщение об ошибке оборудования.

Причина. Модем выключен.

Решение. Проверьте, включен ли модем. Если он выключен, включите его и повторите набор номера.

Причина. Модем работает неправильно.

Решение. Включите ведение журнала команд модема, чтобы проверить подключение.

Причина. Несовместимый кабель.

Решение. Если связь поддерживается через окно терминала, а не с помощью компонента «Сетевые подключения», возможно, модем подключен к компьютеру неподходящим кабелем. Нужно использовать совместимый кабель.

5. Модем все время подключается на более низкой скорости, чем указано.

Причина. Модем и телефонная линия работают неправильно. Избыточное статическое электричество на телефонной линии приводит к разрыву связи.

Решение. Проверьте правильность работы модема с помощью средств диагностики.

Причина. Недостаточно высокое качество исходящей линии.

Решение. Попросите телефонную компанию проверить качество линии.

Причина. На скорость влияет качество вызываемой линии.

Решение. Если к поставщику услуг Интернета можно подключиться по нескольким номерам, попробуйте использовать другой номер.

Причина. Программное обеспечение модема требует обновления.

Решение. Выясните у изготовителя модема, нет ли для модема обновленного программного обеспечения.

Задание:

1. Ознакомится с примерами неисправностей и способами их устранения.
2. Выполнить поиск и устранение неисправностей в задании выданном преподавателем.

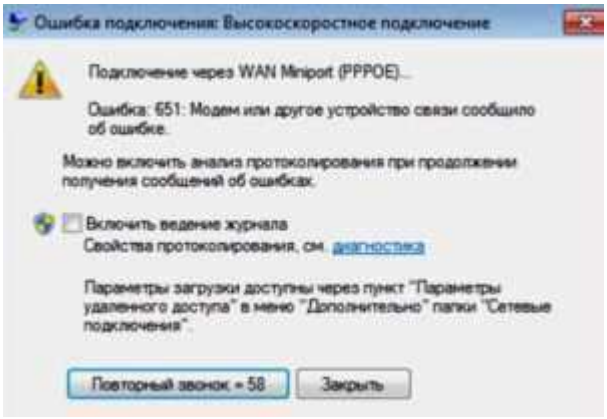
Практическое занятие

Поиск и устранение неисправностей соединений WAN

Цель: Получить практические навыки по поиску и устраниению неисправностей соединения WAN

Ошибка подключения 651 в Windows 7 высвечивается на экране в виде небольшого окна.

Для каждого протокола WAN-порт имеет собственный минипорт. Подключение через WAN miniport PPPoE дает сбой, тогда и появляется это сообщение:



Ошибка 651 при подключении к интернету в Windows 10 выглядит несколько иначе, но принципиальной разницы нет. То же самое касается и Windows 8.

Код ошибки 651 означает, что возник сетевой сбой по протоколу PPPoE. Выдается информация: «Модем или другое устройство связи сообщило об ошибке». В английском варианте: «Error 651: The modem (or other connecting devices) has reported an error». Тем самым система сигнализирует пользователю: «Не могу подключиться к интернету».

Причины возникновения ошибки 651 разные:

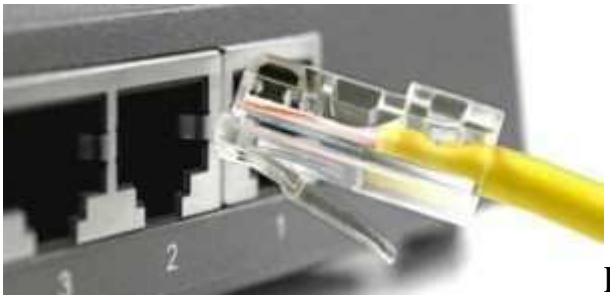
- Повреждение кабеля или оборудования;
- Сбой настроек;
- Дефекты у провайдера;
- Вирусы и антивирусы.

Физические повреждения

Ошибку вызывают повреждения оборудования, а именно:

- Нарушение работы сетевой карты;

- Отказ роутера;
- Повреждение коммуникационных кабелей;
- Неисправность соединительных разъемов;



Начать проверку надо с коммутационных шнуров и разъемов. Визуально осмотреть их, если повреждений нет, осуществить плотное соединение без перекосов. Есть вероятность, что ошибка 651 будет устранена.

Неисправности сетевой карты и мелкие сбои в работе приборов самостоятельно определить невозможно. Тут нужно быть специалистом. Но попытка найти другие причины ошибки может оказаться удачной.

