Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра защиты информации

КОМПЬЮТЕРНЫЕ СЕТИ

Методические указания к лабораторным работам
для студентов специальностей
1-45 01 03 «Сети телекоммуникаций»,
1-98 01 02 «Защита информации в телекоммуникациях»
всех форм обучения

Минск БГУИР 2010

УДК 004.71(076.5)
ББК 32.973.202я73
К63

А в т о р ы:
А. Л. Гурский, Б. И. Беляев, О. Б. Зельманский, С. Н. Петров

Р е ц е н з е н т:
заведующий кафедрой систем и устройств телекоммуникаций
учреждения образования «Белорусский государственный университет
информатики и радиоэлектроники»,
доктор технических наук, профессор В. К. Конопелько

Компьютерные сети : метод. указания к лаб. работам для студ. спец. 1-45 01 03 «Сети телекоммуникаций», 1-98 01 02 «Защита информации в телекоммуникациях» всех форм обуч. / А. Л. Гурский [и др.]. – Минск : БГУИР, 2010. – 71 с. : ил.

К63

ISBN 978-985-488-490-5.

Содержат краткие теоретические сведения по основам построения и функционирования компьютерных сетей и работе с программой Paket Tracer 4.1 для симуляции работы сетей с оборудованием фирмы Cisco; задания к лабораторным работам по конфигурированию сети на примерах коммутационного оборудования фирмы Cisco и список литературы.

УДК 004.71(076.5)
ББК 32.973.202я73

ISBN 978-985-488-490-5

СОДЕРЖАНИЕ

Лабораторная работа №1

ЭТАЛОННАЯ МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ ОТКРЫТЫХ СИСТЕМ

Цель работы: ознакомиться с моделью взаимодействия открытых систем (OSI), программным пакетом Packet Tracer 4.1, а также изучить работу устройств 1-го и 2-го уровней.

1.1. Теоретические сведения

Реализация сетевого проекта – достаточно сложный процесс. Для его упрощения вся система сетевой коммуникации разделяется на уровни. При этом каждый уровень отвечает за определенную часть процесса коммуникации и взаимодействует только с ниже- и вышестоящими уровнями. Такое взаимодействие строго определяет назначение каждого уровня. Основной сетевой моделью является *эталонная модель взаимодействия открытых систем* (Open System Interconnection – OSI).

Эталонная модель OSI является первичной моделью, используемой в качестве основы для сетевых коммуникаций. Она определяет сетевые функции каждого уровня. Модель OSI описывает, каким образом информация перемещается между приложениями по передающим средам разных видов.

Эталонная модель OSI содержит семь пронумерованных уровней, на каждый из которых возлагаются свои функции в сети:

- уровень 1 – физический уровень;
- уровень 2 – канальный уровень;
- уровень 3 – сетевой уровень;
- уровень 4 – транспортный уровень;
- уровень 5 – сеансовый уровень;
- уровень 6 – уровень представления данных;
- уровень 7 – уровень приложений.

Такое разделение обеспечивает следующие преимущества:

- процесс сетевой коммуникации подразделяется на меньшие, более простые этапы;
- стандартизируются сетевые компоненты, что позволяет использовать и поддерживать в сети оборудование разных производителей;
- осуществляется связь между различными типами аппаратного и программного обеспечения;
- изменения на одном уровне не влияют на функционирование других уровней, что позволяет быстрее разрабатывать новые программные и аппаратные продукты.

Уровень 1 – физический уровень (physical layer)

Уровень определяет электрические, процедурные и функциональные спецификации для активизации, поддержки и отключения физических каналов между оконечными системами. Спецификациями физического уровня определяются уровни напряжений, синхронизация изменений напряжения, физическая скорость и максимальная дальность передачи данных, физические соединения и другие аналогичные параметры.

Уровень 2 – канальный уровень (data link layer)

Уровень обеспечивает надежную передачу данных по физическому каналу. При этом канальный уровень решает задачи физической (в противоположность логической) адресации, анализа сетевой топологии, доступа к сети, уведомления об ошибках, упорядоченной доставки кадров (фреймов, пакетов) и управления потоками.

Уровень 3 – сетевой уровень (network layer)

Сетевой уровень является комплексным уровнем, обеспечивающим выбор маршрута и соединение между собой двух рабочих станций, которые могут быть расположены в географически удаленных друг от друга сетях. Кроме того, сетевой уровень решает вопросы логической адресации. Примерами протоколов третьего уровня могут служить межсетевой протокол (Internet-protocol – IP), протокол межсетевого пакетного обмена (Internetwork Packet Exchange – IPX) и протокол AppleTalk.

Уровень 4 – транспортный уровень (transport layer)

Транспортный уровень сегментирует данные передающей станции и вновь собирает их в одно целое на принимающей стороне; организует службу передачи данных таким образом, чтобы скрыть от верхних уровней детали процесса передачи данных. Следовательно, задачей транспортного уровня является обеспечение надежности передачи данных между двумя рабочими станциями. При организации службы связи данных уровень устанавливает, поддерживает и соответствующим образом ликвидирует виртуальные каналы. Для обеспечения надежности службы связи используются выявление ошибок при передаче и управление информационными потоками. Примерами протоколов четвертого уровня могут служить протокол управления передачей (Transmission Control Protocol – TCP), протокол пользовательских дейтаграмм (User Datagram Protocol – UDP) и протокол последовательного обмена пакетами (Sequenced Packet Exchange – SPX).

Уровень 5 – сеансовый уровень (session layer)

Сеансовый уровень устанавливает, управляет и разрывает сеанс связи между двумя рабочими станциями, предоставляет свои службы уровню представления данных. Таким образом, данный уровень синхронизирует диалог между уровнями представления двух систем и управляет обменом данными. Кроме своей основной постоянной функции – управления, сеансовый уровень

обеспечивает эффективную передачу данных, требуемый класс обслуживания и рассылку экстренных сообщений о наличии проблем на данном уровне, уровне представления данных или уровне приложений. Примерами протоколов пятого уровня могут служить сетевая файловая система (Network File System – NFS), система X-Windows и протокол сеанса AppleTalk (AppleTalk Session Protocol –ASP).

Уровень 6 – уровень представления данных (presentation layer)

Задача уровня представления данных состоит в том, чтобы информация уровня приложений, которую посылает система отправителя, могла быть прочитана уровнем приложений системы получателя. При необходимости уровень представления преобразует данные в один из многочисленных форматов, который поддерживается обеими системами. Другой важной задачей этого уровня является шифрование и расшифровка данных. Примерами стандартов шестого уровня эталонной модели, описывающих формат представления звука и видео, являются стандарты MIDI и MPEG, а графику – PICT, TIFF и JPEG.

Уровень 7 – уровень приложений (application layer)

Уровень приложений является ближайшим к пользователю и предоставляет службы его приложениям. От других уровней он отличается тем, что не предоставляет служб другим уровням; вместо этого он предоставляет службы только приложениям, которые находятся вне рамок эталонной модели OSI. Примерами подобных приложений могут служить электронные таблицы или текстовые редакторы. Уровень приложений определяет доступность партнеров по сеансу связи друг для друга, а также синхронизирует связь и устанавливает соглашение о процедурах восстановления данных в случае ошибок и о процедурах контроля целостности данных. Примерами приложений седьмого уровня могут служить протоколы Telnet и HTTP.

Для передачи данных необходимо установить соединение между однотипными уровнями сети (одноранговая связь). Во время этого процесса протоколы одного и того же уровня обеих систем обмениваются информацией, называемой *протокольными единицами обмена* (Protocol Data Unit – PDU).

Пакеты данных создаются станцией-отправителем, а затем передаются в пункт назначения. Функционирование каждого уровня зависит от службы, предоставляемой уровнем модели OSI, лежащим непосредственно под ним. Для предоставления такой службы нижний уровень использует *инкапсуляцию*, которая заключается в размещении модуля PDU вышестоящего уровня в поле данных своего модуля PDU. После этого каждый уровень может добавить заголовки, которые требуются ему для выполнения своих функций. По мере того как данные передаются по уровням модели OSI, к ним добавляются дополнительные заголовки. Модуль данных протокола (PDU) на четвертом уровне называется *сегментом* (segment).

Сетевой уровень предоставляет службы транспортному уровню. Он обеспечивает передачу данных по объединенной сети путем инкапсуляции данных транспортного уровня и добавления заголовка, в результате чего создается *пакет* (packet), являющийся модулем PDU третьего уровня. Заголовок пакета содержит информацию, требуемую для передачи пакета по сети, такую, в частности, как логические адреса отправителя и получателя. Канальный уровень предоставляет службы сетевому уровню. Он инкапсулирует информацию сетевого уровня во *фрейм* (frame), являющийся модулем PDU второго уровня. Заголовок фрейма содержит физический адрес, требуемый для выполнения канальным уровнем своих функций, а *концевик* (trailer) содержит контрольную последовательность фрейма (Frame Check Sequence – FCS), которая используется для проверки того, не был ли поврежден фрейм в процессе передачи. Полученный модуль данных передается вниз, на физический уровень, предоставляющий службы канальному уровню. Физический уровень кодирует фрейм канального уровня, превращая его в последовательность битов для передачи по сетевой среде (обычно по проводу) на первом уровне.

Процесс *инкапсуляции* включает несколько этапов:

1. Первоначальное формирование данных.
2. Упаковка данных для сквозной передачи по сети.
3. Добавление в заголовок сетевого адреса. Данные помещаются в пакеты или дейтаграммы, содержащие сетевой заголовок, в котором расположены логические адреса источника и получателя для пересылки пакета по сети в соответствии с выбранным маршрутом.
4. Добавление локального адреса в заголовок канального уровня. Каждое сетевое устройство должно поместить пакет сетевого уровня во фрейм канального уровня. Преобразование пакета во фрейм позволяет осуществить соединение со следующим, лежащим на данном маршруте, непосредственно подсоединенным сетевым устройством.
5. Преобразование в биты для передачи по сети. Функция синхронизации позволяет устройствам различать передаваемые биты при их передаче по сети. Заголовки и концевики добавляются по мере того, как данные перемещаются по уровням модели OSI.

Когда удаленное устройство получает последовательность битов, его физический уровень передает эти биты на канальный уровень для дальнейшей обработки (*декапсуляция*). Канальный уровень выполняет следующие действия:

1. Проверяет, соответствует ли MAC-адрес пункта назначения адресу этой станции и не является ли он широковещательным адресом. Если ни одно из условий не выполняется, фрейм отбрасывается.
2. Запрашивает повторную передачу данных, если данные отброшены из-за содержащихся в них ошибок.
3. Удаляет заголовок и концевик канального уровня, а затем передает оставшиеся данные на сетевой уровень, основываясь на управляющей информации, содержащейся в заголовке канального уровня.

Оборудование 1-го уровня. Одной из основных задач, которая стоит перед любой технологией транспортировки данных, является их передача на максимально большое расстояние. Физическая среда накладывает на этот процесс свое ограничение в виде затухания сигнала. Используемое в аналоговых системах усиление не годится для высокочастотных цифровых сигналов. В таких ситуациях применяют не усиление, а *повторение* сигнала. При этом устройство на входе должно принимать сигнал, распознавать его первоначальный вид и генерировать на выходе его точное подобие.

Первоначально в сетях стандарта Ethernet с топологией «шина» использовался коаксиальный кабель, соединенный через двухпортовый *повторитель* (repeater). Позже появились многопортовые устройства, называемые *концентраторами* (hub). Концентратор – многопортовый повторитель, соединяющий несколько физических сегментов. В то время как типичный повторитель имеет только два порта, концентратор обычно имеет от 4 до 24 портов. Использование концентратора преобразует сетевую топологию из шинной в звездообразную, оставляя неизменной логическую топологию, увеличивает надежность сети.

Концентраторы принадлежат к одному из трех типов:

- *активный концентратор* должен быть подключен к источнику внешнего питания, поскольку ему нужна энергия для усиления входящего сигнала перед передачей его на внешние порты;
- *интеллектуальный концентратор* (smart hub) в целом функционирует как обычный концентратор, однако имеет встроенный микропроцессор и обладает возможностями диагностики;
- *пассивный концентратор* выступает исключительно в качестве точки физического соединения устройств. Такой концентратор не проверяет проходящий через него трафик и не выполняет никаких действий с потоками данных; он не усиливает и не очищает сигнал. Пассивный концентратор только предоставляет доступ к общей шине и поэтому не требует наличия источника питания.

Оборудование 2-го уровня. *Мосты* (Bridge), как и повторители, принимают данные на входящий порт и передают на исходящий с восстановленным уровнем и формой сигнала (рис. 1.1).

Мост принимает входящий кадр в свой буфер, определяет его целостность и MAC-адрес назначения. При этом каждая половина моста, анализируя поле адреса отправителя, ведет таблицу Ethernet-адресов узлов, находящихся на своей стороне. На другую сторону моста передаются только кадры *широковещательной рассылки* (Broadcast) и кадры, не имеющие получателя на своей стороне (для исключения коллизий при передаче данных).

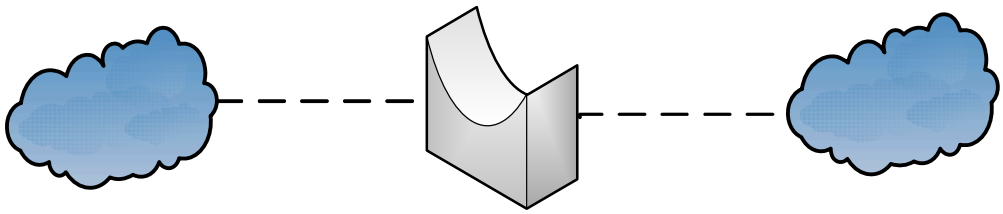

Рис. 1.1. Соединение двух сегментов сети с помощью моста в программной среде

Буферизация данных (store-and-forward) перед их отправкой приводит к возникновению большей по сравнению с концентраторами задержки, что несколько снижает скорость работы сети. Однако количество устройств, которые разделяют между собой физическую среду, снижается, что приводит к увеличению реальной скорости передачи данных.

Мосты не могут выполнять фрагментации и повторной сборки пакетов более высокого (сетевого) уровня. Из этого следует, что при наличии ограничения на размер передаваемого кадра, слишком большой кадр может быть отброшен как поврежденный.

Коммутатор (switch) представляет собой сетевое устройство 2-го уровня, которое выполняет функции *точки концентрации* для соединения между собой *рабочих станций*, *серверов*, *маршрутизаторов*, *концентраторов* и других коммутаторов (рис. 1.2). Коммутаторы можно рассматривать как многопортовые мосты, которые организуют выделенные виртуальные каналы типа «точка – точка» между каждыми двумя подсоединенными сетевыми устройствами, поэтому при одновременной передаче коллизий не происходит. Коммутаторы могут работать в *дуплексном режиме*.

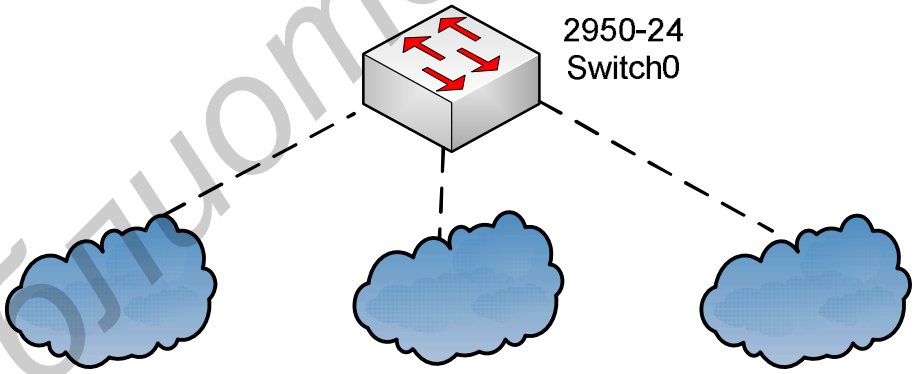

Рис. 1.2. Соединение сегментов сети с помощью коммутатора в программной среде

1.2. Задание для лабораторной работы

Ознакомиться с пользовательским интерфейсом программы Packet Tracer 4.1, с ее службой справки; провести первичную настройку шести компьютеров сети: PC0, PC1, PC2, PC3, PC4, PC5, соединенных коммутатором Switch0 и концентратором Hub0 через мост Bridge0. В сети есть выход в Интернет через маршрутизатор Router0. Логическая схема сети представлена на рис. 1.3.

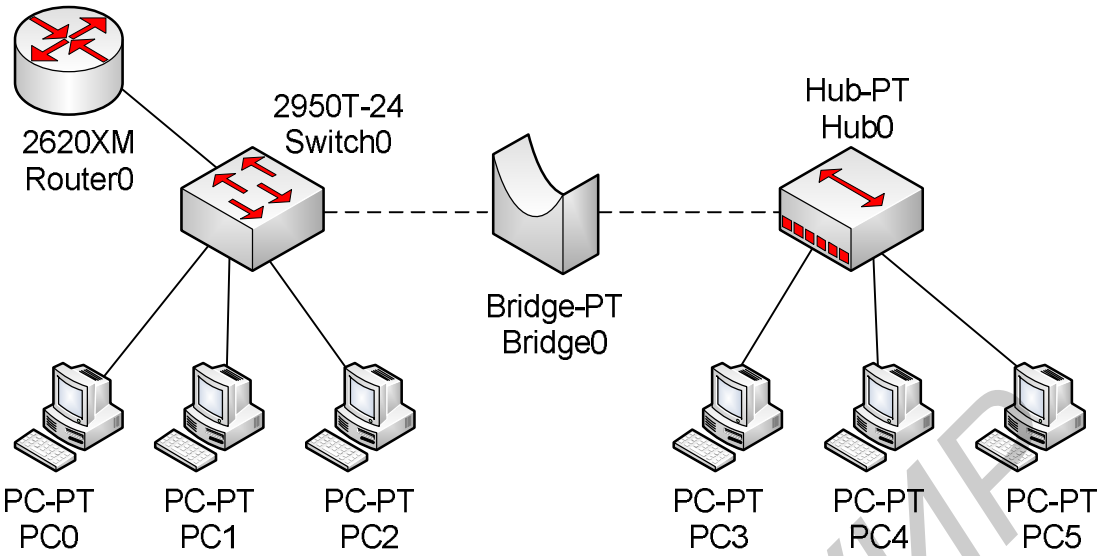

Рис. 1.3. Логическая схема учебной сети

1.3. Содержание отчета

1. Цель работы.
2. Схема топологии сети.
3. Пример конфигурации компьютеров.
4. Выводы.

1.4. Контрольные вопросы

1. Сколько уровней имеет эталонная модель OSI?
2. Назовите уровни модели OSI. Каковы их функции?
3. Что такое инкапсуляция и декапсуляция?
4. Какие этапы включают процессы инкапсуляции и декапсуляции?
5. К оборудованию какого уровня относятся концентраторы?

Лабораторная работа №2

ОБОРУДОВАНИЕ 3-ГО УРОВНЯ. МАРШРУТИЗАТОРЫ. ВИД И НАЗНАЧЕНИЕ ОСНОВНЫХ ЭЛЕМЕНТОВ. ТИПЫ ПАМЯТИ И ПОСЛЕДОВАТЕЛЬНОСТЬ ЗАГРУЗКИ. ОСУЩЕСТВЛЕНИЕ КОНСОЛЬНОГО СОЕДИНЕНИЯ

Цель работы: ознакомиться с оборудованием 3-го уровня. Получить практические навыки в осуществлении консольного соединения.

2.1. Теоретические сведения

Сетевой уровень (network layer) является комплексным уровнем, обеспечивающим выбор маршрута и соединение между собой двух рабочих станций, которые могут быть расположены в географически удаленных друг от друга сетях. Кроме того, сетевой уровень решает вопросы логической адресации (например по IP-адресу). Для реализации данной процедуры используются *маршрутизаторы* (Router).

Маршрутизатор может рассматриваться как специализированный тип компьютера. Он содержит те же компоненты, что и обычный ПК. Маршрутизатор управляется специальной операционной системой (например Cisco IOS (Internetwork Operating System)), которая используется для интерпретации *конфигурационных файлов*, содержащих параметры и инструкции по управлению потоками исходящих и входящих данных. *Файлы конфигурации* содержат всю необходимую для работы устройства информацию. В маршрутизаторах Cisco с операционной системой Cisco IOS существуют два конфигурационных файла: *стартовый* и *рабочий* (текущий) (startup-config и running-config).

