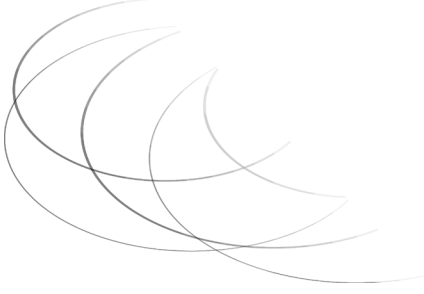
Джо Хабракен

Маршрутизаторы Cisco

Практическое применение

Practical Cisco Routers



Joe Habraken

QUE®

A Division of Macmillan Computer Publishing, USA, 201 W. 103rd Street

Indianapolis, Indiana 46290

Маршрутизаторы Cisco

Практическое применение

Джо Хабракен

Серия
«Защита и администрирование»

ДМК Пресс
издательство
Москва

УДК 004.715
ББК 32.973.202-018.2
Х12

Хабракен Д.
Х12 Маршрутизаторы Cisco. Практическое применение: Пер. с англ. – М.: ДМК Пресс. – 320 с.: ил. (Серия «Защита и администрирование»).

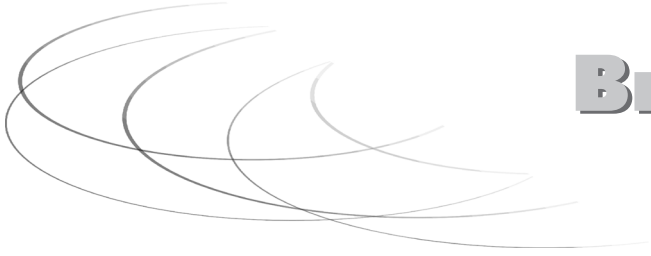
ISBN 5-94074-123-1

В книге рассказывается об основных принципах работы LAN- и WAN-соединений, рассматриваются концепции и технологии маршрутизации различных сетевых протоколов, а также описываются принципы функционирования маршрутизаторов Cisco и сетевой операционной системы Cisco IOS. В изложении материала используется последовательный и систематический подход, который включает пошаговое описание наиболее часто применяемых команд, функций, систему подсказок и решений для самых распространенных проблем.

Издание может послужить незаменимым учебником для новичков, стремящихся освоить сетевые технологии, а также справочным пособием для профессионалов, которые хотят более подробно изучить принципы работы маршрутизаторов Cisco.

ISBN 0-7897-2103-1 (англ.)
ISBN 5-94074-123-1 (рус.)

Содержание



Введение

Компьютерные технологии поразительно быстро развились за последние десять лет. Те из них, которые ранее считались слишком дорогими или сложными для малой и средней компании, в настоящее время внедряются с головокружительной скоростью. Устройства межсетевого взаимодействия, в особенности маршрутизаторы, – один из примеров таких «технологий для крупных компаний», используемых сегодня даже небольшими организациями.

Недорогие низкопроизводительные маршрутизаторы обеспечивают связь с поставщиками услуг и коммутируемую телефонную сеть малым компаниям и частным лицам, испытывающим потребность в увеличении пропускной способности вследствие все более широкого распространения Internet как инструмента коммуникации и маркетинга. По мере своего роста компании ищут способы сохранить пропускную способность собственных локальных сетей. Одним из популярных решений данной проблемы стала сегментация локальных сетей с помощью маршрутизаторов.

Сетевые технологии захлестнули деловой мир, соответственно выросла потребность в профессионалах, умеющих настраивать, поддерживать и обслуживать маршрутизаторы и другие устройства сетевого взаимодействия. Уже издано несколько книг и учебных материалов по продукции Cisco, однако большинство из них предназначено для опытных специалистов в области информационных технологий. Книги, которая излагала бы основы межсетевого взаимодействия, до настоящего момента не было.

Об этой книге

Начиная писать настоящую книгу, я преследовал две цели: рассказать о межсетевом взаимодействии и конфигурировании маршрутизаторов Cisco и познакомить новичков с тем, что представляет собой эта технология. Я стремился создать цельный учебный инструмент, чтобы сделать книгу полезной тому, кто, имея лишь небольшие знания о межсетевых взаимодействиях, вдруг столкнулся в работе с маршрутизаторами Cisco. И хотя это звучит нескромно, я знал, что моя книга будет полезной.

Структура книги

В части I, «Обзор сетей», рассмотрены некоторые сетевые технологии. Приведено описание локальных и глобальных сетей, а также межсетевого взаимодействия. Одна из глав посвящена эталонной модели взаимодействия открытых систем (модель OSI) и способам ее применения к реальным сетевым протоколам. Основы работы маршрутизаторов также включены в эту часть книги.