Сбой клиента RASPPPOE

В Windows за работу протокола PPPoE отвечает системный файл **raspppoe.sys**, расположенный в директории **C:\Windows\System32\Drivers**. Существует вероятность повреждения этого файла. Проверить:

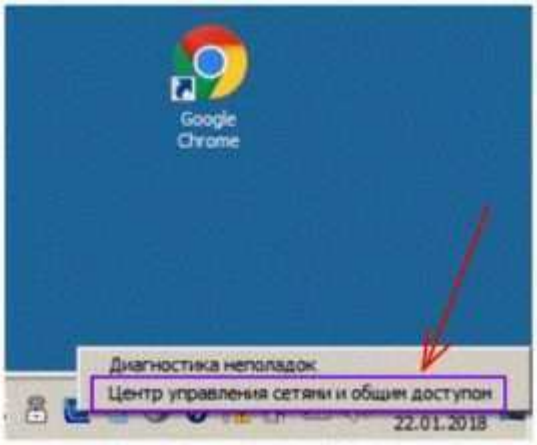
- На копию файла на другом компьютере или ноутбуке. Если такой возможности нет, скачать из интернета;
- Сохранить старый файл во временном каталоге, поменять его на копию;
- Если ошибка 651 не «ушла», вернуть «родной» файл на место и продолжить поиски неисправности.

Наличие второй сетевой карты

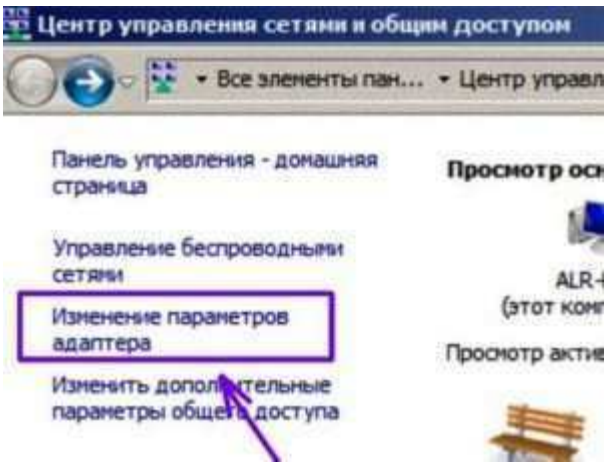
Если имеются две карты и обе задействованы, это вызывает конфликт соединений, приводит к сбою подключения с ошибкой 651. Отключение кабеля второго соединения ничего не даст. Надо отключить второе соединение, для этого:

- Щелкнуть по значку сети правой клавишей мыши;

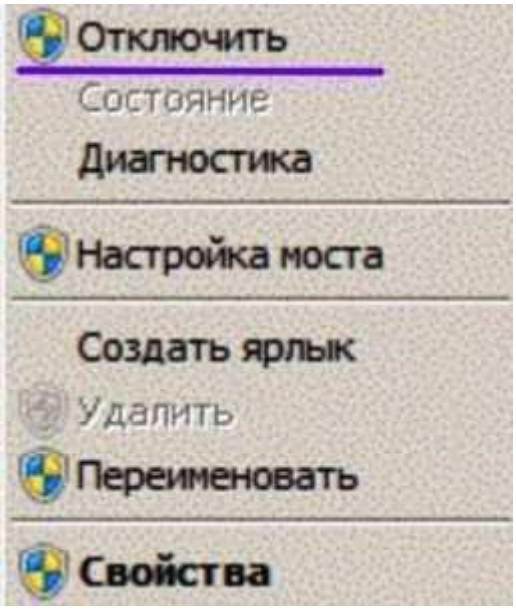
- В открывшемся меню выбрать «Центр управления сетями и общим доступом»;



- Выбрать выделенный пункт меню;



- Появляется список созданных подключений;
- Щелкнуть по нужному правой клавишей мыши;
- Во всплывшем контекстном меню выбрать первый пункт;



Если не помогло, отключить и включить снова подсоединение, вызвавшее ошибку. Если опять не повезло, искать другие причины, но второе соединение пока не трогать.

Сбой настроек роутера или модема

Когда работа идет через роутер или ADSL-модем, попробовать подсоединиться к ним через другой компьютер или через альтернативную сетевую карту. Если таковой возможности нет, или все подключения выдают ошибку, проверить настройки устройств. Любой модем и роутер: TP-link, ASUS, Zyxel и другие имеют встроенный WEB-интерфейс, с помощью которого получится доступ к настройкам. Для этого:

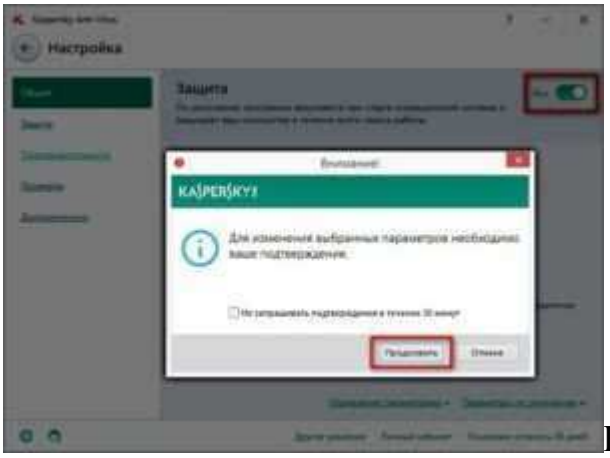
- В адресной строке браузера набрать 192.168.1.1. Должно появиться окно авторизации. Если оно не всплыло, перевернуть устройство. На нижней панели бывает наклейка с реквизитами, необходимыми для входа в WEB-интерфейс. Или найти реквизиты в руководстве к устройству;

- Ввести в окно авторизации найденные логин и пароль;
- В открывшемся окне WEB-интерфейса найти вкладку «Интернет» или «WAN»;
- Сверить данные подключения с реквизитами, полученными от провайдера;
- Исправить ошибочные значения и перезагрузить устройство.