Основное назначение маршрутизаторов – объединение сетей в единую распределенную сеть и определение маршрутов потоков данных между подключенными к устройству сетями. Их также можно использовать и для сегментации локальных сетей.

Маршрутизаторы обеспечивают:

- выбор оптимального маршрута для входящих пакетов данных;
- передачу пакетов соответствующим исходящим интерфейсам.

К основным компонентам маршрутизатора относятся: оперативная память (RAM/DRAM), энергонезависимая память (NVRAM), Flash-память, постоянное запоминающее устройство (ROM) и интерфейсы.

Оперативная память (RAM/DRAM):

- используется для хранения таблиц маршрутизации;
- хранит кэш протокола ARP;
- содержит быстродействующий кэш;
- отвечает за буферизацию пакетов (разделяемая оперативная память);
- обеспечивает хранение пакетов;

- обеспечивает временную и рабочую память для файлов конфигурации маршрутизатора при включенном питании.

Содержимое RAM-памяти теряется после выключения питания или перезагрузки устройства.

Энергонезависимая память (NVRAM) содержит резервную, или стартовую, копию файла конфигурации. При перезагрузке или после выключения данные в этой памяти не стираются.

Flash-память – стираемая перепрограммируемая память, которая обычно работает только в режиме чтения (EPROM):

- содержит образ операционной системы и микрокод;
- позволяет обновлять программное обеспечение без извлечения и перемещения чипа на процессоре;
- содержит данные, которые при перезагрузке или завершении работы маршрутизатора не удаляются.

Во Flash-памяти может быть сохранено несколько версий операционной системы.

Постоянное запоминающее устройство (ROM):

- содержит код команд самотестирования при включении питания (Power-On Self Test – POST);
- содержит программы начальной загрузки и основное программное обеспечение операционной системы.

Для обновления программного обеспечения в ROM требуется замена подключаемого чипа на системной плате устройства.

Интерфейс – сетевое соединение, через которое пакеты данных передаются от маршрутизатора к устройству. Размещается на системной плате или в отдельном модуле.

Существует три типа разъемов в маршрутизаторах: *интерфейсы локальных сетей*, *интерфейсы распределенных сетей* и *порты управления* (рис. 2.1).

Интерфейсы локальных сетей позволяют маршрутизатору соединяться со средой локальной сети – обычно это одна из форм среды Ethernet.

Интерфейсы распределенных сетей обеспечивают подключение к удаленным узлам или к сети Internet через сеть провайдера. При использовании некоторых типов интерфейсов распределенных сетей для подключения маршрутизатора к местной службе провайдера услуг необходимы внешние устройства, такие как CSU/DSU. Некоторые разновидности соединения распределенных сетей позволяют подключить маршрутизатор непосредственно к оборудованию поставщика услуг. Интерфейсы локальных и распределенных сетей обеспечивают сетевое взаимодействие, посредством которого передаются пакеты данных.

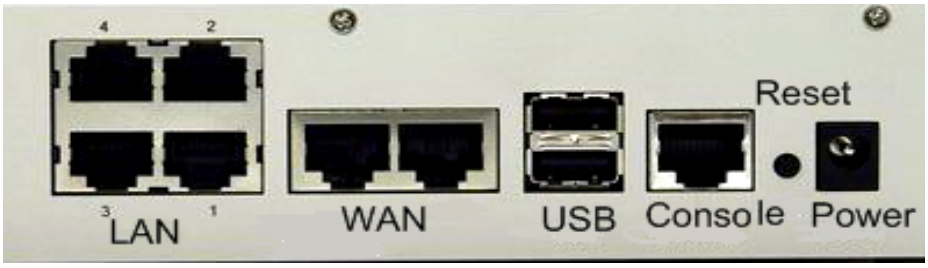

Рис. 2.1. Внешние порты маршрутизатора

Порт управления обеспечивает соединение маршрутизатора и терминального устройства, по которому передается текстовая информация, используемая для конфигурирования и исправления ошибок в работе устройства. Наиболее часто используемые интерфейсы управления – *консоль* и *вспомогательные порты* (AUX). Они представляют собой последовательные асинхронные порты RS-232, которые подсоединяются к коммуникационным портам ПК. Эти асинхронные последовательные порты не предназначены для использования в качестве сетевых. Для начальной конфигурации маршрутизатора требуется использовать один из них.

При первом включении маршрутизатора в нем не настроены сетевые параметры, устройство не способно взаимодействовать с сетями. Для его настройки следует ввести команды конфигурации путем подсоединения ASCII-терминала (или его эмуляции в случае использования ПК в качестве терминала) к порту RS-232. После того как маршрутизатор будет настроен, его можно подключать к сети для устранения неполадок или мониторинга.

Программное обеспечение ПК или алфавитно-цифровой терминал должен поддерживать режим работы или эмуляцию режима vt100 (ранее широко используемый тип видеотерминала и соответствующий протокол связи с ним). Программное обеспечение эмуляции терминала, пакет HyperTerminal, входит в стандартную поставку ОС Windows.

Для поиска и устранения неисправностей предпочтительнее использовать порт консоли. Чтобы подключиться к консольному порту, необходимо использовать консольный кабель и адаптер для разъема RJ-45 на разъем DB-95 для подключения к ПК.

Для подключения персонального компьютера к консольному порту необходимо:

1. Подключить разъем RJ-45 консольного кабеля к консольному порту.
2. Подключить второй разъем RJ-45 кабеля к переходнику DB-9.
3. Подключить переходник DB-9 к COM-порту ПК.
4. Осуществить настройку программы эмуляции терминала ПК:
   - указать соответствующий COM-порт;
   - установить скорость 9600 бод;
   - установить режим «восемь битов данных в посылке»;
   - указать отсутствие проверки четности (no parity);
   - установить использование одного стопового бита;
   - указать отсутствие механизма управления потоком.

Подключение через интерфейсы локальных сетей. К большинству сред локальных сетей маршрутизаторы подключаются посредством соединений Ethernet или Fast Ethernet. В этом случае маршрутизатор является узлом, который подключен к сети LAN посредством коммутатора или концентратора; для такого подключения используется кабель с прямой распайкой контактов. Интерфейс 10/100BASE-TX маршрутизатора должен быть подключен как минимум неэкранированной витой парой категории 5 (UTP) к любому другому устройству независимо от типа маршрутизатора, как показано на рис. 2.2.

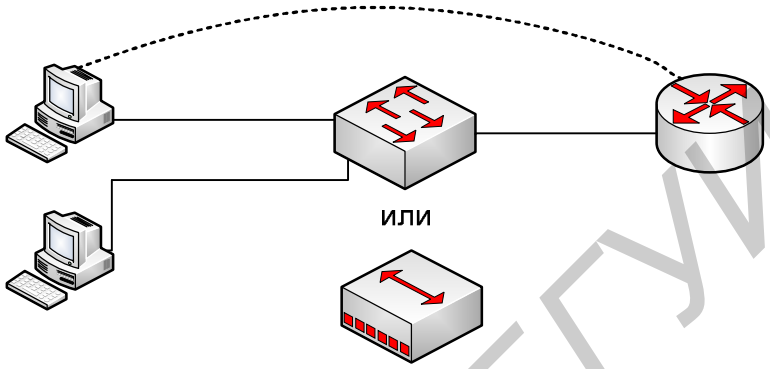

Рис. 2.2. Подключение маршрутизатора посредством неэкранированной витой пары

В некоторых случаях Ethernet-интерфейс устройства необходимо будет подключить напрямую к такому же интерфейсу маршрутизатора или непосредственно к сетевой плате персонального компьютера. В этом случае следует использовать *перекрещенный кабель* (crossover).

В любом соединении необходимо обращать внимание на тип интерфейса. Если для подключения будет использован неподходящий интерфейс, то может пострадать сам маршрутизатор и другое сетевое оборудование. Во многих портах или в различных типах соединений используются одинаковые разъемы, например, для Ethernet, ISDN-BRI, консольных, AUX-портов, интегрированных CSU/DSU и Token Ring-портов используется один и тот же восьмиконтактный разъем – RJ-45, RJ-48 или RJ-49. Для разных типов интерфейсов используются также специальные разноцветные метки.

Существует много вариантов соединений распределенных сетей, поскольку сами WAN-сети служат для объединения телекоммуникационных структур на большой географической площади посредством разнообразных технологий. Некоторые типы соединений показаны на рис. 2.3: выделенные линии, соединения с коммутацией каналов и соединения с коммутацией пакетов.

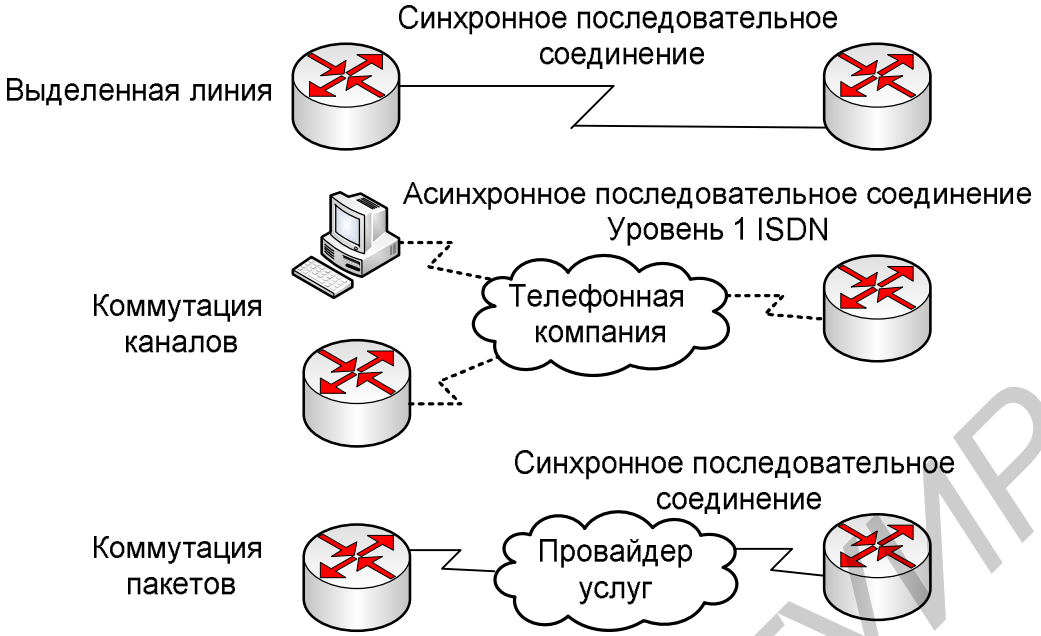

Рис. 2.3. Различные типы соединений распределенных сетей

В каждой разновидности службы WAN-сети оборудование пользователя, которым обычно является маршрутизатор, работает в качестве терминального (DTE). Оно подключено к среде провайдера службы посредством оборудования линии передачи данных (Data Circuit-terminating Equipment – DCE), в качестве которого обычно выступает либо модем, либо устройство CSU/DSU. DCE-устройство конвертирует сигналы от DTE-устройства в форму, приемлемую для линии провайдера WAN-служб.

Конфигурирование маршрутизатора. Чтобы получить доступ к маршрутизатору, необходимо иметь соответствующую учетную запись. После того как администратор получил доступ к интерфейсу устройства, он может войти в один из возможных режимов конфигурирования, используя *интерфейс командной строки*.

Интерфейс командной строки имеет иерархическую структуру. Для выполнения различных задач эта структура требует перехода в разные режимы. Например, для настройки интерфейсов машрутизатора необходимо войти в режим конфигурирования интерфейсов. В режиме настройки интерфейса администратор может изменять только настройки интерфейсов. В разных режимах маршрутизатора командная строка имеет различные метки приглашения командной строки, что позволяет не путать режимы и использовать только команды, присущие текущему режиму.

ОС IOS обеспечивает работу интерпретатора команд (EXEC), который проверяет и выполняет все команды, введенные с консоли.

В целях безопасности в ОС IOS EXEC-сеансы разделены на два уровня доступа: *пользовательский* EXEC-режим и *привилегированный* EXEC-режим, которые еще называют режимами допуска.

В пользовательском режиме (режим просмотра) доступен ограниченный набор основных команд, которые позволяют отследить режимы работы мар-

шрутизатора. Данный режим не допускает изменения файла конфигурации маршрутизатора; используется в основном для проведения мониторинга. В командной строке этот режим идентифицируется символом «>».

Для выполнения команд настройки и управления маршрутизатором системному администратору необходимо войти в привилегированный режим, который дает возможность использовать все команды маршрутизатора. Доступ к этому режиму только авторизированный (по паролю и логину). Кроме того, из привилегированного режима может быть получен доступ к режиму глобальной конфигурации и другим специальным режимам. В командной строке привилегированный режим идентифицируется символом «#».

Для перехода из пользовательского в привилегированный режим необходимо ввести команду enable в командной строке с приглашением, которое заканчивается символом «>». Если пароль был установлен, то для продолжения работы маршрутизатор его запросит. В целях безопасности сетевые устройства не отображают вводимые символы пароля. Если введенный пароль верен, то приглашение командной строки маршрутизатора изменяется на «#», и маршрутизатор входит в привилегированный EXEC-режим.

Введя символ «**?**» в привилегированном режиме, вы увидите список доступных команд; к некоторым из них можно получить доступ также из пользовательского режима.

Примеры команд пользовательского режима:

- enable – переключение режима;
- ping – послать echo сообщение;
- show – показать текущую информацию о системе.

Примеры некоторых команд привилегированного режима:

- configure – режим конфигурирования;
- dir – просмотр файла в файловой системе;
- disable – выход из привилегированного режима.

Режимы конфигурации маршрутизатора. Первый режим конфигурирования называется режимом глобальной конфигурации, настройки которого влияют на всю систему. Для входа в режим глобальной конфигурации используется команда привилегированного режима configure. После ввода этой команды будет запрошен источник команд конфигурации: можно будет выбрать терминал, энергонезависимое ОЗУ или сеть. Стандартно все команды конфигурации принимаются из консоли терминала.

Ниже приведены некоторые команды маршрутизатора, доступ к которым можно получить из режима глобальной конфигурации:

- enable – вход в привилегированный режим;
- exit – выход из режима конфигурации;
- ip – глобальные команды настройки IP.

Некоторые режимы конфигурирования, доступные в глобальном режиме:

- Router(config-if)# – режим конфигурирования интерфейсов;

- Router(config-line)# – режим конфигурирования линии;
- Router(config-router)# – режим конфигурирования маршрутизатора.

Для возврата маршрутизатора в режим глобальной конфигурации из любого подрежима используется команда exit. Нажав сочетание клавиш «Ctrl»+«Z», вы окончательно выйдете из режима конфигурации и попадете в привилегированный EXEC-режим.

Приведем пример переключения между различными режимами маршрутизатора:

```
Router# configure terminal
Router (config) #
!  далее можно ввести нужные команды
Router (config) # exit
Router#
Router#configure terminal
Router(config)# router protocol
Router(config-router)#
! далее можно ввести нужные команды
Router (config-router) # exit
```

Одной из основных задач, которую необходимо решить при установке маршрутизатора, является задание его имени. Имя маршрутизатора позволяет повысить удобство администрирования сети. Имя маршрутизатора задается в режиме настройки глобальной конфигурации (global configuration mode), оно называется именем узла (hostname) и отображается в системном приглашении командной строки. По умолчанию используется имя Router.

В маршрутизаторе существует большое количество типов команды show, которые позволяют просмотреть содержимое файлов; такие команды используются при решении проблем в работе маршрутизатора. В каждом из режимов команда «show ?» отображает допустимые параметры команды. Полный список команд приведен в табл. 4.2 лабораторной работы №4.

2.2. Задание для лабораторной работы

1. Ознакомьтесь с основными режимами конфигурирования маршрутизатора.
2. Сконфигурируйте маршрутизатор по схеме (рис. 2.4).
3. Ознакомьтесь с результатом выполнения команд show version, show flash.
4. Назначьте имя маршрутизатору – Router0.

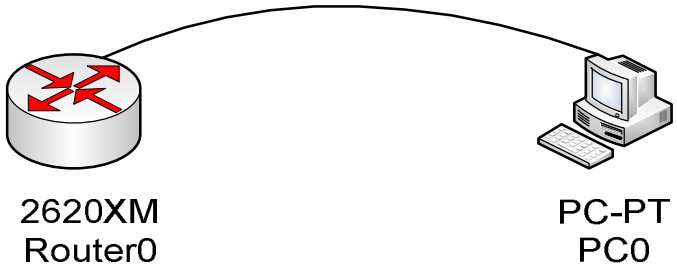

Рис. 2.4. Схема подключения к маршрутизатору для его конфигурирования

2.3. Содержание отчета

1. Цель работы.
2. Схема топологии сети.
3. Конфигурационные файлы маршрутизаторов.
4. Выводы.

2.4. Контрольные вопросы

1. К оборудованию какого уровня относятся маршрутизаторы?
2. Где в маршрутизаторе хранится информация о параметрах и инструкциях управления потоками данных?
3. Каково назначение маршрутизаторов?
4. Какие основные функции маршрутизаторов?
5. Какие основные компоненты маршрутизатора?
6. Какие типы интерфейсов маршрутизаторов вы знаете?
7. Что необходимо сделать для получения доступа к маршрутизатору?

Лабораторная работа №3

КОНФИГУРИРОВАНИЕ ИНТЕРФЕЙСОВ МАРШРУТИЗАТОРОВ. ТЕСТИРОВАНИЕ СОЕДИНЕНИЙ

Цель работы: научиться конфигурировать маршрутизаторы. Провести тестирование полученной сети на ошибки.

3.1. Теоретические сведения

Последовательный интерфейс маршрутизатора может быть настроен посредством консоли или через виртуальный терминал. Для управления синхронизацией соединения последовательному интерфейсу требуется синхронизирующий сигнал. В большинстве оборудования подача синхронизирующих сигналов обеспечивается самой аппаратурой передачи данных (DCE), такой, как устройство обслуживания канала (CSU) и пользовательское устройство, взаимодействующее с цифровым устройством (DSU). Стандартно такими устройствами являются маршрутизаторы Cisco и терминальное оборудование (DTE), которые могут быть настроены как DCE-устройства.

В последовательном соединении двух устройств одно из них должно быть объявлено DCE-устройством (т. е. передающим) и должно обеспечивать передачу синхронизирующих сигналов. Включение таймера синхронизации и его скорость задаются командой clockrate. Существуют следующие возможные скорости передачи в битах в секунду: 1200, 2400, 9600, 19 200, 38 400, 56 000, 64 000, 72 000, 125 000, 148 000, 500 000, 800 000, 1 000 000, 1 300 000, 2 000 000 и 4 000 000.

Для настройки последовательного интерфейса необходимо выполнить следующие действия:

1. Войти в режим глобальной конфигурации.
2. Войти в режим настройки требуемого интерфейса.
3. Сконфигурировать IP-адрес для интерфейса и маску подсети.
4. Указать полосу пропускания канала (необязательно).
5. Установить частоту синхронизирующих импульсов передающего (DCE) устройства (для принимающего устройства этого не требуется).
6. Включить интерфейс.

По умолчанию все интерфейсы отключены. Для включения интерфейса необходимо ввести команду no shutdown, для отключения – команду shutdown. Для выхода из текущего режима настройки интерфейса используется команда exit.

Ethernet-интерфейс маршрутизатора может быть настроен посредством консоли или через виртуальную терминальную линию. Каждый Ethernet-интерфейс должен иметь собственный IP-адрес и маску подсети.

Для настройки интерфейса Ethernet необходимо выполнить следующие действия (см. пример 3.1):

1. Войти в режим глобальной конфигурации.

2. Войти в режим настройки требуемого интерфейса.
3. Сконфигурировать IP-адрес для интерфейса и маску подсети.
4. Включить интерфейс.

Пример 3.1. Настройка Ethernet-интерфейса:

```
Router# configure terminal
Router(config)# interface e0
Router(config-if)#  ip address 192.168.1.150 255.255.255.128
Router(config-if)# no shutdown
```

Тестирование работоспособности соединений. Ниже приведены команды, которые могут использоваться для проверки соединения между сетевыми устройствами:

- ping;
- traceroute;
- show ip route;
- show interfaces serial;
- show interfaces/clear counter;
- debug.