Прочитав часть II, «Устройство маршрутизатора и основная конфигурация», вы узнаете об аппаратных компонентах типичного маршрутизатора Cisco, об основной конфигурации маршрутизаторов и о межсетевой операционной системе Cisco – Cisco IOS.

В части III, «Маршрутизация протоколов локальных сетей», рассказывается о распространенных протоколах локальных сетей: TCP/IP, IPX/SPX и AppleTalk, а также описывается процедура конфигурирования маршрутизатора Cisco для каждого из протоколов.

Часть IV, «Дополнительные возможности конфигурирования», содержит информацию о некоторых технологиях широкомасштабных сетей и их конфигурировании на маршрутизаторе Cisco, освещает вопросы ограниченного доступа и устранения неисправностей. Здесь вы найдете также описание программного обеспечения ConfigMaker.

Для кого предназначена эта книга

Книга адресована всем, кому нужно изучить основы межсетевого взаимодействия или конфигурирования маршрутизаторов Cisco[1]. Работаете вы на крупную компанию, небольшую фирму или только начинаете интересоваться сетями, эта книга послужит вам хорошим подспорьем.

Принятые обозначения

Команды, указания и пояснения представлены в этой книге в предельно ясной форме. Отметим лишь некоторые отличительные черты оформления текста, упрощающие его восприятие.

Команды, которые нужно вводить, выделены моноширинным шрифтом. Например, команда, позволяющая получить сведения об инкапсуляции (настройка WAN-протокола) на последовательном интерфейсе, выглядит в книге так: `show interface serial 0`.

[1] В тексте книги встречается множество адресов ресурсов Internet. В связи с динамическим характером глобальной сети возможны изменения некоторых адресов. В этом случае рекомендуется зайти на главную страницу указанного сайта и произвести поиск необходимого ресурса с нее. – *Прим. научн. ред.*

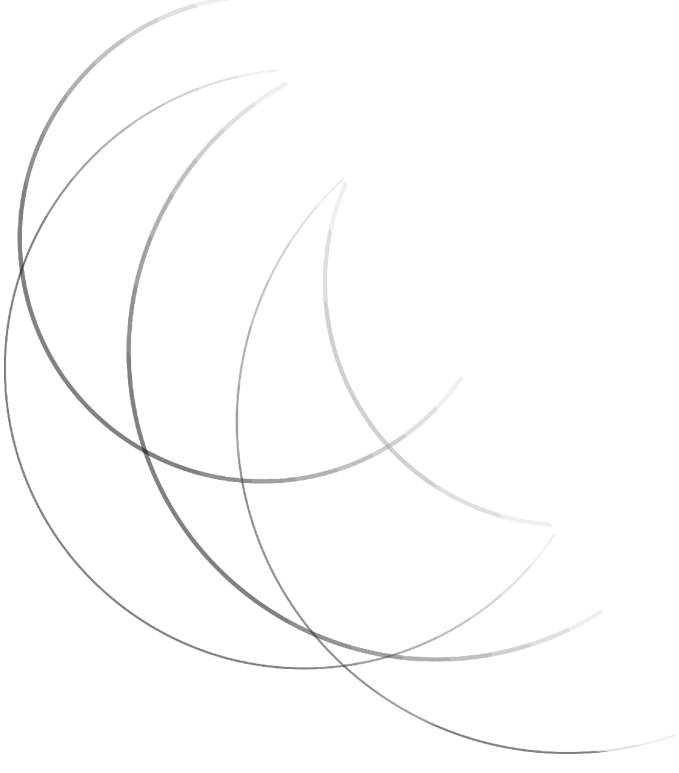
Если несколько клавиш (они выделяются **полужирным шрифтом**) необходимо нажать одновременно, их комбинация сопровождается знаком «плюс», например **Ctrl**+**P**.

Термин, который встречается впервые, выделяется *курсивом* и снабжается определением.

Этим значком отмечены ссылки на главы и/или разделы, в которых более подробно освещается указанная тема.

Дополнительная информация и авторские комментарии помещены на сером фоне, чтобы их было проще отличить от основного текста.

ЧАСТЬ I



Обзор сетей

ГЛАВА 1

Локальные сети

За последние тридцать лет в области компьютерных технологий произошли значительные изменения. В 60-х годах XX века вычисления проводились на огромных ЭВМ. Пользователь такого централизованного компьютера взаимодействовал с ним через посредника – администратора информационной системы или программиста. Со временем пользователи больших ЭВМ получили возможность напрямую связываться с компьютером посредством терминала (как правило, это монитор и клавиатура, аппаратно подключенные к ЭВМ). В 70-х годах на первый план вышли мини-ЭВМ, что сделало компьютерные технологии доступными большему числу компаний и организаций (хотя за это приходилось платить). Однако хранение данных и возможность производить вычисления все еще были централизованы, как и в эпоху больших ЭВМ.