Для ADSL-модемов внимание надо обратить на параметры VPI и VCI, неверные значения которых способны вызвать ошибку 651 при подключении к интернету.

Модем также может не получать сигнала по телефонной линии. Необходимо проверить светодиодные индикаторы на устройстве: они горят.

Проверка антивируса и файервола



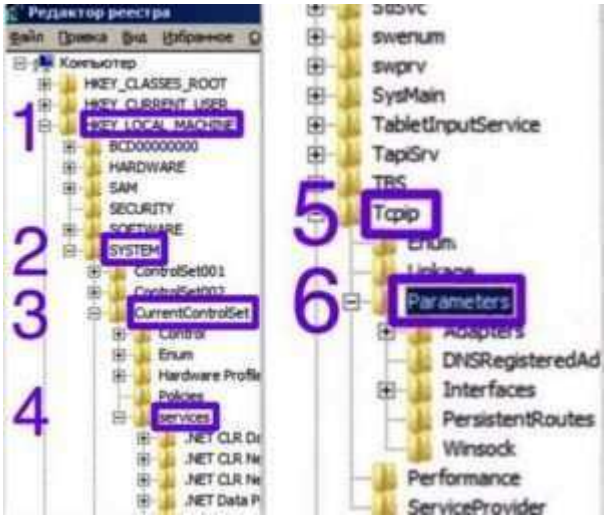
Надо проверить систему на наличие вирусов. Для этого обновить базы антивируса и запустить полную проверку. Если вирусов нет, возможно, сам антивирус или файервол вызывают сбой подключения с ошибкой. Временно отключить их.

Если ошибка 651 не проявляется, связаться с разработчиками антивируса и выяснить причины, а также способ устранения неисправности без отключения. Разработчики должны помочь настроить и файервол, поскольку это взаимосвязанные программы.

Замена значений в реестре для серверных ОС

Манипуляции с реестром решают вопрос для серверов, но, возможно, помогут исправить ошибку и для систем Windows, не являющихся серверными. Если роутер или модем сообщают об ошибке, следует попытаться поработать с реестром:

- Выполнить команду regedit, вводя ее в строке поиска;
- Раскрыть каталог, нажимая «плюсики» и последовательно выбирая;



- Вызвать контекстное меню, щелкнув справа в пустом месте. Дважды создать параметр DWORD (32 бита). Сначала — DisableTaskOffload со значением 1, затем — EnableRSS со значением 0.

- Перезагрузить компьютер. Если и это не помогло, продолжить поиски.

Проблемы у провайдера

Если подключение идет через маршрутизатор или модем и есть возможность подсоединиться к сети по Wi-Fi, попробовать связаться с планшета или смартфона. Если все прошло успешно, продолжить поиск ошибки в компьютере. В другом случае позвонить провайдеру.

Еще несколько полезных советов

Когда сетевое подключение «капризничает», применить еще четыре стандартных приема, способных помочь:

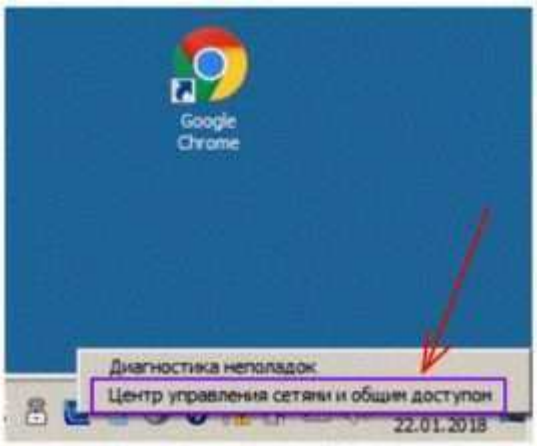
Обновление драйвера сетевой карты

Проверить драйвер сетевой карты. Для этого через панель управления войти в диспетчер устройств. Найти сетевой адаптер. При обнаружении напротив него желтой отметки в виде восклицательного знака надо переустановить драйвер.