Большинство сетевых протоколов поддерживает *эхопротокол*, который позволяет провести простейшую проверку сетевого соединения и проверить корректность маршрутизации сетевых пакетов.

Команда ping отправляет пакеты получателю и затем ждет ответных пакетов. Результаты работы такого эхопротокола могут помочь оценить надежность соединения, задержки передачи пакетов, а также работоспособность узла. Команда ping является основным механизмом тестирования соединения (как в пользовательском, так и в привилегированном режимах).

Для проверки соединения при помощи команды ping следует выполнить следующие действия:

1. Ввести команду ping [IP-address] или [name] получателя.
2. Нажать клавишу «Enter».

В табл. 3.1 приведены возможные значения, возвращаемые командой ping.

Команда traceroute (сокращенный вариант – trace) является удобным инструментом, который позволяет отследить отправителя и маршрут прохождения потока данных по сети. Команда traceroute похожа на команду ping, однако позволяет отследить не только состояние конечных точек маршрута, но и состояние каждого транзитного перехода пакетов в сети. Эта команда может быть выполнена как из пользовательского, так и из привилегированного EXEC-режимов.

Таблица 3.1

Таблица возвращаемых утилитой ping значений

Код	Значение	Возможная причина(ы)
!	Каждый восклицательный знак означает получение ICMP эхоответа	Пакет команды ping переслан успешно
.	Каждая точка означает, что истекло время ожидания ответа сетевым сервером	Может служить признаком одной из проблем: 1) команда ping блокируется списком управления доступом в маршрутизаторе; 2) маршрутизатор не нашел маршрута для доставки ICMP-сообщения; 3) на линии имеются физические неполадки соединения
U	Получено нераспознанное ICMP-сообщение	Маршрутизатор не может найти маршрута к адресу получателя
C	Отправитель сбрасывает полученные ICMP-пакеты и указывает на необходимость подавления отправителя трафика	Устройство на маршруте передачи (возможно, получатель) получило слишком много пакетов данных; проверьте статистику очередей пакетов
&	Истекло время существования ICMP-пакета	Возможно, пакет зациклился

Команда traceroute используется следующим образом:

1. Введите команду traceroute [IP-address] или [name] получателя.
2. Нажмите клавишу «Enter».

В табл. 3.2 представлены расшифровки кодов, возвращаемых командой traceroute, а на рис. 3.1 – схема проверки соединений с помощью этой команды.

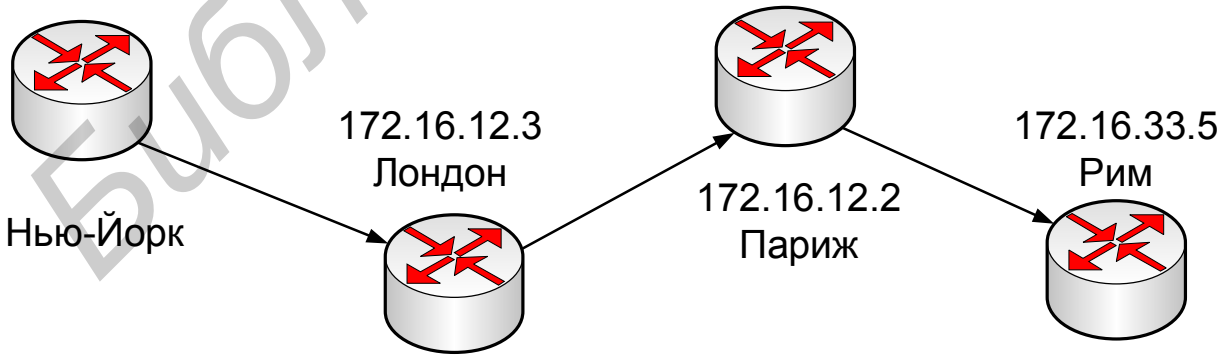

Рис. 3.1. Проверка соединения с помощью команды traceroute

Таблица 3.2

Таблица 3.2

Таблица возвращаемых утилитой traceroute значений

Код	Значение	Возможная причина(ы)
nn msec	Время передачи пакета (в миллисекундах) между узлами	Трассировка прошла успешно
*	Истекло время ожидания запроса	Тестируемое устройство не получило запроса или не ответило на ICMP-сообщение «packet life exceeded»
A	Пересылка пакетов административно запрещена	Устройство па маршруте, например, такое, как маршрутизатор или брандмауэр, блокирует пакеты команды traceroute
Q	Отправитель сбрасывает полученные ICMP-пакеты и требует подавление источника пакетов	Устройство на маршруте, возможно, получило слишком много пакетов, проверьте статистику очередей
H	Получено нераспознанное ICMP-сообщение	Возможно, произошло зацикливание

Команда traceroute использует сообщения об ошибках, генерируемые маршрутизаторами, когда истекает время жизни пакета (TTL) или превышается значение максимального числа переходов. Команда traceroute отправляет несколько ping-пакетов с увеличивающимся значением TTL и отображает время их прохождения. Одним из применений команды traceroute является поиск неисправного участка сети.

В маршрутизаторе имеются мощные инструменты для анализа работы сети. Для просмотра таблицы маршрутизации используется команда show ip route (пример 3.1).В примере 3.2 также показано, что сеть маршрутизатора Рим (131,108,33,0) доступна через интерфейс Ethernet1 (131.108.16.2) и сеть маршрутизатора Париж (см. рис. 3.1).

Пример 3.2. Выводимая командой show ip route информация

```
Paris# show ip route
Codes:    I – IGRP derived, R – RIP derived, O – OSPF derived
          C – connected, S – static, E – EGP derived, B – BGP derived
          i – IS-IS derived, D – EGRP derived
          * – candidate default  route, IA  – OSPF inter area route
          El – OSPF external  type 1  route, E2 – OSPF external  type 2
          route LI – IS-IS level-1 route, L2 – IS-IS  level-2 route
          EX – EIGRP external route
Gateway of  last resort  is not  set
I       144.253.0.0  [100/1300]  via  133.3.32.2  0:00:22  Ethernetl
131.108.0,0  is subnetted  (mask is 255.255.255.0),  3  subnets
I       131.108.33.0  (100/180771)  via 131.108.16.2,  0:01:29,  Ethernetl
C       131.108.12.0 is directly connected,  Ethernetl
C       101.108.16.0  is directly connected,  Ethernet0
I       219.100.103.0  ЦС0/1200)  via 133.3.32.2,  0:00:22,  Ethernetl
```

Протокол CDP (Cisco Discovery Protocol – протокол обнаружения устройств Cisco) помогает построить базовую схему структуры сети. Несмотря на то что этот протокол показывает информацию только о непосредственно подключенных к данному узлу соседних устройствах, он представляет собой мощное средство отладки сети.

Протокол CDP работает на канальном уровне. Получаемая информация включает в себя сведения о типах подключенных устройств; интерфейсах маршрутизатора, к которым соседние устройства подключены; интерфейсах, использующихся для создания соединений; а также моделях устройств. Протокол CDP не зависит от среды передачи и от протоколов, работает с любым оборудованием корпорации Cisco и в качестве своей основы использует *протокол доступа к подсети* (SNAP – Subnetwork Access Protocol). CDP является собственным протоколом сетевых устройств Cisco и работает только с сетевыми устройствами, выпущенными компанией Cisco.

Протокол CDP запускается автоматически при загрузке оборудования Cisco и позволяет сетевому устройству находить соседние узлы, на которых также запущен протокол CDP. Протокол позволяет двум системам получить информацию друг о друге даже в том случае, если они используют различные протоколы сетевого уровня.

Каждое устройство с настроенным протоколом CDP периодически отправляет сообщения, также известные как *анонсы* (advertisement), всем соседним устройствам. При помощи анонсов устройство сообщает другим устройствам по крайней мере об одном адресе, по которому оно способно получать сообщения протокола SNMP (Simple Network Management Protocol – простой протокол сетевого управления). В анонсах также содержится информация о времени жизни пакета (Time To Live – TTL) или времени удержания информации (holdtime). Последний параметр определяет время, в течение которого будет храниться CDP-информация, прежде чем она будет уничтожена. Также каждое сетевое устройство периодически получает CDP-сообщения, отправляемые другими соседними устройствами для получения информации о своих соседях.

Основной задачей протокола CDP является получение данных о платформах соседних устройств и об исполняемых ими протоколах. CDP-фрейм может быть небольшим, однако содержать массу полезной информации о соседних маршрутизаторах и коммутаторах.

В примере 3.3 приводится выводимая командой show cdp entry протокола CDP информация.

Пример 3.3. Использование команды *show cdp entry*

```
routerA# show cdp entry routerB
Device ID: routerB
Entry address (es)-.
IP address: 198.92.68.18
```

Platform: 2501. Capabilities: Router
Interface: Ethernet), Port ID {outgoing port): EthernetO
Holdtime: 155 sec

Примечание. В – параметр времени удержания информации. Определяет время, в течение которого хранится CDP-фрейм, полученный от соседнего устройства. Сжатую информацию о соседнем маршрутизаторе RouterB можно получить, введя команду show cdp entry (имя устройства). Информация о версии и параметрах соседних устройств упростит специалисту процесс определения физической топологии сети и поможет оптимально настроить устройства.

Каждый маршрутизатор, на котором исполняется протокол CDP, обменивается со своими соседями информацией обо всех известных ему протоколах. Администратор может посмотреть результаты этого обмена CDP-информацией посредством консоли, подсоединенной к локальному маршрутизатору (рис. 3.2).

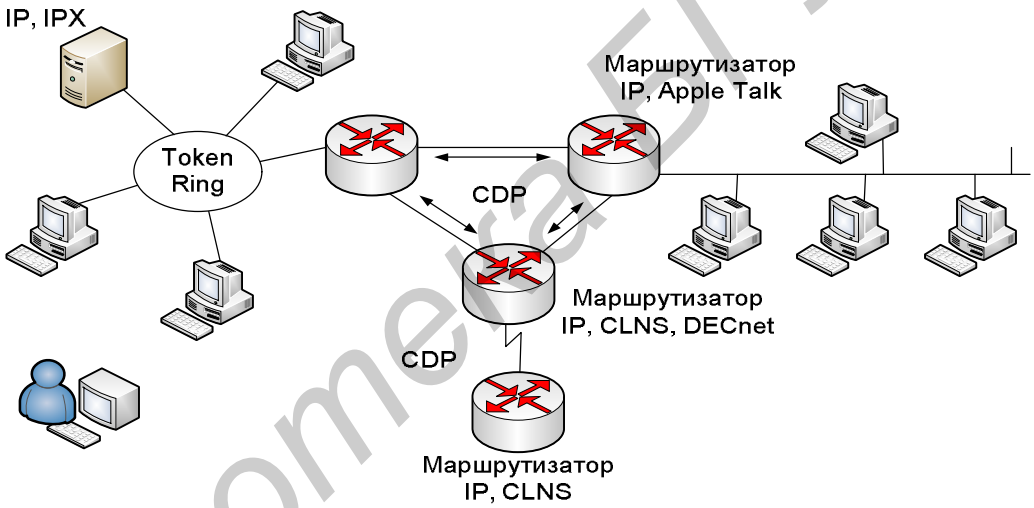

Рис. 3.2. Получение информации о соседних устройствах посредством CDP

Для отображения информации о сетях, непосредственно подсоединенных к маршрутизатору, можно воспользоваться командой show cdp neighbors (пример 3.4). Протокол CDP обеспечивает получение информации о каждом соседнем устройстве путем передачи информации в формате TLV (Type Length Value – тип – длина – значение).

Значения TVL включают в себя такую информацию:

- идентификатор устройства;
- номер и тип локального интерфейса;
- время удержания информации;
- возможности устройства 1;
- платформу;
- идентификатор порта;
- доменное имя VTP (только для протокола CDPv2);

- номер собственной сети VLAN (только для протокола CDPv2);
- информацию о дуплексности соединения (только для CDPv2).

Пример 3.4. Использование команды show cdp neighbors

```
routerA# show cdp neighbors
Capability Codes:
R – Router,   T – Trans  Bridge,
B – Source Route Bridge,
S  – Switch,   H – Host,    I – IGMP
Device ID    Local Interface    Holdtime    Capability    Platform    Port ID
routerB      Eth 0              151         R             2501        Eth  0
routerB      Ser 0              165         R             2501        Ser  0
```

Для отображения всей информации, выводимой командой show cdp neighbors, например как в случае команды show cdp entry, вы можете использовать указанную команду с дополнительным ключом show cdp neighbors detail. Все это позволяет создать карту сети объединенных устройств.

3.2. Задание для лабораторной работы

Каждому студенту дана сеть из трех маршрутизаторов. Задача – настроить интерфейсы на маршрутизаторах и протестировать соединения.

Router0:
Включите маршрутизатор.
Включите поддержку протокола CDP.
Сконфигурируйте интерфейс FastEthernet 0/0
IP = 192.168.1.1
NetMask = 255.255.255.0

Router1:
Включите маршрутизатор.
Включите поддержку протокола CDP.
Сконфигурируйте интерфейс FastEthernet 0/0
IP = 192.168.1.2
NetMask = 255.255.255.0
Сконфигурируйте интерфейс Serial 1/0
IP = 192.168.2.1
NetMask = 255.255.255.0
Протестируйте интерфейс на тип подключения. Если подключение DCE, сконфигурируйте Clock Rate = 56000

Router2:
Включите маршрутизатор.
Включите поддержку протокола CDP.
Сконфигурируйте интерфейс Serial 1/0
IP = 192.168.2.2
NetMask = 255.255.255.0

Протестируйте интерфейс на тип подключения, если подключение DCE, то сконфигурируйте Clock Rate = 56 000. Протестируйте соединения. Представьте результаты выполнения задания преподавателю.

3.3. Содержание отчета

1. Цель работы.
2. Схема топологии сети.
3. Конфигурационные файлы маршрутизаторов.
4. Выводы.

3.4. Контрольные вопросы

1. Что означают термины DTE, DCE, DSU, CSU?
2. Каков порядок настройки последовательного интерфейса маршрутизатора?
3. Как настроить Ethernet-интерфейс маршрутизатора?
4. Какие команды используются для тестирования работоспособности соединений?
5. Что такое протокол CDP и для чего он может быть использован?

Лабораторная работа №4

РАБОТА С КОНФИГУРАЦИЕЙ МАРШРУТИЗАТОРА. СОХРАНЕНИЕ РАБОЧЕЙ КОНФИГУРАЦИИ МАРШРУТИЗТОРА

Цель работы: научиться модифицировать настройки маршрутизаторов и сохранять конфигурационные файлы.

4.1. Теоретические сведения

Для внесения изменений в конфигурацию маршрутизатора необходимо войти в соответствующий режим и произвести эти изменения. Например, если какой-либо интерфейс отключен, то для его включения необходимо войти в режим глобальной конфигурации, затем – в режим настройки интерфейса и выполнить команду no shutdown.

Для проверки внесенных изменений используется команда show running-config. Эта команда отображает текущую конфигурацию. Если отображаемые значения переменных неверны, то для их изменения можно выполнить одно из следующих действий:

- использовать команды конфигурации с префиксом no;
- перезапустить систему и перезагрузить оригинальный конфигурационный файл из энергонезависимой памяти маршрутизатора;
- удалить файл начальной конфигурации при помощи команды erase startup-configuration, перезагрузить маршрутизатор и войти в режим установки.

Для сохранения значений конфигурационных переменных в энергонезависимом ОЗУ в привилегированном режиме служит команда copy running-config startup-config.

В табл. 4.1 приведен список команд, позволяющих управлять содержимым энергонезависимой памяти в операционной системе Cisco IOS версии I l.x и более поздних версий.

Таблица 4.1

Список команд конфигурации

Команда	Описание
configure memory	Загружает информацию о конфигурации из энергонезависимого ОЗУ (NVRAM)
erase startup-config	Очищает содержимое энергонезависимого ОЗУ (NVRAM)
copy running-config startup-config	Сохраняет текущую конфигурацию, находящуюся в ОЗУ (действующую конфигурацию) в энергонезависимое ОЗУ (загрузочную конфигурацию)
show startup-config	Отображает сохраненную конфигурацию, которая находится в энергонезависимом ОЗУ

Для защиты маршрутизатора от несанкционированного доступа используются пароли. Пароли могут быть установлены на доступ к виртуальной линии терминала, линии консоли, привилегированному EXEC-режиму.

Для ограничения доступа паролем к привилегированному режиму в режиме настройки глобальной конфигурации введите команду enable password. Этот пароль будет находиться в незашифрованном виде в конфигурационных файлах маршрутизатора. Для ввода пароля, который будет зашифрован, в привилегированном режиме введите команду enable secret. Если пароль будет задан этой командой, то он будет использоваться вместо пароля, задаваемого командой enable password.

Для задания пароля на вход в консоль терминала используется команда line console 0. Эту команду следует использовать в сети, в которой к маршрутизатору имеет доступ большое количество людей. Задание пароля на доступ к консоли терминала позволит предотвратить несанкционированный доступ к маршрутизатору.

Парольной защиты требует также и telnet-доступ. В разных аппаратных платформах используется различное количество линий. Так, диапазон от 0 до 4 задает пять линий, т.е. может быть установлено до пяти сеансов связи telnet. Для всех линий может быть задан один пароль или же для каждой линии его можно назначить индивидуально. Эта функция часто используется в больших сетях, обслуживаемых большим количеством сетевых администраторов. При возникновении в сети неразрешимых проблем и при всех занятых линиях доступа для восстановления может быть зарезервирована одна линия.

Для установки пароля к сеансу telnet-связи используется команда line vty 0 4. В примере 4.1 показаны различные пути настройки и защиты пароля.

Пример 4.1. Установка пароля

```
!  Пароль  консоли
Router(config)# line console 0
Router(config-line)#  login
Router(config-line)# password Cisco
!  Пароль виртуального терминала
Router(config)#  line vty 0 4
Router(config-line)# login
Router(config-line)# password Cisco
! Пароль для доступа к привилегированному режиму
Router(config)# enable password san-fran
! Шифрование пароля
Router(config)# enable secret [пароль]
! Шифрование всех паролей
Router(config)# service password-encryption
! Отмена шифрования всех паролей
Router(config)# no service password-encryption
```

Пароль, заданный командой enable secret, не может быть прочитан; другой пользователь, получивший доступ к файлам конфигурации, может лишь перезаписать его, но никак не прочитать, поскольку для хранения пароля используется необратимое одностороннее шифрование, что исключает восстановление пароля. Для запрета отображения пароля в виде открытого текста может быть использована команда service password-encryption. Ее следует вво-

дить в режиме глобальной конфигурации. Эта команда действует практически на все пароли за исключением того, который был указан с помощью команды enable secret, поскольку он и так уже зашифрован. Команда service password-encryption позволяет также зашифровать все другие пароли.

В маршрутизаторе существует большое количество вариантов использования команды show, которые позволяют просмотреть содержимое файлов. В каждом из режимов команда show отображает допустимые параметры команды. В табл. 4.2 приведены некоторые параметры этой команды.

Таблица 4.2

Команда show и ее параметры

Команда	Описание
show interfaces	Отображает статистику обо всех интерфейсах маршрутизатора. Если пользователю необходимо проанализировать статистические данные конкретного интерфейса, он может указать в команде show interfaces номер соответствующего интерфейса. Например: Router# show interfaces serial 1
show controllers serial	Отображает информацию об аппаратных средствах
show clock	Отображает время, которое установлено в маршрутизаторе
show hosts	Отображает список котированных имен узлов и адресов
show users	Отображает список пользователей, подключенных к маршрутизатору
show history	Отображает журнал введенных команд
show flash	Отображает информацию о Flash-памяти и о файлах операционной системы Cisco IOS, хранимых в ней
show version	Отображает информацию об образе операционной системы
show arp	Отображает ARP-таблицу маршрутизатора
show protocol	Отображает глобальное состояние и состояние интерфейсов любого настроенного протокола третьего уровня
show startup-configuration	Отображает конфигурацию, сохраненную в энергонезависимом ОЗУ (NVRAM)
show running-configuration	Отображает конфигурацию, которая в настоящее время находится в ОЗУ (RAM)

В примерах 4.2, 4.3 и 4.4 проиллюстрировано использование команд show protocol, show version и show interfaces.