В 80-х годах в мире вычислительной техники произошла революция: появился персональный компьютер (в частности, производства компании IBM), позволивший сосредоточить вычислительные ресурсы на рабочих местах пользователей. Компьютер нового типа был не только простым в использовании (по сравнению с большими и малыми ЭВМ), но и доступным по цене. Единственным недостатком такой технологии стала невозможность объединить компьютеры в группу и создать общие ресурсы: изолированность персональных компьютеров не позволяла им обмениваться информацией.

Объединение персональных компьютеров в сети

Чтобы преодолеть децентрализованность персональных компьютеров, в 80-х и 90-х годах было разработано аппаратное и программное обеспечение для включения ПК в сеть с разделяемыми ресурсами, такими как принтеры и файлы. Объединенные в сеть компьютеры позволили создать коллективную вычислительную среду для любой ситуации в бизнесе. В такой среде компьютеры могут располагать различными общими ресурсами: аппаратными (принтеры, модемы), программными (прикладное программное обеспечение), файловыми (файлы и каталоги).

В зависимости от специфики требований появились различные модели сетей. В ситуации, когда нескольким компьютерам требуются одни и те же конкретные аппаратные устройства (например, принтер), но нет необходимости в централизованном хранении файлов, возникла *одноранговая сеть* (peer-to-peer network). Пользователь обращается к ней только в тех случаях, когда ему необходимо отправить документ на печать.

Альтернативой одноранговому решению стала сеть с большей степенью централизации управления ресурсами и более высоким уровнем безопасности – *серверная сеть* (server-based network). Здесь применяется специальный компьютер-сервер, который проверяет права пользователей и обеспечивает центральное хранение файлов, а также доступ к различным аппаратным и программным ресурсам. Рассмотрим различия между этими моделями подробнее.

Одноранговые сети

Одноранговая сеть дает возможность работать с такими общими ресурсами, как файлы и принтеры, без помощи сервера. Равноправные компьютеры действуют и как *клиенты* (пользуются ресурсами), и как *серверы* (предоставляют ресурсы). Для построения одноранговой сети необходимы лишь установка на всех ПК операционной системы, поддерживающей подобную организацию сети, и их физическое соединение.

Некоторые операционные системы, в частности Windows 3.11, Windows 95/98 и Windows NT Workstation, имеют встроенные средства для организации одноранговой сети. Локальные диски, папки и принтеры могут находиться в общем пользовании (рис. 1.1).

Каждому совместно используемому ресурсу (например, диску или принтеру) разрешается присвоить свой пароль для доступа. Одно из неудобств одноранговой сети:

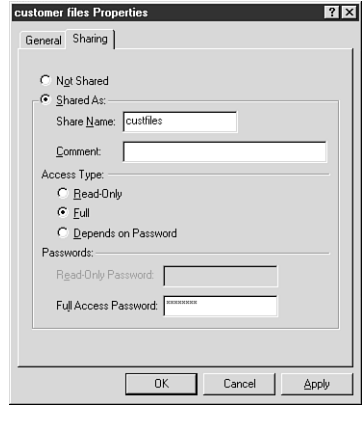


Рис. 1.1. Операционная система Windows 98 может предоставить ресурс в совместное пользование

если в коллективном доступе находится много ресурсов, то нужно помнить все пароли к ним. Такой тип защиты называют *защитой на уровне доступа*[1].

> *Если вы организуете одноранговую сеть, не заботясь о защите информации, поскольку все пользователи знакомы между собой и доверяют друг другу, можете совсем не назначать пароли или наделить ресурсы одним и тем же паролем. Так будет более удобно работать с различными ресурсами, но они становятся доступными каждому, кто физически подсоединится к сети.*

Одноранговые сети не требуют дополнительного администрирования, поскольку каждый пользователь распоряжается ресурсами на собственном компьютере. Тем не менее такие сети обладают рядом недостатков:

- из-за коллективного пользования компьютеру требуется большая производительность;
- отсутствие централизованного размещения общих файлов затрудняет создание резервных копий;
- необходимо применять защиту на уровне ресурсов;
- децентрализованность усложняет поиск конкретного ресурса;
- пользователям приходится запоминать множество паролей.