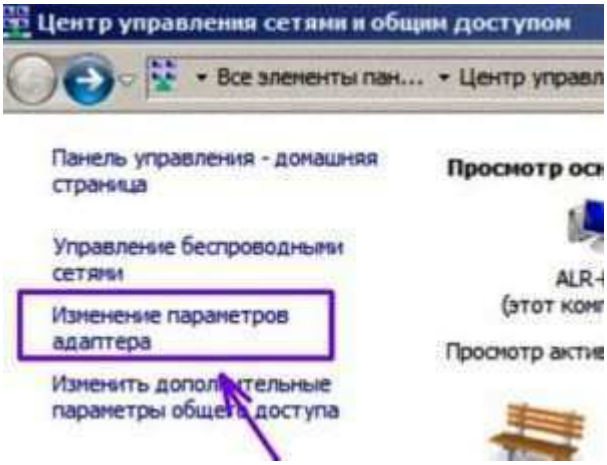
Создание нового высокоскоростного подключения

Удаление и повторное создание подключения способно исправить возможные некорректности. Чтобы это осуществить:

- Щелкнуть правой клавишей по значку сети и выбрать;



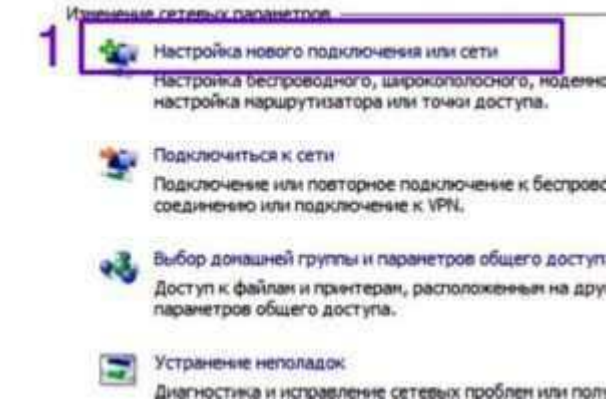
- Вывести на экран список соединений, щелкая по выделенному на рисунке пункту меню;

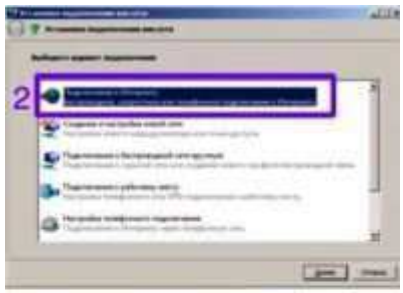


- Удалить подключение с ошибкой. Для этого кликнуть по нему правой клавишей и в появившемся контекстном меню выбрать соответствующий пункт.

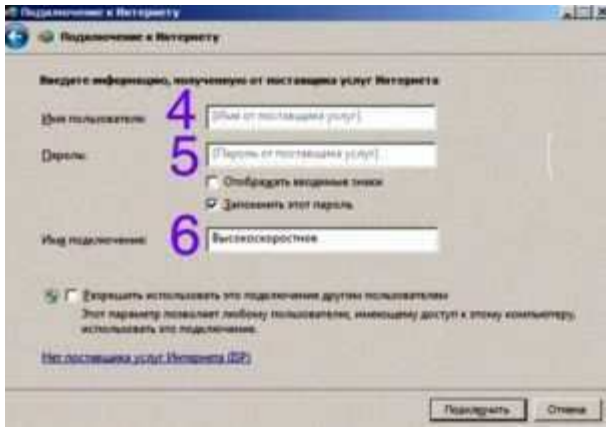
Создать новое подключение:

- Вернуться и последовательно выполнить пункты, начиная с первого;





- Заполнить поля;



Если создание нового соединения не помогло, продолжать искать ошибку.

Отключение IPV6

Попытаться «убить» ошибку, отключив протокол IPV6, переходя на старый проверенный IPV4. Щелкнуть сбоящее соединение правой клавишей, нажать «Свойства». В пункте меню «Сеть» снять галочку с IPV6.

Отключение TCP-настройки

Windows имеет функцию для оптимизации работы приложений, использующих TCP-пакеты, – это IP Receive Window Auto-Tuning. Для работы домашней сети она не нужна, поэтому надо отключить, поскольку велика вероятность, что она «вмешивается» в работу протокола PPPoE. Попытаться отключить эту функцию. Работу выполнить от имени администратора:

- Открыть командную строку.
- Сбросить к заводским настройкам журнал протокола TCP/IP, выполняя команду: **netsh int ip reset resetlog.txt**
- Отключить функцию, выполнив команду: **netsh interface tcp set global autotuning = disabled.**

Задание:

1. Ознакомится с теорией.
2. Выполнить задание выданное преподавателем.