Пример 4.2. Результат выполнения команды show protocol

```
Router# show protocols
Global values:
Internet Protocol  routing is enabled
DECnet routing  is enabled
XNS routing  is enabled
Vines routing  is enabled
AppleTalk routing is enabled
Novell  routing is enabled
--More--
Ethemet0 is up, line protocol is up
Internet address is 183.8.126.2, subnet mask is 255.255.255.128
DECnet cost is 5
XNS address is 3010.aaOO.0400.0284
CLNS enabled
Vines metric is 32
AppleTalk address is 3012.93, zone ld-eO
Novell address is 3010.aa00.0400.0284
--More--
```

Пример 4.3. Использование команды show version

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 4500 Software (C4500-J-M). Version 12.1.5
Copyright (c) 1986-1996 by Cisco Systems, Inc.
Compiled Fri 28-Jun-96 16:32 by rbeach
Image text-base: 0x600088A0, data-base: 0x6076E000
RCM: System Bootstrap. Version 5.1(1) RELEASE SOFTWARE (fcl)
ROM: 4500-XBOOT Bootstrap Software, Version 10.1(1) RELEASE SOFTWARE (fcl)
router uptime is 1 week, 3 days, 32 minutes
System restarted by reload
System image file is c4500-j-mz, booted via tftp from 171.69.1.129
--More--
```

Пример 4.4. Использование команды show interfaces