Практическое занятие

Поиск и устранение неисправностей DHCP и NAT

Цель: Получить практические навыки по поиску и устранению неисправностей DHCP и NAT

Топология

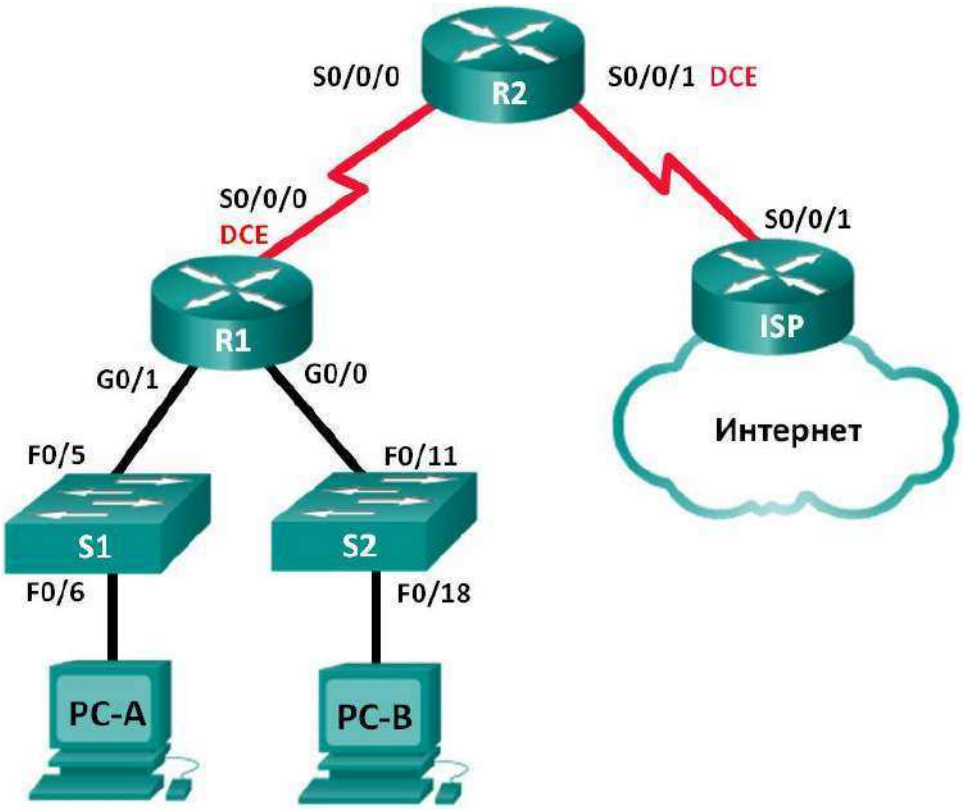


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.0.1	255.255.255.128	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.0.253	255.255.255.252	N/A
R2	S0/0/0	192.168.0.254	255.255.255.252	N/A
	S0/0/1 (DCE)	209.165.200.226	255.255.255.252	N/A
ISP	S0/0/1	209.165.200.225	255.255.255.252	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.0.2	255.255.255.128	192.168.0.1

PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

Задачи

Часть 1. Построение сети и настройка базовых параметров устройства
Часть 2. Выполнение поиска и устранения неполадок в работе DHCPv4

Исходные данные/сценарий

Протокол динамической конфигурации сетевого узла (DHCP) — сетевой протокол, позволяющий сетевым администраторам управлять назначением и автоматизировать назначение IP-адресов. Без использования DHCP администратору приходится вручную назначать и настраивать IP-адреса, предпочтительные DNS-серверы и шлюз по умолчанию. По мере увеличения сети и перемещении устройств из одной внутренней сети в другую это становится административной проблемой.

В предложенном сценарии размеры компании увеличились, и сетевые администраторы больше не имеют возможности назначать IP-адреса для устройств вручную. Маршрутизатор R2 был настроен в качестве сервера DHCP для назначения IP-адресов узловым устройствам в локальных сетях

маршрутизатора R1. В результате нескольких ошибок в настройках возникли проблемы со связью. Вас попросили выполнить поиск и устранение неполадок в конфигурации и написать отчёт о проделанной работе.

Убедитесь в том, что сеть соответствует следующим требованиям:

1. Маршрутизатор R2 должен функционировать в качестве сервера DHCP для сетей
192.168.0.0/25 и 192.168.1.0/24, подключённых к маршрутизатору R1.

2. Все ПК, подключённые к коммутаторам S1 и S2, должны получить IP-адрес в нужной сети с помощью DHCP.

Часть 1: Построение сети и настройка базовых параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить основные параметры на маршрутизаторах и коммутаторах, такие как пароли и IP-адреса. Также вам предстоит настроить параметры IP для компьютеров в приведённой топологии.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 3: Настройте базовые параметры каждого маршрутизатора.

b. Отключите поиск DNS.

c. Присвойте имена устройствам в соответствии с топологией.

d. Назначьте **class** в качестве пароля привилегированного режима EXEC.

e. Назначьте **cisco** в качестве паролей консоли и VTY.

f. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.

g. Назначьте IP-адреса всем интерфейсам маршрутизатора.

h. Установите тактовую частоту на **128000** для всех интерфейсов маршрутизатора DCE.

i. Настройте EIGRP на маршрутизаторе R1.

R1(config)# **router eigrp 1**

R1(config-router)# **network 192.168.0.0 0.0.0.127** R1(config-router)# **network 192.168.0.252 0.0.0.3**

R1(config-router)# **network 192.168.1.0** R1(config-router)# **no auto-summary**

j. На маршрутизаторе R2 настройте EIGRP и статический маршрут по умолчанию.

R2(config)# **router eigrp 1**

R2(config-router)# **network 192.168.0.252 0.0.0.3**

R2(config-router)# **redistribute static**

R2(config-router)# **exit**

R2(config)# **ip route 0.0.0.0 0.0.0.0 209.165.200.225**

k. Настройте суммарный статический маршрут на маршрутизаторе ISP к сетям на маршрутизаторах

R1 и R2.

ISP(config)# **ip route 192.168.0.0 255.255.254.0 209.165.200.226**

Шаг 4: Выполните проверку сетевого соединения между маршрутизаторами.

При неудачных эхо-запросах между маршрутизаторами исправьте обнаруженные ошибки, прежде чем переходить к следующему шагу. Используйте команды **show ip route** и **show ip interface brief**, чтобы определить возможные неполадки.

Шаг 5: Настройте базовые параметры каждого коммутатора.

b. Отключите поиск DNS.

c. Присвойте имена устройствам в соответствии с топологией.

d. Назначьте IP-адрес интерфейсу VLAN 1 и шлюз по умолчанию для каждого коммутатора.

e. Назначьте **class** в качестве пароля привилегированного режима EXEC.

f. Назначьте **cisco** в качестве паролей консоли и VTY.

g. Настройте **logging synchronous** для консольного канала.

Шаг 6: Убедитесь в том, что на узлах включена работа с DHCP.

Шаг 7: Загрузите начальную конфигурацию DHCP для маршрутизаторов R1 и R2.

Маршрутизатор R1

interface GigabitEthernet0/1

ip helper-address 192.168.0.253

Маршрутизатор R2

ip dhcp excluded-address 192.168.11.1 192.168.11.9 ip dhcp excluded-address 192.168.0.1 192.168.0.9 ip dhcp pool R1G1

network 192.168.1.0 255.255.255.0 default-router 192.168.1.1

ip dhcp pool R1G0

network 192.168.0.0 255.255.255.128 default-router 192.168.11.1

Часть 2: Поиск и устранение неполадок в работе DHCPv4

После настройки маршрутизаторов R1 и R2 с параметрами DHCPv4 появилось несколько ошибок

в настройке DHCP, которые привели к неполадкам в подключении. Маршрутизатор R2 настроен

в качестве сервера DHCP. В обоих пулах адресов DHCP первые девять адресов зарезервированы для маршрутизаторов и коммутаторов. Маршрутизатор R1 ретранслирует информацию о DHCP во все локальные сети маршрутизатора R1. На данный момент компьютеры PC-A и PC-B не имеют доступа

к сети. Используйте команды **show** и **debug** для выявления и исправления проблем с сетевым соединением.

Шаг 1: Запишите IP-параметры для компьютеров PC-A и PC-B.

b. В командной строке компьютеров PC-A и PC-B введите **ipconfig /all** для отображения IP- и MAC-адресов.

c. Запишите IP- и MAC-адреса в таблице. MAC-адрес можно использовать для определения какой ПК упоминается в сообщении об ошибке.

Шаг 2: Устраните неполадки в работе DHCP для сети 192.168.1.0/24 на маршрутизаторе

R1.

Маршрутизатор R1 является агентом DHCP-ретрансляции для всех сетей LAN маршрутизатора R1. На данном этапе будет рассматриваться только процесс DHCP для сети 192.168.1.0/24. Первые девять адресов зарезервированы для других сетевых устройств, включающих маршрутизаторы, коммутаторы и серверы.

b. Для наблюдения за процессом DHCP на маршрутизаторе R2 используйте команду DHCP **debug**.

R2# **debug ip dhcp server events**

c. На маршрутизаторе R1 отобразите текущую конфигурацию интерфейса G0/1.

R1# **show run interface g0/1** interface GigabitEthernet0/1

ip address 192.168.1.1 255.255.255.0 ip helper-address 192.168.0.253 duplex auto

speed auto

При наличии каких-либо проблем с DHCP-ретрансляцией, запишите команды, которые понадобятся для исправления ошибок конфигурации.

d. дной строке компьютера PC-A введите **ipconfig /renew**, чтобы получить адрес от сервера DHCP. Запишите полученный IP-адрес, маску подсети и шлюз по умолчанию для PC-A.

e. Проследите за процессом обновления информации для PC-A с помощью отладочных сообщений на маршрутизаторе R2. Сервер DHCP пытался назначить компьютеру PC-A адрес 192.168.1.1/24. Данный адрес уже используется для интерфейса G0/1 маршрутизатора R1. Та же проблема возникла с IP-адресом 192.168.1.2/24, поскольку в начальной конфигурации адрес был назначен коммутатору S1. Поэтому компьютеру PC-A был назначен IP-адрес 192.168.1.3/24. Конфликт при назначении адреса DHCP указывает, что при настройке сервера DHCP на маршрутизаторе R2 определенные адреса могли быть не исключены из пула DHCP.