```
Router# show interfaces
Serial0 is up, line protocol is up
Hardware is MK5025
Internet address is 183.8.64.129, subnet mask is 255.255.255.128
MTU 1500 bytes, BW 56 kbit, DLY 20000 usec, rely 255/255. load 9/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 0:00:00, output 0:00:01, output hang never
Last clearing of show interfaces counters never
Output queue 0/40, 0 drops, input queue 0/75, 0 drops
Five minute input rate 1000 bits/sec, 0 packets/sec
331885 packets input, 62400237 bytes, no buffer
Received 230457 broadcasts, 0 runts, 0 giants
3 input errors, 3 CRC, 0 frame, 0 overrun, Oignored, 0 abort
403591 packets output, 66717279 bytes, 0 underruns
0 output errors, 0 collisions, 8 interface resets, 0 restarts    45 carrier transitions
```

4.2. Задание для лабораторной работы

Имеется небольшая сеть, состоящая из двух маршрутизаторов и двух компьютеров. Требуется настроить в ней удаленное управление всеми элементами.

Настройка маршрутизатора Router0:

1. Настройте интерфейс FE0/0 с IP 192.168.1.1 и маской 255.255.255.0;
2. Настройте интерфейс FE 0/1 с IP 192.168.0.1 и маской 255.255.255.0;
3. Настройте линии виртальных терминалов 0 – 4:
   – установите пароль cisco;
   – установите motd-banner;
   – установите пароль cisco на доступ к привилегированному режиму работы с маршрутизатором, примените к нему настройки шифрования;
4. Сохраните конфигурацию маршрутизатора.

Настройка маршрутизатора Router1:

1. Настройте интерфейс FE0/0 с IP 192.168.1.2 и маской 255.255.255.0;
2. Настройте интерфейс FE 0/1 с IP 192.168.2.1 и маской 255.255.255.0;
3. Настройте линии виртальных терминалов 0 – 4:
   – установите пароль cisco;
   – установите motd-banner;
   – установите пароль cisco на доступ к привилегированному режиму работы с маршрутизатором, примените к нему настройки шифрования;
4. Сохраните конфигурацию маршрутизатора.

Настройте ПК0: установите IP 192.168.x.x и маску 255.255.255.0.

Настройте ПК1: установите IP 192.168.x.x и маску 255.255.255.0.

Попробуйте установить telnet-соединение между компьютером ПК0 и маршрутизатором Router0, компьютером ПК1 и маршрутизатором Router 1, маршрутизаторами Router 1 и Router0 и наоборот. Покажите результат преподавателю.

4.3. Содержание отчета

1. Цель работы.
2. Схема топологии сети.
3. Конфигурационные файлы маршрутизаторов.
4. Выводы.

4.4. Контрольные вопросы

1. Что нужно сделать для внесения изменений в конфигурационные файлы маршрутизатора?
2. Как установить пароль для защиты маршрутизатора от несанкционированного доступа?
3. Какие различают команды группы show и каковы их функции?

Лабораторная работа №5

IP-АДРЕСАЦИЯ. ДЕЛЕНИЕ СЕТЕЙ НА ПОДСЕТИ

Цель работы: изучить общие принципы IP-адресации и классы IP-адресов. Получить практические навыки в делении сетей на подсети.

5.1. Теоретические сведения

Сетевой уровень отвечает за перемещение данных по сети, т. е. его задача заключается в нахождении наилучшего маршрута. Устройства используют схему адресации сетевого уровня для определения адреса пункта назначения информации при ее передаче по сети.

Чтобы любые две системы могли взаимодействовать между собой, они должны иметь возможность однозначно идентифицировать друг друга. В повседневной жизни имена или номера (например телефонов) часто используются в качестве уникальных идентификаторов. Аналогично этому каждый компьютер в TCP/IP-сети обязан иметь как минимум один уникальный идентификатор или адрес. Такой адрес (IP-адрес) позволяет одному компьютеру в сети находить другой.

Компьютеры хранят IP-адрес (рис. 5.1) в виде 32-битовой последовательности единиц и нулей. IP-адрес состоит из двух логических частей – номера сети и номера узла в сети. Для простоты использования IP-адрес обычно записывается в виде четырех десятичных номеров (частей), разделенных точками. Предположим, адрес одного из компьютеров – 192.168.1.2. Данный способ написания адреса называется *точечно-десятичным форматом.* Каждая из частей называется *октетом,* поскольку состоит из восьми двоичных цифр. Например, адресу 192.168.1.8 соответствует запись 11000000.10101000.00000001.00001000 в двоичном представлении. Точечно-десятичный формат позволяет намного быстрее различить цифровые составляющие адреса. И двоичный, и десятичный номера на рисунке (см. рис. 5.1) соответствуют одному и тому же адресу, но в десятичном формате он выглядит намного проще и короче. Этот формат помогает избежать ошибок вследствие перестановки цифр, что часто случается при использовании двоичных номеров.

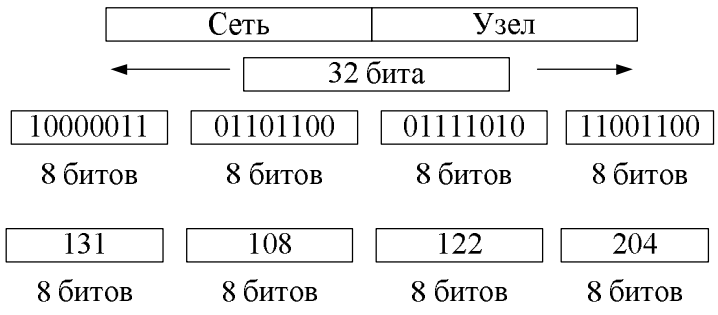

Рис. 5.1. Двоичный и десятичный формат IP-адреса

Намного проще увидеть связь между такими двумя номерами 192.168.1.8 и 192.168.1.9, чем распознать ту же связь в двоичных эквивалентах тех же адресов: 11000000.10101000.00000001.00001000 и 11000000.10101000.00000001.00001001.

Классы адресов. Адреса класса А (рис. 5.2) предназначены для очень больших сетей. В адресе класса А в качестве идентификатора сети используется только первый октет. Оставшиеся три октета выделены для перечисления адресов узлов.

Первый бит в адресе класса А всегда равен 0. С учетом этого наименьшее допустимое число будет равно 00000000_2 (0_{10}), а наибольшее – 01111111_2 (число 127_{10}). Следует заметить, что оба номера, 0 и 127, являются зарезервированными и не могут быть использованы в качестве сетевых адресов. Любые адреса, начинающиеся с числа в диапазоне от 1 до 126 в первом октете, являются адресами класса А.

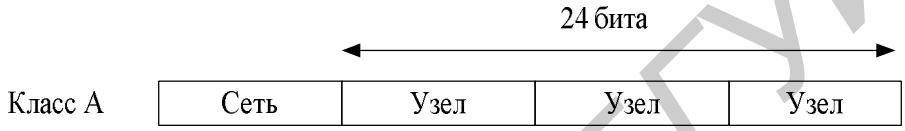

Рис. 5.2. Адреса класса А

Адреса класса В используются для сетей среднего и крупного размера (рис. 5.3). В IP-адресе класса В используются два первых октета для сетевого адреса. Оставшиеся два октета представляют адрес узла.

Рис. 5.3. Адреса класса В

Первые два бита первого октета всегда равны 10, оставшиеся шесть битов могут содержать любые комбинации нулей и единиц. Таким образом, наименьшее число, которое может быть использовано для адресов этого класса, равно 10000000_2 (128_{10}), а наибольшее – 10111111_2 (191_{10}). Любые адреса, содержащие в первом октете числа от 128 до 191, являются адресами класса В.

Адреса класса С (рис. 5.4) – это наиболее используемый класс адресов, применяемый в малых сетях.

Рис. 5.4. Адреса класса С

Адрес этого класса начинается с двоичной комбинации 110. Таким образом, наименьшее допустимое число – 11000000_2 (192_{10}), а наибольшее –

11011111_2 (223_{10}). Если адрес в первом октете содержит числа от 192 до 223, значит, он относится к классу C.

Адреса класса D (рис. 5.5) были созданы для реализации в IP-адресах механизма *многоадресатной* рассылки. Многоадресатным, или *групповым, адресом* (multicast address) называется уникальный сетевой адрес, используемый для отправки пакетов, содержащих адрес рассматриваемого класса в поле получателя, предопределенным группам сетевых устройств. Таким образом, одна сетевая станция передает один поток данных нескольким получателям.

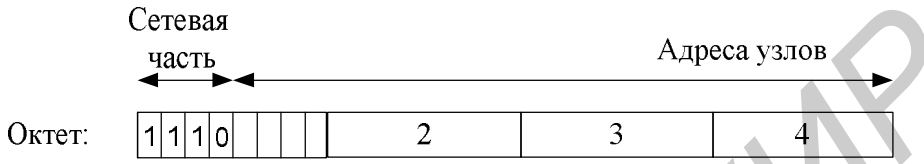

Рис. 5.5. Адреса класса D

Диапазон адресов класса D так же, как и других классов определенным образом ограничен. Первые четыре бита адреса класса D должны быть равны 1110. Следовательно, первый октет адресов этого класса может принимать значения от 11100000_2 до 11101111_2 или от 224_{10} до 239_{10}. Многоадресатный IP-адрес, первый октет которого начинается с чисел в диапазоне от 224 до 239, является адресом класса D.

Адреса класса E (рис. 5.6) – были зарезервированы специальной комиссией интернет-разработок (Internet Engineering Task Force – IETF) для исследовательских нужд. В результате адреса класса E никогда не использовались в сети Internet. Первые четыре бита адресов класса E всегда содержат 1. Следовательно, значение первого октета находится в диапазоне от 11110000_2 до 11111111_2 или от 240_{10} до 255_{10}.

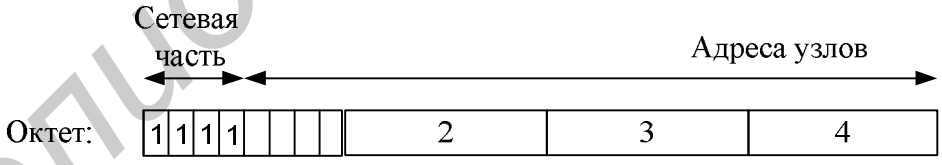

Рис. 5.6. Адреса класса E

Диапазоны значений первого октета в IP-адресах для каждого из классов приведены в табл. 5.1.

Таблица 5.1

Диапазон значений первого октета в IP-адресах

Класс IP-адреса	Диапазон IP-адресов	
Класс A	от 1 до 126	от 00000001 до 01111111
Класс B	от 128 до 191	от 10000000 до 10111111
Класс C	от 192 до 223	от 11000000 до 11011111
Класс D	от 224 до 239	от 11100000 до 11101111
Класс E	от 240 до 255	от 11110000 до 11111111

К *зарезервированным* адресам, которые не могут быть присвоены сетевым устройствам, относятся:

- сетевые адреса, идентифицирующие саму сеть;
- широковещательный адрес, используемый для широковещательной рассылки всем сетевым устройствам в данной сети;
- IP-адрес сети, у которого все биты, отведенные под адрес узла, заполнены нулями (рис. 5.7).

Рис. 5.7. Структура адреса сети

Для адреса сети класса B, записанного в виде чисел в точечно-десятичном формате, первые два октета стандартно идентифицируют сеть. Последние два октета содержат нули, поскольку именно эти 16 битов являются той частью адреса, которая отведена для идентификации подключенных к сети устройств. Такой адрес называется *одноадресатным* (unicast), где «uni» обозначает «один». Одноадресатный адрес указывает только на один узел во всей сети. IP-адрес из рассмотренного выше примера (176.10.0.0) зарезервирован в качестве адреса сети и ни при каких условиях не может быть использован в качестве адреса подключенного к сети устройства. Примером IP-адреса сетевого устройства в сети 176.10.0.0 может быть 176.10.16.1. В данном примере 176.10 является сетевой частью адреса, а 16.1 – это часть, обозначающая узел.

Для передачи данных всем узлам в сети требуется *широковещательный адрес*. Широковещательная рассылка используется, когда отправитель пересылает данные всем устройствам в сети (рис. 5.8). Адрес класса B 176.10.255.255 на рис. 5.8 является широковещательным для данной сети. Когда пакеты будут получены в соответствии с широковещательным адресом получателя, данные будут обработаны на каждом из компьютеров. Чтобы быть уверенным в том, что все устройства в сети получили и обработали пакеты широковещательной рассылки, отправитель должен использовать специальный IP-адрес, который будет понят и правильно обработан остальными устройствами. В широковещательных IP-адресах все биты, отведенные под адрес узла (поле узла), равны единице.

Рис. 5.8. Широковещательный адрес

Для сети с адресом 176.10.0.0, в котором последние 16 битов формируют поле узла (или отведенную для узла часть адреса), адресом широковещательной рассылки является адрес 176.10.255.255 (поскольку 255_{10} соответствует 11111111_2).

Сеть с номером 127.0.0.0 зарезервирована для обратного петлевого (loopback) тестирования (маршрутизаторы или локальные узлы могут использовать его для передачи пакетов самим себе). Следовательно, такой адрес не может быть присвоен сети.

На рис. 5.9 приведено соответствие классов адресов значениям первых битов октета.

Количество начальных битов префикса	1	7	24
Класс A: значение префикса	0	Сетевые биты	Биты узла

Количество начальных битов префикса	2	14	16
Класс B: значение префикса	10	Сетевые биты	Биты узла

Количество начальных битов префикса	3	14	8
Класс C: значение префикса	110	Сетевые биты	Биты узла

Количество начальных битов префикса	4	28
Класс D: значение префикса	1110	Адрес

Количество начальных битов префикса	4	28
Класс E: значение префикса	1111	Адрес

Адреса класса D используются для многоадресатной рассылки. Нет необходимости выделять биты или октеты отдельно для адресов сети и узлов.

Адреса класса E зарезервированы для исследовательских целей.

Рис. 5.9. Начальные биты, образующие классы IP-адресов

Стабильное функционирование сети Internet зависит от у*никальности* используемых в сети публичных адресов. Наличие дублирующихся адресов могло бы привести к нестабильности работы сети Internet и дополнительной нагрузке на устройства из-за доставки пакетов сетям, использующим дублирующиеся адреса.

Открытые IP-адреса уникальны. Не существует двух устройств с одинаковыми IP-адресами, которые были бы подключены к открытой сети, поскольку такие адреса используются в глобальном масштабе и подчиняются стандарту. Открытые IP-адреса должны выделяться поставщиками услуг Internet (Internet Service Provider – ISP) или регистрироваться за определенную плату.

Вследствие быстрого роста сети Internet количество незанятых IP-адресов уменьшается, поэтому появляются новые схемы адресации, такие, как *бесклассовая междоменная маршрутизация* (Classless InterDomain Routing – CIDR) и IPv6, призванные помочь решить проблему ограниченности адресного пространства.

Чтобы частично решить проблему нехватки адресного пространства, был разработан альтернативный вариант – частные IP-адреса (табл. 5.2). Как уже говорилось, узлы в сети Internet должны иметь глобально-уникальные адреса. Однако частные сети, не подключенные к открытой сети, могут использовать любые действительные адреса, которые должны быть уникальны только внутри локальной сети. Многие частные сети используются совместно с открытыми сетями, поэтому настоятельно не рекомендуется использовать выбранные произвольно адреса, поскольку однажды частная сеть может оказаться подключенной к глобальной сети Internet.

В спецификации RFC 1918 выделены три блока IP-адресов (один адрес класса A, серия адресов классов B и C) для внутреннего использования в частных сетях. Адреса из этих диапазонов не передаются магистральными маршрутизаторами сети Internet.

Таблица 5.2

Частные IP-адреса

Класс IP-адреса	Диапазон адресов (для внутреннего использования) по RFC 1918
Класс A	от 10.0.0.0 до 10.255.255.255
Класс B	от 172.16.0.0 до 176.31.255.255
Класс C	от 192.168.0.0 до 192.168.255.255

В том случае, когда нужно выбрать схему адресации для внутренней сети тестовой лаборатории или домашней сети, можно использовать диапазоны адресов, перечисленные в табл. 5.2, вместо глобально-уникальных. Частные IP-адреса могут использоваться совместно с публичными (открытыми) для внутренних соединений, что позволяет экономить открытые уникальные адреса.

При подключении сети предприятия, в которой используются частные адреса, к сети Internet необходимо обеспечить преобразование частных адресов в открытые. Такой процесс называется *трансляцией сетевых адресов* (Network Address Translation – NAT) и обычно выполняется маршрутизатором.

Подсети. Еще одним способом экономии IP-адресов является механизм использования *подсетей* (subnetting). Этот метод позволяет разбивать полные классовые блоки сетевых адресов на меньшие и помогает избежать полного

исчерпания IP-адресов. На рис. 5.10 показана сеть класса B (131.108.0.0), которая разбита на три подсети.

Каждый сетевой администратор должен понимать механизм создания подсетей как способ деления и идентификации отдельных сетей внутри локальной сети. Небольшие сети требуется разбивать на более мелкие подсети достаточно редко, но в случае использования больших блоков адресов и очень крупных сетей такое деление необходимо. Согласно определению *создание в сети подсетей* означает использование маски подсети для разделения ее на более мелкие, более эффективные, легче управляемые сегменты. Такая схема похожа на используемую в телефонных сетях нумерацию, которая состоит из телефонного кода страны, кода региона или города и телефона конечного абонента. Такие компоненты телефонных систем сравнимы с соответствующими элементами в IP-сетях – адресами сетей, подсетей и отдельных узлов.

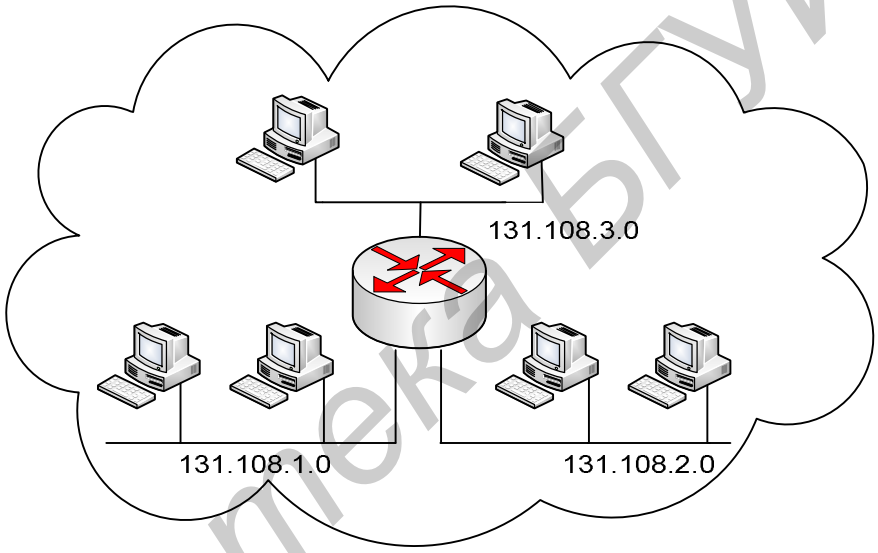

Рис. 5.10. Схема сети класса B с использованием подсетей

Системный администратор должен уметь решать проблемы, возникающие при добавлении новых сегментов в инфраструктуру и при расширении сети. Наиболее важный вопрос, на который необходимо дать ответ, связан с определением нужного количества подсетей и допустимого количества узлов, которые могут входить в каждую из полученных в процессе разбиения сетей. Благодаря использованию механизма подсетей можно создать гибкую структуру сети, которая не будет ограничиваться масками или рамками стандартных сетей классов A, B и C.

Адреса подсетей состоят из сетевой части класса A, B или C, поля подсети и поля адреса узла. Указанные поля формируются из исходного адреса всей сети. Умение определить, каким образом разделить исходное поле адреса узла на поля адреса подсети и адреса узла, дает сетевым администраторам определенную свободу при выборе схемы адресации.

Чтобы создать подсеть, сетевой администратор «заимствует» биты из поля адресов узлов исходного адреса всей сети и назначает их в качестве адре-

са подсети. Минимальное количество битов, которое может быть заимствовано, – два. Если использовать всего один бит, то после разбиения будет получен только один сетевой адрес (.0 – адрес сети) и один широковещательный (.255). Максимальное число битов, которые разрешено заимствовать, может быть любым (в рамках максимальной длины узловой части адреса), при условии, что останутся незадействованными не менее двух битов для адресов узлов. Для сети класса С может быть заимствовано не более шести битов из поля адреса
узла для создания подсети.

Чтобы выделить подсеть, биты сетевого узла должны быть переназначены как сетевые биты посредством деления октета (или октетов) сетевого узла на части. Такой механизм часто называют *заимствованием битов*, но более точным термином будет *аренда битов*, хотя последний используется очень редко. Процесс деления всегда начинается с крайнего левого бита узла, положение которого зависит от класса IP-адреса.

Помимо повышения управляемости, создание подсетей позволяет сетевым администраторам ограничить широковещательные рассылки и реализовать механизм низкоуровневой безопасности в локальной сети. Безопасность при использовании подсетей в локальных сетях реализуется благодаря тому, что доступ в другие подсети организуется через маршрутизаторы. Маршрутизатор может быть настроен так, чтобы разрешить или запретить доступ к подсети на основе различных критериев, таким образом реализуется политика безопасности. Некоторые организации, обладатели сетей классов А и В, продают или передают в аренду не использованные ранее IP-адреса.

На рис. 5.11 показано, как в среде многочисленные сети подключены к сети Internet посредством единой точки доступа – общего маршрутизатора. С использованием подсетей можно организовать частную сеть, в которой внутренние устройства будут заниматься доставкой данных пользователей.

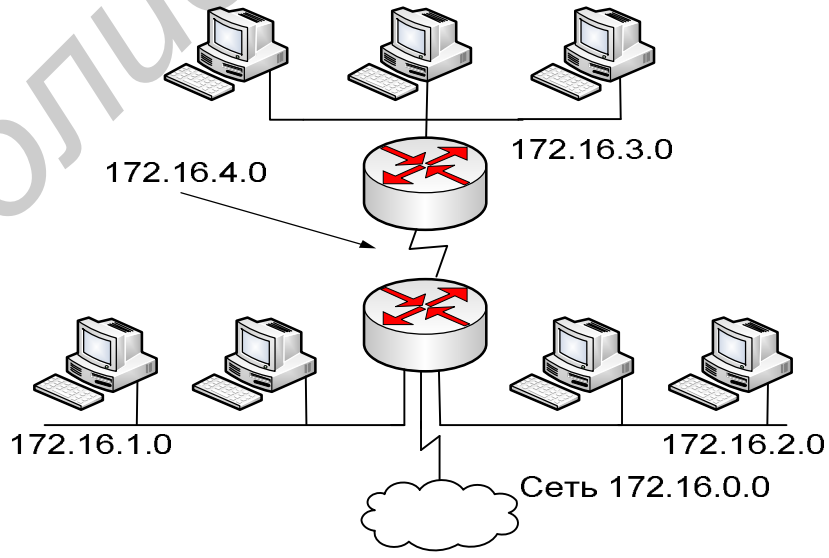

Рис. 5.11. Подсети

Поскольку адрес подсети формируется из узловой части адреса класса A, B или C, он назначается локально, обычно местным сетевым администратором. Кроме того, как и остальные части IP-адреса, каждый адрес подсети должен быть уникальным внутри области его использования (рис. 5.12).

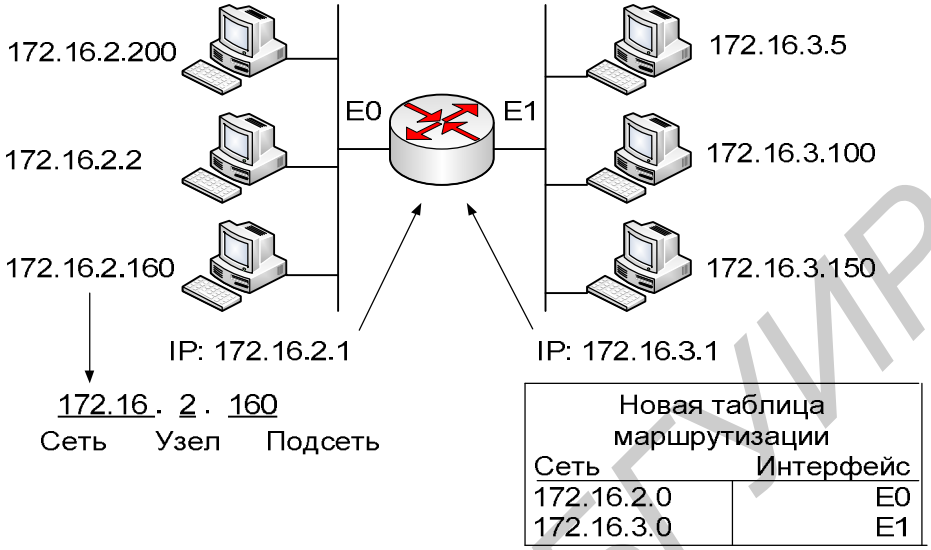

Рис. 5.12. Адреса подсетей

Подсети часто используются при объединении локальных сетей с целью создания единой распределенной сети. Например, при объединении двух локальных сетей, расположенных в географически удаленных точках, можно назначить уникальные подсети каждой из локальных сетей и каналу распределенной сети между ними. В таком случае могут быть использованы два маршрутизатора (по одному в каждой из сетей) для передачи пакетов между локальными сетями (подсетями).

Еще одной важной причиной использования подсетей является необходимость в уменьшении размеров широковещательных доменов. Широковещательные пакеты рассылаются всем узлам в сети или подсети. Когда широковещательный трафик начинает расходовать значительную часть доступной полосы пропускания, сетевой администратор может принять решение об уменьшении размеров широковещательного домена.

Внешний мир «видит» локальную сеть как единую сеть, ничего не зная о ее внутренней структуре. Такой подход позволяет уменьшить таблицы маршрутизации и эффективно их использовать. Получив локальный адрес узла 192.168.10.14, внешний мир за пределами локальной сети использует только объявленный основной сетевой адрес 192.168.10.0. Причина этого в том, что локальный адрес 192.168.10.14 действителен только в пределах локальной сети 192.168.10.0. В других местах он работать не будет.

Адрес подсети включает сетевую часть адреса классов A, B или C плюс поле подсети и поле узла. Эти поля создаются на основе оригинального IP-адреса заимствованием битов из узловой части адреса и присоединением к исходной сетевой части адреса. Как показано на рис. 5.13, возможность деле-

ния оригинальной узловой части адреса на новые подсети и адреса узлов предоставляет гибкость в выборе схемы адресации для сетевых администраторов. Это означает, что у сетевого администратора есть более широкий выбор при выборе схемы адресации как изначально, так и при расширении сети.

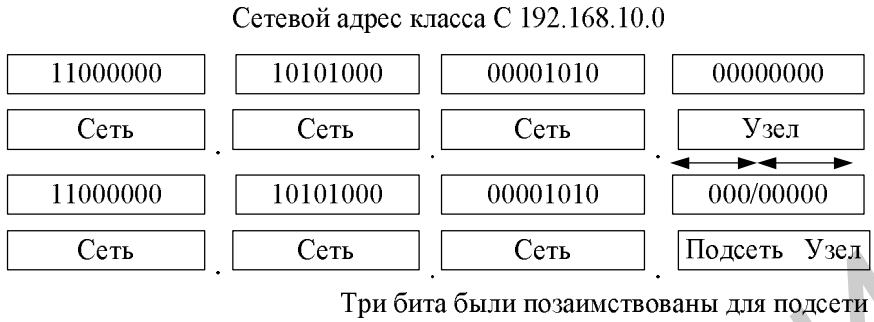

Рис. 5.13. Деление узлового октета адреса класса С

Назначение маски подсети. Выбор необходимого количества битов для создания подсети зависит от требуемого максимального количества узлов в подсети. Чтобы вычислить результат заимствования определенного количества узловых битов для создания подсети, необходимо иметь базовые знания из области двоичной математики и помнить битовые значения в каждой из позиций октета (табл. 5.3).

Таблица 5.3

Расчет подсети: два формата маски подсети

Формат с обратной косой чертой	/25	/26	/27	/28	/29	/30	–	–
Маска	128	192	224	240	248	252	254	255
Бит	1	2	3	4	5	6	7	8
Значение	128	64	32	16	8	4	2	1

Независимо от класса IP-адреса два последние бита в последнем октете никогда не могут быть использованы для формирования подсети. Они называются *наименее значимыми битами.* Заимствование всех доступных битов за исключением двух последних позволяет создать подсеть, которая содержит только два узла. На практике такой способ используется для экономии адресов при адресации последовательных связей между маршрутизаторами. Однако для работающих локальных сетей такой способ заимствования вызвал бы недопустимые расходы на оборудование.

Чтобы создать маску подсети, дающую маршрутизатору информацию, необходимую для вычисления адреса подсети, которой принадлежит конкретный узел, необходимо выбрать столбец из таблицы с нужным количеством битов (см. табл. 5.3) и в качестве значения маски воспользоваться числом, взятым из строки выше того же столбца. Это значение получено в результате сложения двоичных значений для знакомест используемых битов. Как показано в табл. 5.3, если заимствованы три бита, маска подсети для сети класса С

будет равна 255.255.255.224. При использовании формата записи маски с обратной косой чертой он может быть представлен как «/27». Число, указанное после символа обратной косой черты, представляет собой количество битов, составляющих адрес сети, плюс биты, используемые для маски подсети.

Чтобы определить требуемое количество битов, разработчик сети должен рассчитать, какое максимальное число узлов будет в подсети и общее количество подсетей. В качестве примера предположим, что необходимо разместить по 30 узлов в пяти подсетях. Чтобы определить необходимое количество битов для переназначения, воспользуемся строкой «Количество используемых узлов» из табл. 5.4. Таким образом, будет создано шесть подсетей, что также удовлетворяет указанным выше требованиям. Следует помнить, что разница в количестве доступных узлов и полном количестве возникает из-за того, что первый доступный адрес является идентификатором сети, а последний – ее широковещательным адресом. Классовая маршрутизация не предоставляет механизм использования соответствующих подсетей, в то время как при бесклассовой маршрутизации множество «потерянных» адресов доступно для использования.

Таблица 5.4

Расчет подсети: подсети и узлы

Формат с обратной косой чертой	/25	/26	/27	/28	/29	/30	–	–
Маска	128	192	224	240	248	252	254	255
Бит	1	2	3	4	5	6	7	8
Значение	128	64	32	16	8	4	2	1
Всего подсетей	–	4	8	16	32	64	–	–
Доступные подсети	–	2	6	14	30	62	–	–
Всего узлов	–	64	32	16	8	4	–	–
Количество используемых узлов	–	62	30	14	6	2	–	–

Для создания подсети необходимо расширить часть адреса, с которой оперируют маршрутизаторы. В сети Internet устройства оперируют с сетью как с единым целым согласно классу адресов A, B или C, которые задаются восемью, шестнадцатью или двадцатью четырьмя битами в маске (номером сети). Поле подсети описывает дополнительные биты, давая возможность локальным маршрутизаторам оперировать разными подсетями внутри единой большой сети.

В маске подсети используется тот же формат, что и в IP-адресе. Иными словами, маска подсети состоит из четырех октетов, а длина ее составляет 32 бита. Сетевая часть маски подсети, как и часть, определяющая подсеть, состоит из всех единиц, а узловая ее часть заполнена нулем. Стандартно, если ни один бит не заимствован для разбиения сети на подсети, маска для сети класса B выглядит как 255.255.0.0. Если заимствовано восемь битов, соответствующая маска будет иметь вид 255.255.255.0, как показано на рис. 5.14 и 5.15. Поскольку в адресе класса B выделены два октета под адреса узлов, для задания маски подсети может быть заимствовано не более 14 битов. В сети

класса С используются только восемь битов для поля узла. Следовательно, для задания маски подсети может быть заимствовано не более шести битов.

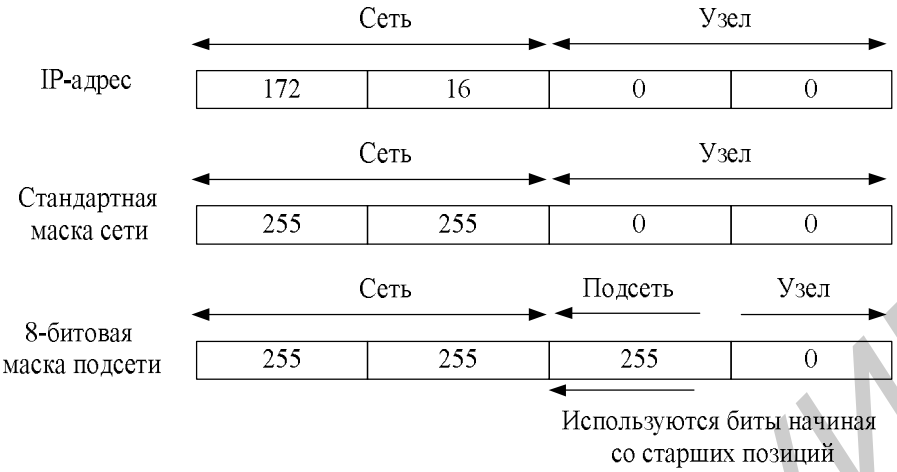

Рис. 5.14. Адреса сети и узла

Поле подсети всегда следует непосредственно за номером сети. Такое требование означает, что заимствовать можно первых *n* битов из стандартного поля узлов, где *n* – необходимая длина поля создаваемой подсети. Маска подсети является инструментом, который используется маршрутизатором при определении сетевой части адреса и его узловой части.

128	64	32	16	8	4	2	1		
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

Рис. 5.15. Схема двоичных преобразований

5.2. Задание для лабораторной работы

Разделите сети (рис. 5.16) на подсети согласно следующим условиям:

1. Каждая подсеть в сети 172.16.0.0 /16 должна содержать до 1000 хостов.
2. Каждая подсеть в сети 172.17.0.0 /16 должна содержать до 80 хостов.
3. В сети 172.18.0.0 /16 должно быть минимум 19 подсетей.
4. В сети 172.19.0.0 /16 должно быть минимум 4 подсети.
5. Настройте PC0: IP адрес 172.16.3.5 с вычисленной маской.
6. Настройте PC1: IP адрес 172.17.0.90 с вычисленной маской.

7. Настройте PC2: IP адрес 172.18.0.2 с вычисленной маской
8. Настройте PC3: IP адрес 172.19.0.9 с вычисленной маской

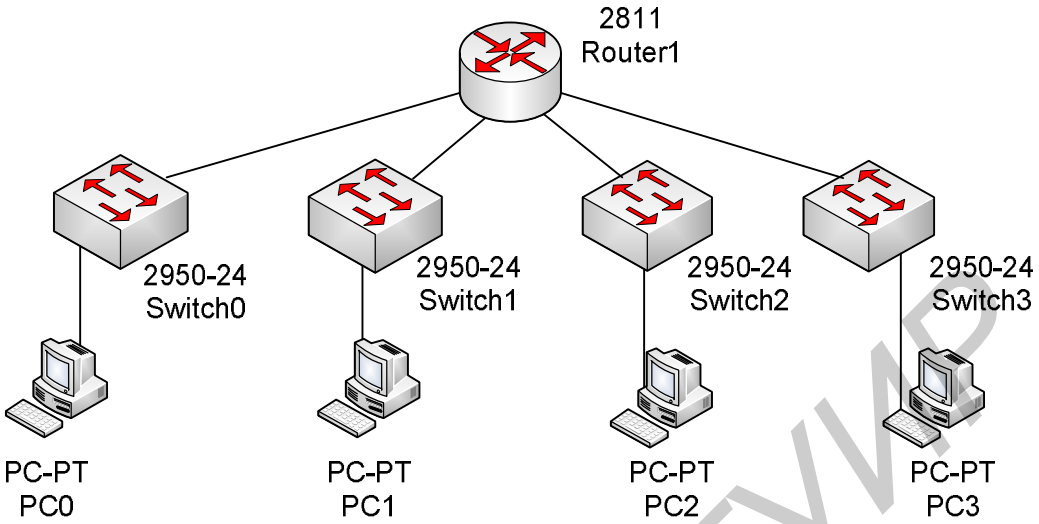

Рис. 5.16. Схема сети

5.3. Содержание отчета

1. Цель работы.
2. Схема сети.
3. Описание деления сети на подсети.
4. Выводы.

5.4. Контрольные вопросы

1. Что такое IP-адреса? Из каких частей они состоят?
2. Какие классы IP-адресов вы знаете?
3. Сколько может быть создано сетей класса A?
4. Какие примеры частных IP-адресов в сетях классов A, B, C вы можете назвать?
5. Каково назначение маски подсети?
6. Какие есть форматы записи масок подсети?

Лабораторная работа №6

МАРШРУТИЗАЦИЯ. ПОНЯТИЕ АДМИНИСТРАТИВНОГО РАССТОЯНИЯ МАРШРУТА. СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Цель работы: ознакомиться с принципами статической маршрутизации в сетях, а также получить практические навыки в настройке статических маршрутов.

6.1. Теоретические сведения

Маршрутизация представляет собой процесс, который используется маршрутизатором для пересылки пакета в сеть получателя. Маршрутизатор принимает решения, основываясь на IP-адресе получателя пакета. Для того чтобы переслать пакет в требуемом направлении, все устройства на пути его следования используют IP-адрес получателя. Этот адрес позволяет пакету достичь требуемого пункта назначения. Для принятия правильного решения маршрутизаторы должны знать направления к удаленным сетям. При использовании *статической маршрутизации* (static routing*)* информация об удаленных сетях и любые изменения сетевой топологии и статических маршрутов задаются вручную сетевым администратором в явном виде при конфигурировании маршрутизатора. Маршрутизация при этом происходит без участия каких-либо протоколов маршрутизации.

Из-за дополнительных требований к настройке и необходимости вмешательства администратора статическая маршрутизация не обладает гибкими возможностями масштабирования. Однако в крупных сетях часто конфигурируются статические маршруты для специальных целей в комбинации с протоколом динамической маршрутизации.

В некоторых случаях в целях безопасности требуется скрыть некоторые части сети. Статическая маршрутизация позволяет пользователю указать, какая информация может распространяться относительно таких скрытых сетей с ограниченным доступом.

Основные достоинства статической маршрутизации:

- лёгкость отладки и конфигурирования в малых сетях;
- отсутствие дополнительных накладных расходов (из-за отсутствия протоколов маршрутизации)