*Mar 5 06:32:16.939: DHCPD: Sending notification of DISCOVER: *Mar 5 06:32:16.939: DHCPD: htype 1 chaddr 0050.56be.768c *Mar 5 06:32:16.939: DHCPD: circuit id 00000000

*Mar 5 06:32:16.939: DHCPD: Seeing if there is an internally specified pool class: *Mar 5 06:32:16.939: DHCPD: htype 1 chaddr 0050.56be.768c

*Mar 5 06:32:16.939: DHCPD: circuit id 00000000

*Mar 5 06:32:16.943: DHCPD: Allocated binding 2944C764

*Mar 5 06:32:16.943: DHCPD: Adding binding to radix tree (192.168.1.1) *Mar 5 06:32:16.943: DHCPD: Adding binding to hash tree

*Mar 5 06:32:16.943: DHCPD: assigned IP address 192.168.1.1 to client 0100.5056.be76.8c.

*Mar 5 06:32:16.951: %DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.1.1.

*Mar 5 06:32:16.951: DHCPD: returned 192.168.1.1 to address pool R1G1. *Mar 5 06:32:16.951: DHCPD: Sending notification of DISCOVER:

*Mar 5 06:32:16.951: DHCPD: htype 1 chaddr 0050.56be.768c *Mar 5 06:32:16.951: DHCPD: circuit id 00000000

*Mar 5 06:32:1

R2#6.951: DHCPD: Seeing if there is an internally specified pool class: *Mar 5 06:32:16.951: DHCPD: htype 1 chaddr 0050.56be.768c

*Mar 5 06:32:16.951: DHCPD: circuit id 00000000

*Mar 5 06:32:16.951: DHCPD: Allocated binding 31DC93C8

*Mar 5 06:32:16.951: DHCPD: Adding binding to radix tree (192.168.1.2) *Mar 5 06:32:16.951: DHCPD: Adding binding to hash tree

*Mar 5 06:32:16.951: DHCPD: assigned IP address 192.168.1.2 to client 0100.5056.be76.8c.

*Mar 5 06:32:18.383: %DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.1.2.

*Mar 5 06:32:18.383: DHCPD: returned 192.168.1.2 to address pool R1G1. *Mar 5 06:32:18.383: DHCPD: Sending notification of DISCOVER:

*Mar 5 06:32:18.383: DHCPD: htype 1 chaddr 0050.56be.6c89 *Mar 5 06:32:18.383: DHCPD: circuit id 00000000

*Mar 5 06:32:18.383: DHCPD: Seeing if there is an internally specified pool class: *Mar 5 06:32:18.383: DHCPD: htype 1 chaddr 0050.56be.6c89

*Mar 5 06:32:18.383: DHCPD: circuit id 00000000

*Mar 5 06:32:18.383: DHCPD: Allocated binding 2A40E074

*Mar 5 06:32:18.383: DHCPD: Adding binding to radix tree (192.168.1.3) *Mar 5 06:32:18.383: DHCPD: Adding binding to hash tree

*Mar 5 06:32:18.383: DHCPD: assigned IP address 192.168.1.3 to client 0100.5056.be76.8c.

<output omitted>

f. Отобразите конфигурацию сервера DHCP на маршрутизаторе R2. Первые девять адресов для сети 192.168.1.0/24 не исключены из пула DHCP.

R2# **show run | section dhcp**

ip dhcp excluded-address 192.168.11.1 192.168.11.9 ip dhcp excluded-address 192.168.0.1 192.168.0.9 ip dhcp pool R1G1

network 192.168.1.0 255.255.255.0 default-router 192.168.1.1

ip dhcp pool R1G0

network 192.168.0.0 255.255.255.128 default-router 192.168.1.1

Запишите команды для решения обнаруженной проблемы на маршрутизаторе R2.

i. В командной строке компьютера PC-A введите **ipconfig /release**, чтобы вернуть адрес 192.168.1.3 обратно в пул DHCP. За процессом можно проследить с помощью сообщений команды debug на маршрутизаторе R2.

*Mar 5 06:49:59.563: DHCPD: Sending notification of TERMINATION: *Mar 5 06:49:59.563: DHCPD: address 192.168.1.3 mask 255.255.255.0 *Mar 5 06:49:59.563: DHCPD: reason flags: RELEASE

*Mar 5 06:49:59.563: DHCPD: htype 1 chaddr 0050.56be.768c

*Mar 5 06:49:59.563: DHCPD: lease time remaining (secs) = 85340

*Mar 5 06:49:59.563: DHCPD: returned 192.168.1.3 to address pool R1G1.

j. В командной строке компьютера PC-A введите **ipconfig /renew**, чтобы компьютеру был назначен новый IP-адрес сервером DHCP. Запишите назначенные IP-адреса и данные шлюза по умолчанию.

За процессом можно проследить с помощью сообщений команды debug на маршрутизаторе R2.

*Mar 5 06:50:11.863: DHCPD: Sending notification of DISCOVER: *Mar 5 06:50:11.863: DHCPD: htype 1 chaddr 0050.56be.768c *Mar 5 06:50:11.863: DHCPD: circuit id 00000000

*Mar 5 06:50:11.863: DHCPD: Seeing if there is an internally specified pool class: *Mar 5 06:50:11.863: DHCPD: htype 1 chaddr 0050.56be.768c

*Mar 5 06:50:11.863: DHCPD: circuit id 00000000

*Mar 5 06:50:11.863: DHCPD: requested address 192.168.1.3 has already been assigned. *Mar 5 06:50:11.863: DHCPD: Allocated binding 3003018C

*Mar 5 06:50:11.863: DHCPD: Adding binding to radix tree (192.168.1.10) *Mar 5 06:50:11.863: DHCPD: Adding binding to hash tree

*Mar 5 06:50:11.863: DHCPD: assigned IP address 192.168.1.10 to client 0100.5056.be76.8c.

<output omitted>

k. Проверьте сетевое соединение.

Можно ли отправить эхо-запрос от компьютера PC-A на назначенный шлюз по умолчанию?

Можно ли отправить эхо-запрос от компьютера PC-A на маршрутизатор R2?

Можно ли отправить эхо-запрос от компьютера PC-A на маршрутизатор ISP?

Шаг 3: Выполните поиск и устранение неполадок в работе DHCP для сети 192.168.0.0/25 на маршрутизаторе R1.

Маршрутизатор R1 является агентом DHCP-ретрансляции для всех сетей LAN маршрутизатора R1. На этом этапе будет рассматриваться только процесс DHCP для сети 192.168.0.0/25. Первые девять адресов зарезервированы для других сетевых устройств.

a. Для наблюдения за процессом DHCP на маршрутизаторе R2 используйте команду DHCP **debug**.

R2# **debug ip dhcp server events**

b. Отобразите текущую конфигурацию интерфейса G0/0 маршрутизатора R1, чтобы определить возможные проблемы в работе DHCP.

R1# **show run interface g0/0**

interface GigabitEthernet0/0

ip address 192.168.0.1 255.255.255.128 duplex auto

speed auto

Запишите обнаруженные проблемы и все команды, которые понадобятся для исправления ошибок конфигурации.

c. В командной строке компьютера PC-B введите **ipconfig /renew**, чтобы получить адрес от сервера DHCP. Запишите полученный IP-адрес, маску подсети и шлюз по умолчанию для PC-B.

d. За процессом обновления для PC-A можно проследить с помощью сообщений команды debug на маршрутизаторе R2. Сервер DHCP назначил компьютеру PC-B адрес 192.168.0.10/25.

*Mar 5 07:15:09.663: DHCPD: Sending notification of DISCOVER: *Mar 5 07:15:09.663: DHCPD: htype 1 chaddr 0050.56be.f6db *Mar 5 07:15:09.663: DHCPD: circuit id 00000000

*Mar 5 07:15:09.663: DHCPD: Seeing if there is an internally specified pool class:
*Mar 5 07:15:09.663: DHCPD: htype 1 chaddr 0050.56be.f6db

*Mar 5 07:15:09.663: DHCPD: circuit id 00000000

*Mar 5 07:15:09.707: DHCPD: Sending notification of ASSIGNMENT:

*Mar 5 07:15:09.707: DHCPD: address 192.168.0.10 mask 255.255.255.128 *Mar 5 07:15:09.707: DHCPD: htype 1 chaddr 0050.56be.f6db

*Mar 5 07:15:09.707: DHCPD: lease time remaining (secs) = 86400

e. Проверьте сетевое соединение.

Можно ли отправить эхо-запрос от компьютера PC-B на шлюз по умолчанию, назначенный сервером DHCP?

Можно ли отправить эхо-запрос от PC-B на его шлюз по умолчанию (192.168.0.1)?

Можно ли отправить эхо-запрос от компьютера PC-B на маршрутизатор R2?

Можно ли отправить эхо-запрос от компьютера PC-B на маршрутизатор ISP?

f. При возникновении каких-либо неполадок на шаге e, запишите обнаруженные проблемы и все команды, необходимые для устранения неполадок.

g. Очистите и обновите настройки IP на компьютере PC-B. Повторите шаг e для проверки сетевого соединения.

h. Прервите процесс отладки с помощью команды **undebug all**.

R2# **undebug all**

All possible debugging has been turned off