- мгновенная готовность (не требуется интервал для конфигурирования или подстройки);
- низкая нагрузка на процессор маршрутизатора;
- предсказуемость в каждый момент времени.

Недостатки:

- плохое масштабирование (добавление N+1 сети потребует сделать 2·(N+1) записей о маршрутах, причём на большинстве маршрутизаторов

таблица маршрутов будет различной, при N>3-4 процесс конфигурирования становится весьма трудоёмким);

- низкая устойчивость к повреждениям линий связи (особенно в ситуациях, когда обрыв происходит между устройствами второго уровня и порт маршрутизатора не получает статус down);
- отсутствие динамического балансирования нагрузки;
- необходимость в ведении отдельной документации к маршрутам, проблема синхронизации документации и реальных маршрутов.

Функционирование статических маршрутов может быть описано тремя положениями.

1. Сетевой администратор задает статический маршрут.
2. Маршрутизатор заносит этот маршрут в свою таблицу маршрутизации.
3. Пакеты пересылаются с использованием указанного статического маршрута.

Для установки статического маршрута сетевой администратор должен ввести соответствующую команду ip route. Эта команда имеет следующий синтаксис:

Router(config)#ip route prefix mask (ip-address\interface-type interface number)[distance]

На рис. 6.1 сетевому администратору маршрутизатора Hoboken требуется сконфигурировать статический маршрут к сетям 172.16.1.1/24 и 172.16.5.1/24, подсоединенным к другим маршрутизаторам.

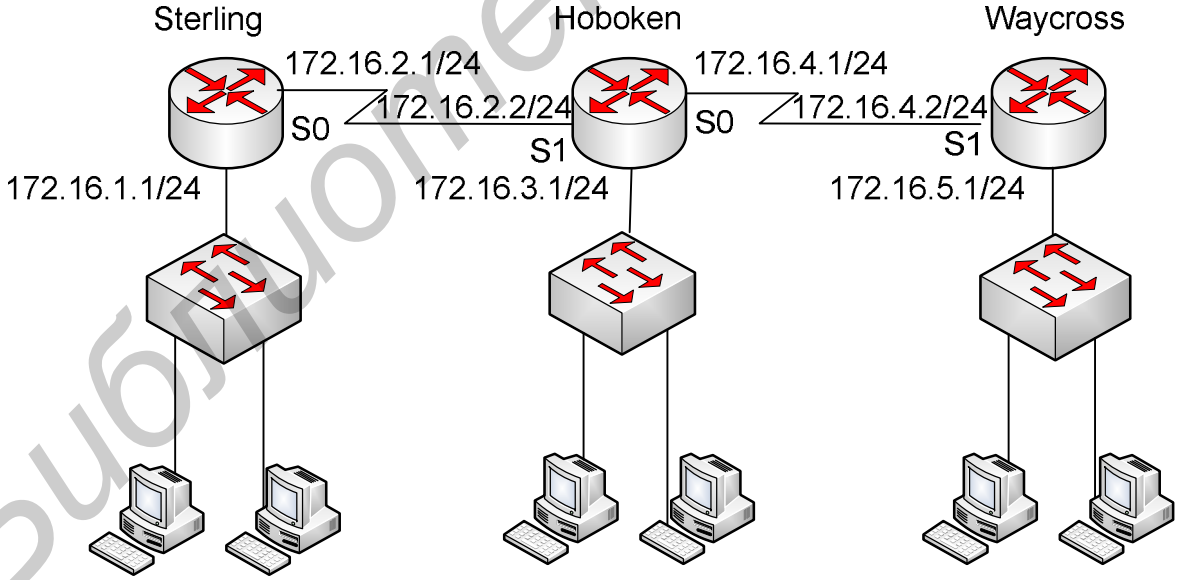

Рис. 6.1. Статические маршруты

Для решения этой задачи сетевой администратор может ввести одну или две команды. В примере 6.1 для этого указывается выходной интерфейс (Serial 0). В примере 6.2 указывается IP-адрес соседнего маршрутизатора (172.16.2.2). Любая из этих команд задает статический маршрут в таблице маршрутизации маршрутизатора Hoboken.

Пример 6.1. Пример статического маршрута с использованием интерфейса
Sterling(config)#ip route 172.16.3.0 255.255.255.0 s0

Пример 6.2. Статический маршрут с использованием IP-адреса маршрутизатора:
Sterling(config)#ip route 172.16.3.0 255.255.255.0 172.16.2.2

Единственным различием между этими двумя командами является *административное расстояние* (administrative distance), назначаемое маршруту при его занесении в таблицу маршрутизации. Под административным расстоянием понимается необязательный параметр, который характеризует надежность маршрута. Меньшему значению административного расстояния соответствует более надежный маршрут. Такое утверждение означает, что маршрут с меньшим административным расстоянием будет установлен в таблицу маршрутизации прежде, чем маршрут с большим административным расстоянием. Стандартно при использовании адреса следующего перехода административное расстояние устанавливается равным единице. При задании выходного интерфейса для административного расстояния устанавливается значение ноль. В табл. 6.1 приведены административные расстояния для каждого поддерживаемого протокола. Маршрутам с меньшим административным расстоянием отдается предпочтение по сравнению с аналогичными маршрутами с большим административным расстоянием. Если требуется установить административное расстояние, отличающееся от стандартного, то следует ввести значение в интервале от 0 до 255 после адреса следующего перехода или указания выходного интерфейса, как показано ниже.

ip route 172.16.3.0 255.255.255.0 192.168.2.1 255

Если маршрутизатор по каким-либо причинам не может использовать выходной интерфейс, заданный в маршруте, то этот маршрут не будет использоваться устройством. Это означает, что если указанный интерфейс неработоспособен, то маршрут не будет занесен в таблицу маршрутизации.

Иногда статические маршруты используются в качестве резервных. На маршрутизаторе может быть сконфигурирован статический маршрут, который будет использован только в том случае, если не удастся отправить данные по динамически созданному маршруту. Для использования статического маршрута как резервного его административное расстояние должно быть установлено большим, чем у маршрута, предоставляемого протоколом динамической маршрутизации.

Таблица 6.1

Административные расстояния в ОС Cisco IOS

Источник маршрута	Стандартное значение административного расстояния
1	2
Подсоединенный интерфейс	0
Статический маршрут	1

Окончание табл. 6.1

1	2
Суммарный маршрут протокола EIGRP	5
Протокол BGP	20
Внутренний маршрут протокола EIGRP	90
Протокол IGRP	100
Протокол OSPF	110
Протокол IS-IS	115
Протокол RIP	120
Протокол EGP	140
Внешние маршруты протокола EIGRP	170
Внутренние маршруты BGP	200
Неизвестен	255

Чтобы сконфигурировать статические маршруты, необходимо выполнить следующее.

Этап 1. Определить все требуемые сети-получатели, их маски подсетей и префиксы. В качестве адреса шлюза может выступать либо локальный интерфейс маршрутизатора, либо адрес следующего транзитного перехода, который ведет к требуемому пункту назначения.

Термином *префикс* зачастую обозначают адреса сетей. Наиболее полное определение данного термина подразумевает, что под ним обычно понимается адрес, узловые биты маски которого равны нулю, а сетевые – единице. Префиксный адрес также может подразумевать под собой суммарный адрес. Например, можно суммировать (агрегировать) несколько указанных ниже адресов в один суммарный с префиксом 192.168.0.0/22. Обозначение «/22» указывает на то, что 22 первых бита являются префиксом. Сети, которые войдут в указанный суммарный адрес:

192.168.0.0/24
192.168.1.0/24
192.168.2.0/24
192.168.3.0/24

Этап 2. Войти в режим глобального конфигурирования.

Этап 3. Ввести команду ip route с адресом сети-получателя и маской подсети, за которыми следует адрес следующего транзитного узла. Указание административного расстояния не является обязательным.

Этап 4. Повторить этап 3 для всех сетей-получателей, которым требуется задать статический маршрут.

Этап 5. Выйти из режима глобального конфигурирования.

Этап 6. Сохранить активную конфигурацию в памяти NVRAM с помощью команд copy running-config startup-config и write memory.

Сеть, показанная на рис. 6.2, включает в себя три маршрутизатора. Маршрутизатор Hoboken должен быть сконфигурирован таким образом, чтобы он обеспечивал доступ к сетям с адресами 172.16.1.0 и 172.16.5.0. В обеих сетях маска подсети имеет вид 255.255.255.0.

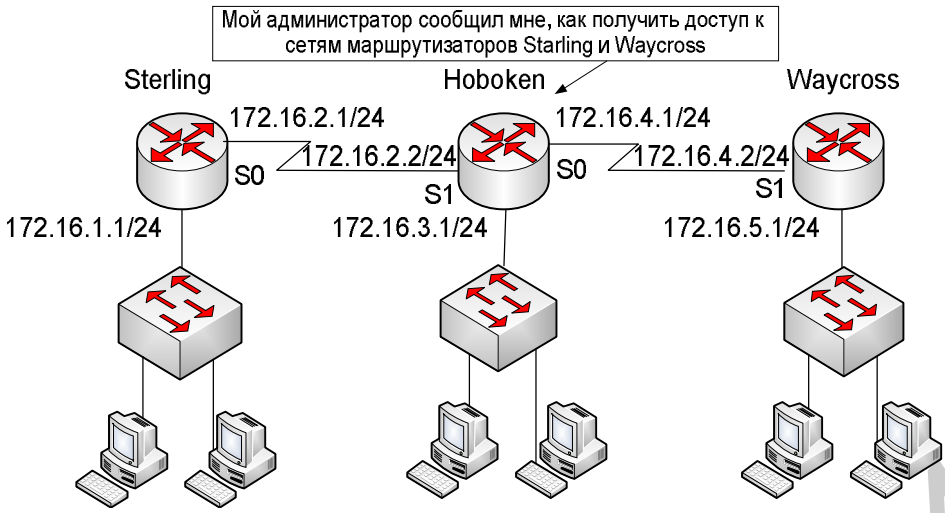

Рис. 6.2. Функционирование статических маршрутов

Пакеты, у которых получателем является сеть 172.16.1.0, требуется направлять на маршрутизатор Sterling. Пакеты, у которых получателем является сеть 172.16.5.0, требуется направлять на маршрутизатор Waycross. Для этого необходимо сконфигурировать статические маршруты с использованием выходных интерфейсов маршрутизатора S0 и S1, как показано в примере 6.3.

Пример 6.3. Задание выходных интерфейсов IP-маршрутов
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 s1
Hoboken(config)#ip route 172.16.5.0 255.255.255.0 s0

Оба статических маршрута конфигурируются с использованием локального интерфейса в качестве шлюза к сетям-получателям, как показано на рис. 6.2. Поскольку административное расстояние не указано, при занесении маршрутов в таблицу маршрутизации оно стандартно принимается равным нулю. Следует обратить внимание на то, что административное расстояние, равное нулю, также присуще непосредственно подсоединенной сети.

Те же статические маршруты могут быть сконфигурированы с использованием в качестве шлюза адреса следующего перехода. Первый маршрут к сети 172.16.1.0 проходит через шлюз 172.16.2.1. У сети 172.16.5.0 шлюз имеет адрес 172.16.4.2. В примере 6.4 показано, как сконфигурировать статические маршруты с использованием адреса интерфейса следующего транзитного перехода; в него включены комментарии, которые не будут отображены в файле конфигурации. Поскольку административное расстояние явным образом не задано, стандартно оно устанавливается равным единице.

Пример 6.4. Статические маршруты с использованием адреса следующего транзитного перехода и комментариями

Hoboken(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1 !Данный маршрут ведет к локальной сети Sterling

Hoboken(config)#ip route 172.16.1.0 255.255.255.0 172.16.4.2 !Данный маршрут ведет к локальной сети Waycross

Конфигурирование пересылки пакетов по стандартному маршруту. Стандартные маршруты используются маршрутизаторами в тех случаях, когда адрес сети-получателя пакета не совпадает ни с одним из маршрутов, содержащихся в таблице маршрутизации. Стандартные маршруты, как правило, конфигурируются для передачи потоков данных через сеть Internet, поскольку нерационально и нет необходимости поддерживать все маршруты ко всем сетям Internet. Стандартный маршрут фактически является специальным статическим маршрутом, использующим следующий формат:

ip route 0.0.0.0 0.0.0.0 [next-hop-address/outgoing interface]

По умолчанию для конфигурирования маршрутов необходимо выполнить описанные ниже действия.

Этап 1. Войти в режим глобальной конфигурации.

Этап 2. Ввести в командной строке команду ip route с адресом 0.0.0.0 для сети-получателя и значением 0.0.0.0 для маски подсети.

Этап 3. Выйти из режима глобального конфигурирования.

Этап 4. Сохранить текущую конфигурацию в памяти NVRAM с помощью команды copy running-config startup-config.

Проверка статических маршрутов. Для просмотра активной конфигурации в памяти NVRAM и проверки правильности ввода статических маршрутов используется команда show running-config. Для проверки наличия маршрута в таблице маршрутизации используется команда show ip route.

6.2. Задание для лабораторной работы

Необходимо настроить статическую маршрутизацию на двух маршрутизаторах Router_Brest и Router_Minsk (рис. 6.3) так, чтобы из вашей сети был доступ к ISP (Internet Service Provider). В вашем распоряжении только один персональный компьютер «Ваш ПК» и пароли доступа по telnet к маршрутизаторам (password: cisco).

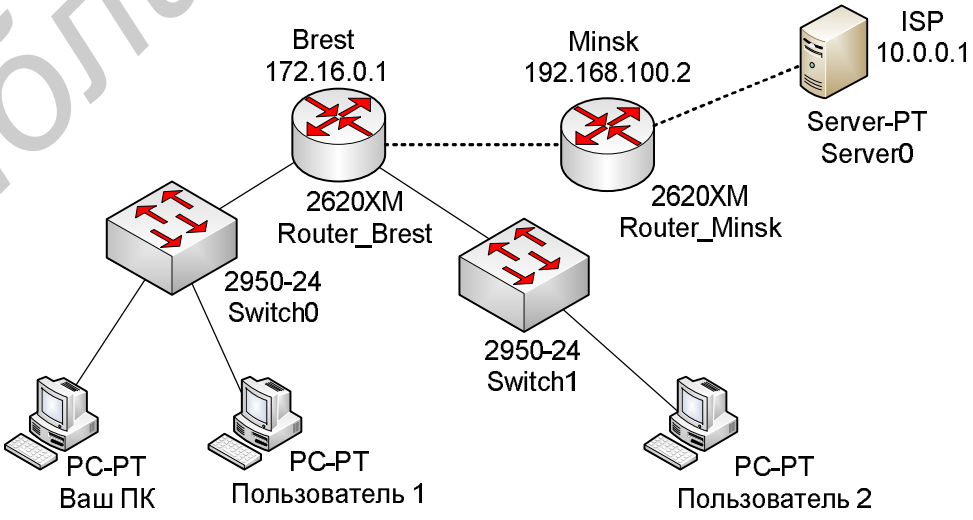

Рис. 6.3. Маршрутизируемая сеть

6.3. Содержание отчета

1. Цель работы.
2. Схема сети.
3. Конфигурационные файлы маршрутизаторов.
4. Выводы.

6.4. Контрольные вопросы

1. Что такое маршрутизация?
2. В чем различие статических и динамических маршрутов?
3. Что такое административное расстояние?
4. Какие этапы конфигурирования статических маршрутов вы знаете?
5. Для чего нужен стандартный маршрут?
6. Как проверить правильность конфигурирования статических маршрутов?

Лабораторная работа №7

ПОНЯТИЕ ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ. ПРОТОКОЛЫ МАРШРУТИЗАЦИИ. ПРОТОКОЛ RIP

Цель работы: изучить теорию динамической маршрутизации в сетях, принципы работы дистанционно-векторных протоколов, а также приобрести практические навыки в настройке протокола маршрутизации RIP.

7.1. Теоретические сведения

Динамическая маршрутизация (dynamic routing) необходима для того, чтобы сети могли обновлять свои таблицы маршрутизации и быстро адаптироваться к изменениям в топологии и состоянии соединений. Протоколы динамической маршрутизации могут направлять потоки данных одного и того же сеанса по нескольким маршрутам для повышения эффективности работы сети. Этот механизм представляет собой *распределение нагрузки* (load sharing) между несколькими каналами и устройствами.

После того как сетевой администратор вводит команды конфигурирования динамической маршрутизации, информация о маршрутах обновляется автоматически в процессе маршрутизации при каждом получении из сети новой информации о маршрутах. Маршрутизаторы обмениваются сообщениями об изменениях в топологии сети в процессе динамической маршрутизации.

Успешное осуществление динамической маршрутизации зависит от выполнения маршрутизатором двух его основных функций:

- поддержки таблицы маршрутизации в актуальном состоянии;
- распространения информации в виде анонсов и обновлений маршрутов среди остальных маршрутизаторов.

При распространении информации о сети механизм динамической маршрутизации использует один из протоколов маршрутизации. Такой протокол определяет набор правил, используемых маршрутизатором при осуществлении связи с соседними маршрутизаторами. Например:

- каким образом рассылаются обновления маршрутов;
- какая информация содержится в обновлениях;
- как часто рассылаются обновления;
- каким образом выполняется поиск получателей обновлений.

Первичной задачей устройства при обновлении таблицы маршрутизации с помощью алгоритма маршрутизации является выбор наилучшего маршрута для включения его в таблицу. Каждый алгоритм маршрутизации использует собственный способ выбора наилучшего маршрута. Для этого генерируется определенное значение, называемое *метрикой* (metric), для каждого маршрута в сети. Обычно, чем меньше значение метрики, тем лучше маршрут.

Могут использоваться *простые* метрики, которые вычисляются на основе одной характеристики, такой, например, как количество переходов на

маршруте, или более *сложные* метрики, использующие несколько параметров маршрутов. Ниже перечислены часто используемые в метриках характеристики.

- *Полоса пропускания* (Bandwidth) описывает пропускную способность канала.
- *Задержка* (Delay) представляет собой время, требуемое пакету для прохождения по каналу от отправителя до получателя.
- *Нагрузка* (Load) – это степень использования сетевых ресурсов на маршрутизаторе или канале.
- *Надежность* (Reliability) обычно характеризует уровень ошибок в сетевом канале.
- *Количество переходов* (Hop count) – это число маршрутизаторов, через которые должен пройти пакет до поступления в пункт назначения.
- *Стоимость* (Cost) представляет собой произвольное значение, обычно вычисляемое на основе ширины полосы пропускания, финансовых затрат или других характеристик, выбираемых сетевым администратором.

Протоколы *маршрутизации* отличаются от *маршрутизируемых* протоколов как по своим функциям, так и по задачам, которые перед ними стоят.

Протокол маршрутизации – это средство коммуникации между маршрутизаторами, позволяющее устройствам совместно использовать информацию о сетях и определять расстояние до разных узлов и сетей. Информация, которую один маршрутизатор получает от другого (посредством протокола маршрутизации), используется для построения и поддержания в актуальном состоянии таблицы маршрутизации.

К наиболее распространенным протоколам маршрутизации локальных сетей можно отнести следующие:

- *протокол маршрутной информации* (Routing Information Protocol – RIP);
- *протокол маршрутизации внутреннего шлюза* (Interior Gateway Routing Protocol – IGRP);
- *усовершенствованный протокол маршрутизации внутреннего шлюза* (Enhanced Interior Gateway Routing Protocol – EIGRP);
- *протокол выбора кратчайшего маршрута* (Open Shortest Path First – OSPF).

Маршрутизируемые или сетевые протоколы (протоколы передачи данных) используются для доставки пользовательской информации. Маршрутизируемый протокол содержит достаточное количество информации в адресе сетевого уровня для пересылки пакета от одного узла к другому на основе используемой схемы адресации. Маршрутизируемые протоколы определяют форматы полей внутри пакета. Пакеты обычно передаются от одной конечной системы к другой.

К наиболее распространенным маршрутизируемым протоколам сетей можно отнести следующие:

- *Internet-протокол* (Internet Protocol – IP);
- *межсетевой пакетный обмен* (Internetwork Packet Exchange – IPX).

Автономная система (Autonomous System – AS) – это набор сетей, которые находятся под единым административным управлением и в которых используются единая стратегия и правила маршрутизации. Автономная система для внешних сетей представляется как некий единый объект. Ее может поддерживать как несколько операторов-владельцев, так и один, все они будут нести ответственность за правильную маршрутизацию.

Реестр Internet-маршрутов (Internet Routing Registry – IRR), провайдер службы или сетевой администратор присваивает номер каждой автономной системе. Идентификатор автономной системы представляет собой 16-битное число. Некоторые протоколы маршрутизации, такие как фирменные протоколы IGRP и EIGRP корпорации Cisco, используют такое понятие, как *номер автономной системы* в своей конфигурации; в действительности же нет никакой необходимости прописывать в них реальный номер. Этот параметр представляет собой просто идентификатор процесса. Для двух указанных протоколов маршрутизации нет необходимости использовать номер системы, который получен от реестра IRR, или частный номер автономной системы.

Автономные системы делят объединенную сеть на несколько меньших легче управляемых сетей. Каждая автономная система имеет свой набор правил и политик, а ее номер является глобально уникальным, т. е. отличает ее от всех остальных автономных систем мира.

Целью использования протокола маршрутизации является построение и поддержка таблицы маршрутизации. В этой таблице содержатся информация об известных маршрутизатору сетях и соответствующие порты, ведущие к этим сетям.

Протокол маршрутизации идентифицирует все доступные маршруты, помещает лучшие таблицы в таблицу маршрутизации и удаляет из нее маршруты, если они становятся недоступными. Маршрутизатор использует информацию таблицы маршрутизации для пересылки пакетов сетевых (маршрутизируемых) протоколов.

В том случае когда все маршрутизаторы объединенной сети обладают одинаковой информацией о ней, говорят, что в ней произошла *конвергенция*. Быстрая конвергенция является желательной, поскольку она сокращает период принятия неправильных решений маршрутизации.

Зачастую можно обнаружить, что крупные сети, например, сети университетов, крупных компаний, даже школ имеют свою собственную автономную систему. Каждая подсеть или сегмент сети университета может быть построен с использованием какого-либо протокола маршрутизации, статических маршрутов; тем не менее все отдельные подсети в организации соединены между собой статическими или коммутируемыми каналами и входят в состав единой автономной системы.

Большинство алгоритмов маршрутизации может быть отнесено к одной из двух категорий:

- *дистанционно-векторный протокол* (distance vector routing protocol);
- *протокол с учетом состояния канала* (link-state routing protocol).

Дистанционно-векторный протокол определяет направление, или вектор, и расстояние до нужного узла объединенной сети.

Протокол с учетом состояния канала также называемый алгоритмом выбора кратчайшего пути (shortest path first – SPF) воссоздает топологию всей сети.

Сбалансированный гибридный протокол (balanced hybrid routing protocol) соединяет в себе определенные черты обоих алгоритмов: дистанционно-векторного и протокола с учетом состояния канала.

При использовании дистанционно-векторных алгоритмов маршрутизаторы периодически пересылают копии таблиц маршрутизации друг другу. В этих регулярных обновлениях маршрутизаторы сообщают об изменении топологии сети. Дистанционно-векторные алгоритмы маршрутизации также называются алгоритмами Беллмана – Форда (Bellman – Ford).

На рис. 7.1 каждый маршрутизатор получает таблицу маршрутизации от соседних маршрутизаторов. В частности, маршрутизатор B получает информацию от маршрутизатора A. Маршрутизатор B добавляет значение вектора расстояния, количество переходов, что увеличивает результирующий вектор расстояния. После этого маршрутизатор B передает свою новую таблицу маршрутизации своему соседу, маршрутизатору C. Такой пошаговый процесс происходит на всех соседних маршрутизаторах.

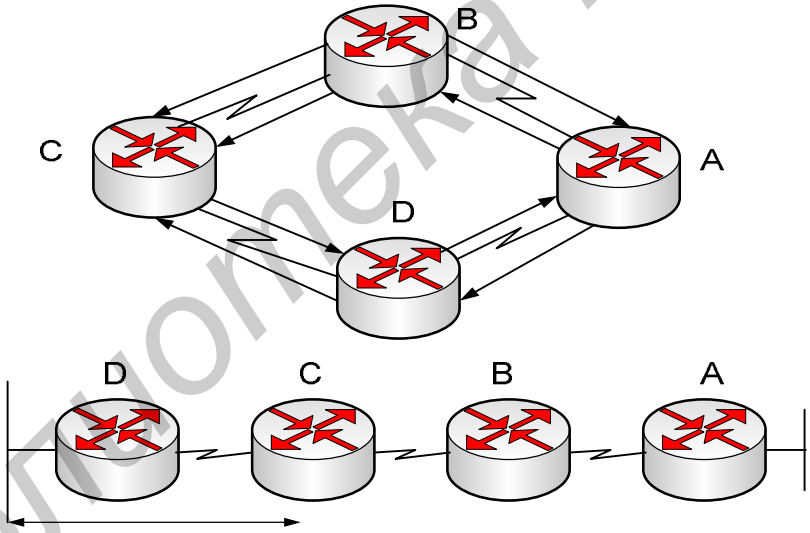

Рис. 7.1. Концепция дистанционно-векторной маршрутизации

Дстанционно-векторный алгоритм позволяет маршрутизатору накапливать значения векторов расстояния, что позволяет поддерживать базу данных, содержащую информацию о топологии сети. Однако использование дистанционно-векторных алгоритмов не предоставляет маршрутизатору точную топологию всей сети, поскольку каждому маршрутизатору известны только соседние с ним маршрутизаторы.

Каждый маршрутизатор, использующий дистанционно-векторную маршрутизацию, начинает свою работу с определения соседних маршрутизаторов.

Формирование вектора расстояния. Для каждого интерфейса, ведущего к непосредственно подсоединенной сети, вектор расстояния устанавливается равным нулю. По мере того как процесс расчета вектора расстояния продолжается, маршрутизаторы находят наилучший маршрут к сетям-получателям на основе информации, которую они получают от своих соседей. Например, маршрутизатор А узнает о других сетях на основе информации, которую он получает от маршрутизатора В (см. рис 7.1). В каждой из позиций таблицы маршрутизации есть суммарный вектор расстояния, который показывает, на каком расстоянии находится соответствующая удаленная сеть.

Обновление таблицы маршрутизации происходит при изменении топологии сети. По мере формирования векторов расстояния изменения топологии заносятся в таблицы маршрутизации последующих маршрутизаторов. При использовании дистанционно-векторных алгоритмов каждый маршрутизатор пересылает всю таблицу маршрутизации каждому из своих непосредственных соседей. В этой таблице содержится общая оценка маршрута, определяемая метрикой, и логический адрес маршрутизатора на пути к каждой сети, имеющейся в таблице. Например, как показано на рис. 7.2, маршрутизатор Б получает информацию от маршрутизатора А. Маршрутизатор Б добавляет свое значение к вектору расстояния (например количество переходов) и передает новую таблицу маршрутизации соседнему маршрутизатору.

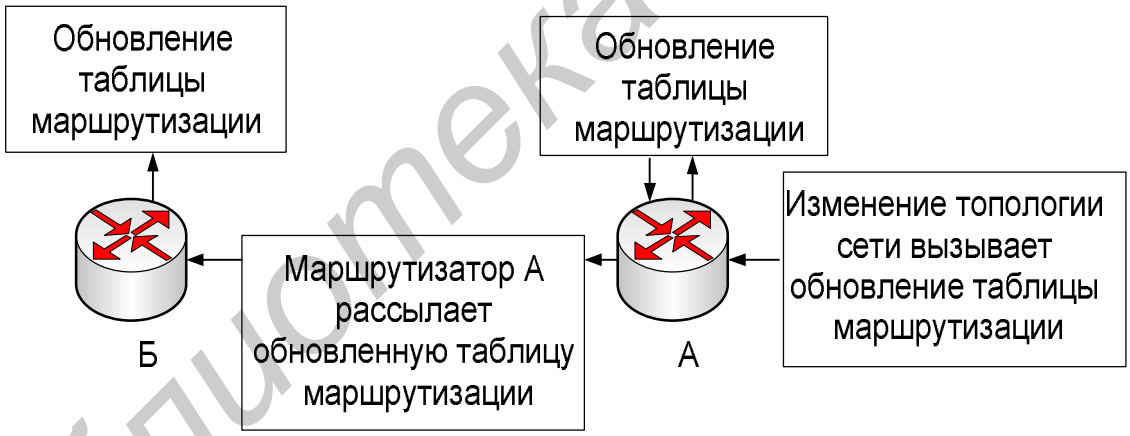

Рис. 7.2. Обработка изменений топологии дистанционно-векторным протоколом маршрутизации

Подобный пошаговый процесс происходит между всеми соседними маршрутизаторами. Вектор расстояния можно сравнить с дорожными знаками на шоссе. Эти знаки указывают направление к пункту назначения и расстояние до него. Далее по этому шоссе могут встретиться знаки, указывающие то же направление, однако указываемое ими расстояние будет меньшим. Уменьшение этого расстояния при последующем движении свидетельствует о движении в правильном направлении.

Маршрутизация по состоянию канала. Вторым базовым алгоритмом маршрутизации является алгоритм выбора маршрута по состоянию канала. Такие алгоритмы известны как алгоритмы Дейкстры, или алгоритмы выбора

кратчайшего пути. Они поддерживают сложную базу топологической информации. В то время как дистанционно-векторные алгоритмы не содержат определенной информации об удаленных сетях и удаленных маршрутизаторах, алгоритмы с использованием состояния канала поддерживают полную информацию об удаленных маршрутизаторах и их соединениях друг с другом. При маршрутизации по состоянию канала используются следующие компоненты:

- *анонсы состояния канала* (Link-State Advertisement – LSA). Эти объявления представляют собой небольшие пакеты, содержщие информацию о маршрутах и рассылаемые между маршрутизаторами;
- *топологическая база данных* (Topological Database). Эта база включает в себя информацию, полученную в сообщениях LSA;
- *алгоритм выбора первого кратчайшего пути* (Shortest Path First – SPF). Соответствующий алгоритм осуществляет вычисления над базой данных, результатом чего является построение связующего дерева протокола SPF;
- *таблица маршрутизации* (Routing table). Эта таблица содержит известные маршруты и соответствующие им интерфейсы.

Такая концепция маршрутизации на основе состояния канала была реализована в протоколе маршрутизации OSPF. Основные положения и операции протокола описаны в документе RFC 1583.

Маршрутизаторы обмениваются сообщениями LSA, начиная с непосредственно подсоединенных сетей. Каждый маршрутизатор параллельно с остальными создает топологическую базу данных, состоящую из информации, полученной из этих сообщений LSA.

Алгоритм SPF вычисляет доступность сетей. Маршрутизатор строит логическую топологию в виде дерева, корнем которого является он сам, а ветвями – все возможные маршруты ко всем сетям, входящим в объединенную сеть протокола состояния канала, после чего маршруты сортируются с помощью алгоритма. Маршрутизатор заносит наилучшие маршруты и связанные с ними интерфейсы в таблицу маршрутизации. Маршрутизатор также поддерживает другие базы данных – базы топологических элементов и базы подробностей состояния каналов.

Для создания общей картины всей сети в протоколах с учетом состояния канала используются специализированные механизмы обнаружения сетей, включающие в себя следующие пункты:

- Маршрутизаторы обмениваются друг с другом LSA-сообщениями. Каждый маршрутизатор начинает построение своей таблицы маршрутизации с непосредственно подсоединенных к нему сетей, от которых он получает информацию «из первых рук».
- Каждый маршрутизатор параллельно с остальными создает топологическую базу данных, состоящую из информации, полученной из всех LSA-сообщений объединенной сети.
- Алгоритм SPF вычисляет доступность сетей. Маршрутизатор строит логическую топологию в виде дерева, корнем которого является он сам, а вет-

вями – все возможные маршруты ко всем сетям, входящим в объединенную сеть протокола состояния канала. Позже маршруты сортируются с использованием алгоритма SPF.

- Маршрутизатор заносит наилучшие маршруты и ведущие к ним порты в свою таблицу маршрутизации. Маршрутизатор также поддерживает другие базы данных топологических элементов и информации о состоянии каналов.

Если маршрутизатор узнает об изменении состояния канала, он рассылает эту информацию всем остальным маршрутизаторам объединенной сети с тем, чтобы они могли ее использовать для маршрутизации. Для того чтобы закончилась конвергенция, каждый маршрутизатор поддерживает информацию о соседних маршрутизаторах, их именах, состоянии интерфейсов и стоимости каналов к соседним устройствам. Маршрутизатор создает пакет LSA в котором содержится перечисленная информация наряду с информацией о новых соседях, изменениях в стоимости каналов и о каналах, которые перестали функционировать. Затем этот пакет LSA направляется всем остальным маршрутизаторам.

При использовании протоколов состояния канала возникают три основные проблемы:

- перегрузка процессора служебной информацией;
- повышенные требования к памяти;
- потребление процессом маршрутизации значительной части полосы пропускания.

Маршрутизаторы, на которых работают протоколы с учетом состояния канала, требуют большего объема памяти и выполняют больший объем обработки данных, чем маршрутизаторы, использующие дистанционно-векторный протокол маршрутизации. Маршрутизаторы должны иметь достаточно памяти для хранения большого объема информации в различных базах данных, поддержки логического дерева и таблицы маршрутизации. Первоначальные потоки маршрутных данных о состоянии каналов занимают большую часть полосы пропускания, поскольку в первоначальной фазе обнаружения сетей все маршрутизаторы, использующие протоколы с маршрутизацией по состоянию канала, рассылают друг другу пакеты LSA. Эта рассылка в значительной степени заполняет сеть и временно уменьшает полосу пропускания, доступную для передачи данных пользователей. После этого временного переполнения протоколы состояния канала обычно требуют лишь минимальной полосы пропускания для рассылки нечастых или вызванных особыми изменениями в сети пакетов LSA, отражающих эти изменения.

Третий тип протоколов маршрутизации, называемых протоколами сбалансированной гибридной маршрутизации, соединяет в себе черты как дистанционно-векторных протоколов, так и протоколов с учетом состояния каналов связи. Протоколы сбалансированной гибридной маршрутизации для определения наилучших маршрутов используют векторы расстояния с более точными метриками. Однако они отличаются от дистанционно-векторных протоколов тем, что обновления баз данных маршрутизации происходят не периодиче-

ски, а только при изменении топологии сети. Они отличаются от дистанционно-векторных протоколов и от протоколов с учетом состояния канала связи еще и тем, что они в меньшей степени используют полосу пропускания, память и создают меньшую нагрузку на процессор для обработки служебной информации. Пример гибридного протокола – протокол EIGRP.

Конфигурирование службы маршрутизации. Для включения на маршрутизаторе протокола IP-маршрутизации должны быть установлены как глобальные, так и локальные параметры интерфейса. Глобальные установки включают в себя выбор протокола маршрутизации, такого, как IGRP, EIGRP или OSPR. Главной задачей, решаемой в режиме конфигурирования, является указание IP-адресов сетей. При динамической маршрутизации для связи с маршрутизаторами используются широковещательные адреса многоадресатной рассылки. Для поиска наилучших маршрутов к каждой сети или подсети маршрутизаторы используют какую-либо метрику маршрутизации.

Процесс конфигурирования маршрутизации начинается с выполнения команды router. Эта команда имеет следующий синтаксис:

```
router(config)#router protocol (process-id autonomous-system)
```

где под параметром protocol понимается один из протоколов маршрутизации: RIP, IGRP или EIGRP. Параметр process-id или autonomous-system содержит идентификатор процесса маршрутизации или номер автономной системы, используемой в протоколах IGRP и EIGRP.

Команда network позволяет протоколу маршрутизации идентифицировать интерфейсы, которые принимают участие в отправке и получении сообщения об обновлении маршрутов. Команда network имеет следующий синтаксис:

```
router(config-router)#network network-number
```

где параметр network-number представляет собой номер (IP-адрес) непосредственно подсоединенной сети.

Дня протоколов RIP и IGRP номер сети должен базироваться на классах сетевых адресов, а не на адресах подсетей или на индивидуальных адресах узлов.

В качестве возможных адресов сетей могут выступать только номера (т. е. адреса) сетей классов A, B или C.

- На Internet-уровне стека протоколов TCP/IP маршрутизатор может использовать протокол IP-маршрутизации для осуществления маршрутизации путем реализации конкретного алгоритма.

Протокол маршрутной информации был первоначально определен в документе RFC 1058 в 1988 г. Наиболее существенны его следующие характеристики:

- RIP является дистанционно-векторным протоколом маршрутизации;
- в качестве метрики при выборе маршрута используется количество переходов;
- если количество переходов становится больше 15, пакет отбрасывается;
- стандартно обновления маршрутизации (routing updates) рассылаются широковещательным способом каждые 30 секунд.

Протокол RIP с течением времени претерпел значительную эволюцию: от основанного на классах протокола маршрутизации RIP первой версии к бесклассовому протоколу RIP второй версии. Усовершенствования протокола RIP-2 включают в себя:

- способность переносить дополнительную информацию о маршрутизации пакетов;
- механизм аутентификации для обеспечения безопасного обновления таблиц маршрутизации;
- способность поддерживать маски подсетей.

Протокол RIP предотвращает появление петель в маршрутизации, по которым пакеты могли бы циркулировать очень долго, устанавливая максимально допустимое количество переходов на маршруте от отправителя к получателю. При получении маршрутизатором обновления маршрутов, содержащего новую или измененную запись, он увеличивает значение метрики на единицу. Если при этом значение метрики превышает 15, то оно считается бесконечно большим, и сеть получателя считается недостижимой. Протокол RIP обладает рядом функций, которые являются общими для него и других протоколов маршрутизации. Например, он позволяет использовать механизмы *расщепления горизонта* и *таймеры удержания информации* для предотвращения распространения некорректных сведений о маршрутах.

Конфигурирование протокола RIP. Команда router rip включает RIP в качестве протокола маршрутизации. После этого выполняется команда network для указания протоколу сетей, которые непосредственно подсоединены к маршрутизатору и должны быть им анонсированы. После выполнения указанных двух действий в процессе маршрутизации, интерфейсы логически связываются с сетевыми адресами.

Для обновления маршрутов в случае изменения топологии сети протокол RIP в реализации компании Cisco использует *мгновенные анонсы* (event-triggered или event-driven). Мгновенные обновления значительно ускоряют конвергенцию таблиц маршрутизации и, следовательно, снижают риск образования петель маршрутизации.

Маршрутизатор при получении сообщения об обновлении, содержащего изменения, обновляет свою таблицу маршрутизации для отображения в ней нового маршрута. Значение метрики при этом увеличивается на единицу, а интерфейс отправителя обновления указывается в качестве следующего транзитного перехода на маршруте. Маршрутизаторы RIP вписывают только наилучший маршрут к пункту назначения, в то же время они могут поддерживать и несколько маршрутов, имеющих одинаковое значение метрики.

После обновления таблицы маршрутизации вследствие изменения топологии сети маршрутизатор сразу начинает рассылать сообщения об обновлении маршрутов, для того чтобы проинформировать другие маршрутизаторы о произошедших изменениях. Обновления рассылаются независимо от обычных регулярных сообщений RIP-маршрутизаторов. Если обновление пересылается через интерфейс другой суперсети с несовпадающим суммарным адресом, то

протокол RIP анонсирует только сети, основанные на классах или сети главного класса. Иными словами, информация о подсетях не суммируется к одному агрегированному адресу, а пересылается в виде отдельных записей, если анонс пересылается через интерфейс, адрес которого принадлежит той же суперсети.

Для включения на маршрутизаторе протокола RIP используются команды режима глобального конфигурирования:

Router(config)#router RIP // Включает процесс RIP-маршрутизации, после чего устройство переходит в режим конфигурирования

Router(config-router)#network // Связывает сеть с процессом RIP-маршрутизации

Приведенные ниже команды иллюстрируют процесс включения на маршрутизаторе протокола RIP и указания ему непосредственно подсоединенных сетей:

BHM(config) flrouter rip // Включение протокола маршрутизации RIP

BHM(config-router)#network 1.0.0.0 // Указание на непосредственно подключенную к устройству сеть

BHM(config-router)#network 2.0.0.0 // Указание на непосредственно подключенную к устройству сеть

Интерфейсы маршрутизатора Cisco, подсоединенные к сетям 1.0.0.0 и 2.0.0.0, рассылают и получают обновления протокола RIP. Эти обновления позволяют данному маршрутизатору изучить сетевую топологию с помощью соседних маршрутизаторов, на которых также включен протокол RIP.

В команде network протокола RIP можно указывать только классовые сети или суперсети. Если на одном или более интерфейсах маршрутизатора используются подсети такой сети, то для ее подключения можно использовать команду network с указанием классового адреса сети. Если же администратор попытается указать в данной команде подсеть, программное обеспечение автоматически преобразует такой адрес в адрес классовой сети, в чем можно убедиться с помощью команды show running-config.

7.2. Задание для лабораторной работы

Вы – администратор корпоративной локальной сети, состоящей из трех различных подсетей (рис. 7.3):

192.168.0.0 /24

192.168.1.0 /24

192.168.2.0 /24

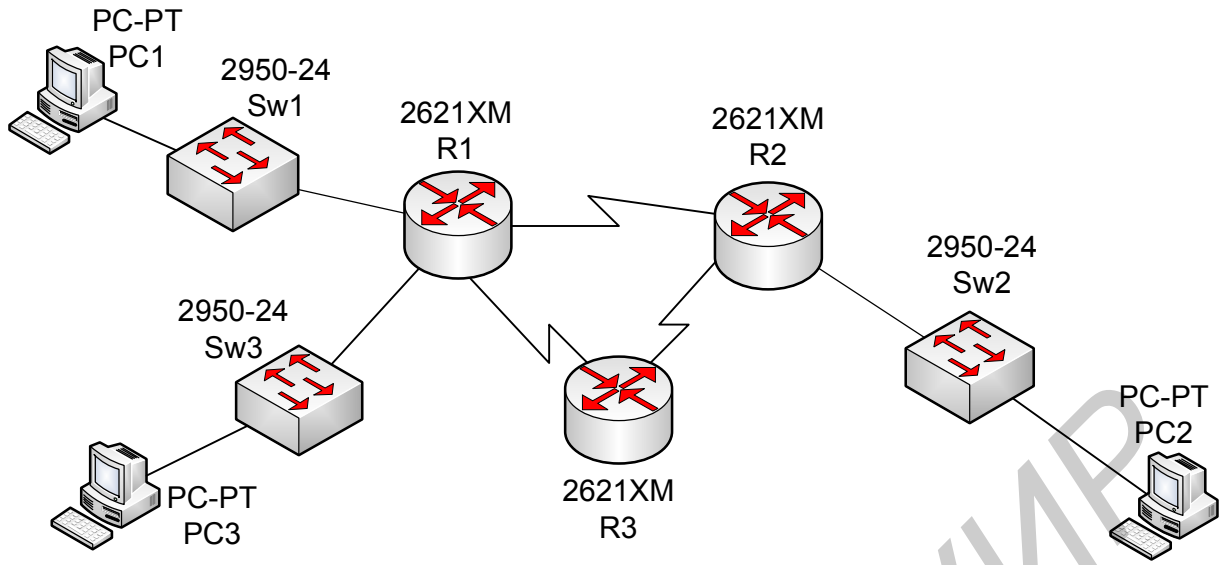

Рис. 7.3. Состав локальной сети

Маршрутизация осуществляется с помощью трёх маршрутизаторов R1, R2 и R3, соединенных между собой соединением Serial.

1. Настройте интерфейсы маршрутизаторов. Обратите внимание, что соединение Serial требует назначение со стороны DCE-устройств параметра clock rate. Задайте clock rate равным 56 000.

Для маршрутизатора R1:

Включите маршрутизатор.

Сконфигурируйте интерфейс serial 1/0, используя ip address 192.168.4.1 /30.

Сконфигурируйте интерфейс serial 1/1, используя ip address 192.168.6.1 /30.

Сконфигурируйте интерфейс Fast Ethernet 0/0, используя ip address 192.168.0.1 /24.

Для маршрутизатора R2:

Включите маршрутизатор.

Сконфигурируйте интерфейс serial 1/0, используя ip address 192.168.6.2 /30.

Сконфигурируйте интерфейс serial 1/1, используя ip address 192.168.5.1 /30.

Сконфигурируйте интерфейс Fast Ethernet 0/0, используя ip address 192.168.1.1 /24.

Для маршрутизатора R3:

Включите маршрутизатор.

Сконфигурируйте интерфейс serial 1/0, используя ip address 192.168.4.2 /30.

Сконфигурируйте интерфейс serial 1/1, используя ip address 192.168.5.2 /30.

Сконфигурируйте интерфейс Fast Ethernet 0/0, используя ip address 192.168.2.1 /24.

2. Настройте проколол маршрутизации RIP. После обновления таблиц маршрутизации проверьте доступность подсетей.

7.3. Содержание отчета

1. Цель работы.
2. Схема сети.
3. Конфигурационные файлы маршрутизаторов.
4. Выводы.

7.4. Контрольные вопросы

1. Что такое метрика?
2. Какие вы знаете основные характеристики, используемые в метриках?
3. Что такое протокол маршрутизации и маршрутизируемый протокол, в чем их различия?
4. Что такое автономная система и зачем она нужна?
5. Какие категории (классы) протоколов маршрутизации вы знаете?
6. Как происходит процесс обнаружения сетей при маршрутизации по состоянию канала?
7. Что такое протокол RIP?

Лабораторная работа №8

ПРОТОКОЛ IGRP

Цель работы: ознакомиться с характеристиками протокола маршрутизации IGRP, а также получить практические навыки в его настройке.

8.1. Теоретические сведения

Как и RIP, протокол маршрутизации внутреннего шлюза (IGRP) является дистанционно-векторным протоколом маршрутизации. Данный протокол разработан фирмой CISCO для своих многопротокольных маршрутизаторов. Протокол IGRP прост в реализации, но вместе с тем является более развитым протоколом маршрутизации по сравнению с протоколом RIP и позволяет использовать большее количество параметров для определения наилучшего маршрута к пункту назначения.

IGRP представляет собой дистанционно-векторный протокол внутреннего шлюза. Дистанционно-векторные протоколы маршрутизации определяют наилучший маршрут путем сравнения соответствующих числовых величин, отражающих длину маршрутов. Измерение такой длины называется построением *вектора расстояния* (distance vector). Маршрутизаторы, использующие дистанционно-векторные протоколы, должны регулярно рассылать свои таблицы маршрутизации полностью или частично в сообщениях об обновлениях маршрутов всем соседним маршрутизаторам.

По мере того как информация маршрутизации будет распространяться по сети, маршрутизаторы могут, в частности, выполнять следующие функции:

- обнаруживать новые пункты назначения;
- обнаруживать ставшие недействительными маршруты.

Протокол IGRP рассылает обновления маршрутизации с 90-секундными интервалами, анонсируя сети, принадлежащие конкретным автономным системам. Основные достоинства протокола IGRP:

- стабильность маршрутов даже в очень больших и сложных сетях;
- быстрый отклик на изменения топологии сети;
- минимальная избыточность. Поэтому IGRP не требует дополнительной пропускной способности каналов для своей работы;
- разделение потока данных между несколькими параллельными маршрутами, примерно равного достоинства;
- учет частоты ошибок и уровня загрузки каналов;
- возможность реализовать различные виды сервиса для одного и того же набора информации.

Стандартно в качестве параметров метрики используются только полоса пропускания и задержка. Протокол IGRP использует составную метрику, которая вычисляется как функция полосы пропускания, задержки, загрузки и

надежности канала в том случае, если их коэффициенты явно заданы в конфигурации. Метрики протокола IGRP включают в себя следующие компоненты:

- *полоса пропускания* (Bandwidth) – выбирается наибольшее значение ширины полосы пропускания на маршруте;
- *задержка* (*Delay*) – кумулятивная задержка на интерфейсах при прохождении пакетов по маршруту;
- *надежность* (Reliability) – описывает надежность канала, ведущего к пункту назначения; эта величина определяется в процессе обмена тестовыми сообщениями;
- *загрузка канала* (Load), ведущего к пункту назначения; это значение выражается в битах в секунду.

Значения задержки и полосы пропускания не измеряются в процессе работы устройством, а задаются в конфигурации командами delay и bandwidth определенного интерфейса. Для нахождения ширины полосы пропускания необходимо выбрать наименьшее ее значение среди всех выходных интерфейсов и разделить 10 000 000 на это значение (выражается в кбит/с с коэффициентом 10 000 000). Для вычисления задержки необходимо сложить ее значения для всех выходных интерфейсов и разделить это значение на 10 (в десятках долей микросекунды). Наилучшим считается маршрут с наименьшей метрикой.

С помощью команды show ip protocols отображаются параметры, фильтры и другая сетевая информация о протоколах маршрутизации. Такая информация необходима для определения параметров К1 – К5 и включает в себя максимальное количество переходов; она также используется для вычисления составной метрики протокола IGRP:

Метрика = [К1·полоса пропускания + К2·полоса пропускания/(256 – загрузка) + К3·задержка] [К5/(надежность + К4)].

Параметр метрики К1 представляет собой весовой коэффициент, определяющий важность величины ширины полосы пропускания, а К3 – задержки. Стандартным значением коэффициентов К1 и К3 является единица, К2, К4 и К5 – ноль, загрузка лежит в интервале от 1 до 255. В случае если К5 = 0, используется упрощенная формула расчета метрики, в которой компонент надежности [К5/(надежность + К4)] опущен. Композитная метрика рассчитывается по формуле

Метрика = Полоса пропускания + Задержка.

Значения параметров метрики К в указанных формулах являются постоянными и могут быть заданы с помощью следующей команды режима конфигурирования маршрутизатора:

metric weights *tos* Kl К2 К3 К4 К5

В примере 8.1 показано действие команды show ip route. В квадратных скобках отображаются значения метрик протокола IGRP. Первое значение представляет собой административное расстояние, а второе – вычисленное значение метрики. Канал с большей шириной полосы пропускания имеет

меньшую метрику, аналогично маршрут с наименьшей задержкой также имеет меньшую метрику.

Пример 8.1. Действие команды show ip route

```
RouterAtt#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 El - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, LI - TS-TS level-1, L2 - TS-TS level-2, via - TS-TS inter area
* - candidate default, V - per-user static route,
o - ODR P - periodic downloaded static route
Gateway of last resort is not set
C       192.168,1.0/24is directly connected, FastEthernetO/0
C       192,168.2.0/24is directlyconnected, SerialO/0
T       192.168.3.0/24 [100/30135] via 192.168.2.2, 00:00:30,SerialO/0
```

Маршруты протокола IGRP. Протокол IGRP анонсирует три типа маршрутов:

- *внутренний* (Inferior route) – представляет собой маршрут между подсетями сети, подсоединенной к интерфейсу маршрутизатора. Если сеть, подсоединенная к маршрутизатору, не имеет подсетей, то внутренние маршруты не анонсируются;
- *системный* (System route) – представляет собой маршрут между сетями, находящимися в одной автономной системе. Программное обеспечение Cisco IOS создает системные маршруты на основе интерфейсов непосредственно подсоединенных сетей и информации, полученной от других IGRP-маршрутизаторов или серверов доступа. Системные маршруты не содержат информацию о подсетях;
- *внешний* (Exterior route) – представляет собой маршрут к сетям, находящимся вне рассматриваемой автономной системы, которые устанавливаются при поиске стандартного шлюза. Программное обеспечение Cisco IOS выбирает стандартный шлюз из списка внешних маршрутов, предоставляемого протоколом IGRP. Такой стандартный шлюз (маршрутизатор) используется программным обеспечением в том случае, если не найден лучший маршрут и сеть получателя не является непосредственно подсоединенной сетью. Если автономная система имеет более одного соединения с внешней сетью, то разные маршрутизаторы могут выбрать в качестве стандартного шлюза различные внешние маршрутизаторы.

Протокол IGRP обладает рядом функций, предназначенных для повышения устойчивости работы сети:

- *таймеры удержания информации* (Holddown);
- *механизм расщепления горизонта* (Split horizon);
- *удаление маршрута в обратном направлении* (Poison reverse update).

Таймеры удержания информации используются для предотвращения рассылки обновлений маршрутизации, содержащих маршруты, которые в дей-

ствительности неработоспособны. Если маршрутизатор выходит из строя, то соседние маршрутизаторы определяют такое его состояние по отсутствию регулярных сообщений об изменении маршрутизации.

Использование механизма расщепления горизонта основано на предположении, что обычно нецелесообразно посылать информацию о маршруте в том же направлении, по которому она была получена. Расщепление горизонта предотвращает появление кольцевых маршрутов между смежными маршрутизаторами, однако для предотвращения петель большей протяженности требуется использование другого механизма – удаления маршрута. Строго говоря, увеличение метрики маршрутизации обычно указывает на появление петель маршрутизации.

Удаление маршрута в обратном направлении происходит посредством рассылки уведомлений для отмены маршрута и перевода его в состояние удержания. В протоколе IGRP такие сообщения рассылаются только в том случае, если метрика маршрута увеличилась в 1,1 раза или более.

Протокол IGRP также поддерживает ряд таймеров и переменных, в которых содержатся временные интервалы, влияющие на работу механизма маршрутизации. Эти таймеры и их параметры описаны ниже:

- *таймер обновления* (Update timer) задает частоту, с которой рассылаются сообщения об обновлении маршрутизации. Стандартно его значение равно 90 секундам;
- *таймер действительности маршрута* (Invalid timer) задает промежуток времени ожидания, в течение которого маршрутизатор, не получая сообщения об обновлении по определенному маршруту, не рассылает информацию перед объявлением этого маршрута недействительным. В протоколе IGRP стандартно устанавливается значение в три раза больше, чем период регулярной рассылки анонсов маршрутов;
- *таймер удержания информации* (Hold time*r*) задает время, в течение которого информация о ненадежных маршрутах игнорируется. В протоколе IGRP стандартным значением является утроенное значение периода рассылки анонсов маршрутов;
- *таймер сброса маршрута* (Flush timer) задает время до того момента, когда маршрут будет удалён из таблицы маршрутизации. Стандартно значение этого параметра в семь раз больше периода рассылки анонсов маршрутизации.

Для конфигурирования процесса маршрутизации протокола IGRP используется команда глобального конфигурирования router igrp:

```
RouterA(config)#router igrp as-number
```

Для отключения процесса IGRP-маршрутизации используется форма этой команды с ключевым словом «no».

Под *номером автономной системы* понимается номер, идентифицирующий процесс маршрутизации протокола IGRP. Следует помнить, что такой номер необязательно должен быть реальным номером автономной системы, который присваивает соответствующая международная организация, или

номером частной автономной системы. Такой номер действует только внутри домена маршрутизации протокола IGRP и должен быть одинаков на всех маршрутизаторах, обменивающихся информацией по протоколу IGRP. Он также используется для маркировки информации о маршрутизации.

Для задания списка сетей процессов IGRP-маршрутизации используется команда network режима конфигурирования маршрутизатора.

Для удаления сети из списка используется форма этой команды с ключевым словом «no», аналогично отключается сам процесс маршрутизации протокола IGRP.

В примере 8.2 показана конфигурация протокола IGRP на маршрутизаторах RouterA и RouterB, принадлежащих автономной системе с номером 101.

Пример 8.2. Конфигурирование протокола IGRP

```
RouterA(config)# router igrp 101
RouterA(config-router)#network
RouterA(config-router)# network 192.168.2.0
RouterE(config)# router igrp 101
RouterB(config-router)# network 192.168.2.0
RouterE(config-router)# network
```

Для проверки правильности конфигурации протокола IGRP используется команда show ip route и анализируются маршруты IGRP, отмеченные символом «i».

Дополнительно используются следующие команды проверки конфигурирования протокола IGRP:

- команда show interface позволяет проверить правильность конфигурирования Ethernet-интерфейса;
- команда show running-config указывает, включен ли в маршрутизаторе протокол IGRP;
- команда show running-config interface проверяет правильность конфигурации IP-адреса;
- команда show running-config begin interface проверяет, включен ли протокол IGRP на интерфейсах маршрутизатора, начиная с указанного в команде интерфейса;
- команда show running-config begin igrp проверяет, включен ли в маршрутизаторе протокол IGRP;
- команда show ip protocol*s* проверяет функционирование протокола IGRP.

Большинство ошибок в конфигурации протокола IGRP связано с неверными параметрами команды network, неверным указанием подсетей, или номеров автономных систем.

При поиске и устранении ошибок в конфигурации протокола IGRP используются следующие команды:

- команда show ip protocols – для отображения общей информации протоколу IP-маршрутизации; команда show ip route используется для отображения таблицы IP-маршрутизации;
- команда debug ip igrp events – для отображения информации общего

характера о маршрутизации для данной сети;

- команда debug ip igrp transactions отображает сообщения, полученные от соседних маршрутизаторов, на которых запрашивается обновление маршрутов, и широковещательные сообщения, посылаемые маршрутизатором-инициатором соседнему маршрутизатору;
- команда ping – для определения доступности конкретного IP-адреса;
- команда traceroute – для трассировки пути перемещения пакета от компьютера пользователя к узлу сети Internet; при этом выводится число требуемых переходов и время, затрачиваемое на такие переходы.

8.2. Задание для лабораторной работы

Вы – администратор корпоративной локальной сети, состоящей из трех различных подсетей (рис. 8.1).

1. Выполните настройку интерфейсов маршрутизаторов аналогично настройке интерфейсов маршрутизаторов, описанной в лабораторной работе №7.

2. Настройте протокол маршрутизации IGRP для автономной системы 101. После обновления таблиц маршрутизации проверьте доступность одной подсети из другой.

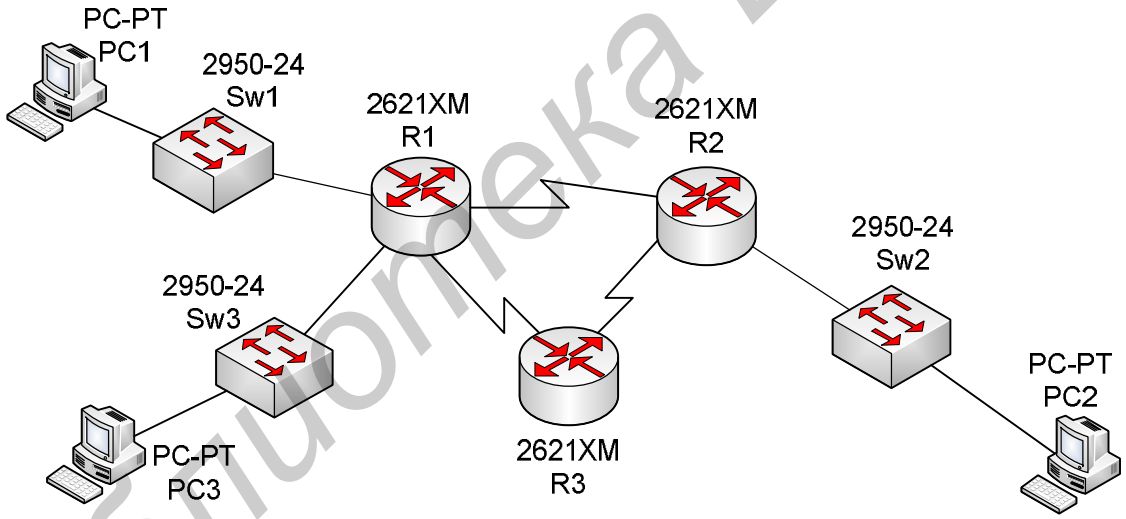

Рис. 8.1. Состав локальной сети

8.3. Содержание отчета

1. Цель работы.
2. Схема топологии сети.
3. Конфигурационные файлы маршрутизаторов.
4. Выводы.

8.4. Контрольные вопросы

1. Какие функции протокола IGRP вы можете назвать?
2. Что входит в метрики протокола IGRP?
3. Охарактеризуйте типы маршрутов протокола IGRP.
4. Перечислите таймеры протокола IGRP.
5. Какие команды используются для настройки и поиска ошибок в рамках протокола IGRP?

ЛИТЕРАТУРА

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – 3-е изд. – СПб. : Питер, 2007. – 958 с.
2. Танненбаум, Э. Компьютерные сети / Э. Танненбаум. – 4-е изд. – СПб. : Питер, 2007. – 993 с.
3. CCNA 2: Routers and Routing Basics v.3.0. Student Lab Manual. – Cisco Systems Inc., 2003. – 300 с.

Св. план 2009, поз. 104

Учебное издание

Гурский Александр Леонидович
Беляев Борис Илларионович
Зельманский Олег Борисович
Петров Сергей Николаевич

КОМПЬЮТЕРНЫЕ СЕТИ

Методические указания к лабораторным работам
для студентов специальностей
1-45 01 03 «Сети телекоммуникаций»,
1-98 01 02 «Защита информации в телекоммуникациях»
всех форм обучения

Редактор Л. А. Шичко
Корректор Е. Н. Батурчик

Подписано в печать 26.01.2010.	Формат 60×84 1/16.	Бумага офсетная.
Гарнитура «Таймс».	Отпечатано на ризографе.	Усл. печ. л. 4,3.
Уч.-изд. л. 4,5.	Тираж 100 экз.	Заказ 395.

Издатель и полиграфическое исполнение: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6