Одноранговая сеть – быстрый и дешевый способ объединения нескольких компьютеров, однако она способна вместить лишь небольшое количество пользователей. Такая сеть не масштабируема (то есть не расширяема, поскольку большинство одноранговых сетей ограничены десятью равноправными ПК) и, очевидно, не подходит для растущей компании.

Администраторы информационных систем единодушны во мнении, что одноранговые сети идеально функционируют не более чем с пятью равноправными компьютерами.

➢ Подробнее о физических соединениях рассказывается ниже, в разделе «Сетевые адаптеры».

Серверные сети

Серверные сети обеспечивают большую степень централизации управления ресурсами и, если требуется, расширяемость сети. Компьютер-сервер – это, как правило, специальная машина, регистрирующая пользователей и предоставляющая им ресурсы. Сервер проверяет права каждого пользователя, поэтому в такой сети легче

[1] В одноранговой сети Windows NT для общих ресурсов применяется защита на уровне пользователей. Вместо пароля общий ресурс имеет атрибут Список доступа (Access Control List – ACL), определяющий, какие пользователи или группы обладают тем или иным уровнем доступа к данному ресурсу. – *Прим. научн. ред.*

распоряжаться ресурсами, если определить для разных пользователей различные уровни доступа. Имя и пароль дают пользователю возможность войти в сеть и получить доступ к любому ресурсу в рамках соответствующих разрешений.

В качестве сервера в такой сети обычно применяется более мощный (в смысле скорости процессора, объема оперативной памяти и дискового пространства) компьютер. Помимо аппаратного обеспечения, позволяющего обрабатывать большое количество пользовательских запросов, сервер должен также иметь и специальное программное обеспечение – сетевую операционную систему. Широко используются две сетевые ОС: Microsoft Windows NT Server и Novell NetWare.

Серверные сети, как уже было отмечено, масштабируемы, то есть способны расти вместе с вашей компанией. К такой сети могут добавляться новые серверы, выполняющие различные задачи. Например, один сервер занимается подключением и проверкой прав пользователей (в частности, главный контроллер домена в сети Windows NT), а другой управляет системой электронной почты (сервер коммуникаций). В табл. 1.1 представлен список некоторых специальных серверов, подходящих для локальных сетей.

Таблица 1.1. Типы серверов в локальных сетях

Тип сервера	Применение
Файловый	Хранит файлы и каталоги общего доступа и предоставляет пользователям дисковое пространство для домашних директорий (например, сервер Novell NetWare)
Коммуникационный	Обеспечивает такие услуги связи, как электронная почта (в частности, сервер Microsoft Exchange)
Сервер приложений	Обеспечивает доступ к базе данных или другому приложению (например, SQL-сервер)
Сервер печати	Поддерживает очередь печати и другие сервисы, связанные с сетевой печатью

Серверная сеть, занимающая сравнительно небольшое пространство (скажем, расположенная в пределах одного здания), называется *локальной сетью* (local area network – LAN). Локальные сети встречаются в малых, средних и больших компаниях. Когда несколько локальных сетей соединяются, образуется *интерсеть* (internetwork), представляющая собой сеть сетей (ее часто именуют *кампусной* – campus network). Если сеть включает в себя множество зданий и распространяется на большие расстояния, можно говорить о широкомасштабной, или глобальной, сети (wide area network – WAN).

Серверные сети – стандарт даже для маленьких локальных сетей. Однако у них есть и недостатки. Одним из главных, по крайней мере для небольшой фирмы, желающей установить компьютерную сеть, является высокая стоимость сервера и сетевой операционной системы. Кроме того, для поддержания рабочего состояния сети и управления ею требуется администратор.

Другие отрицательные черты подобных сетей связаны со сбоями серверов, *широковещательными штормами* (обильным широковещательным трафиком от

устройств в сети) и прочими аппаратными и программными неполадками, слишком многочисленными, чтобы их перечислять. Управление сетями достаточно сложно, поэтому хороший администратор ценится весьма высоко.

➢ Подробная информация об интерсетях содержится в главе 4. Дополнительные сведения о глобальных сетях можно найти в главе 3.

Установка соединения

Для создания компьютерной сети необходима среда передачи данных. Такой средой могут быть как кабели, так и инфракрасные лучи. Мы ограничимся рассмотрением медных и волоконно-оптических кабелей, учитывая, однако, и то, что существует множество других способов передачи информации от одного пункта к другому.

После того как соединяющая среда (например, медный кабель) выбрана, требуется устройство, которое будет подготавливать данные в компьютере к отправке по проводам. Реструктурированием информации занимается сетевой адаптер. Как правило, такой адаптер устанавливается в одно из расширительных гнезд шины компьютера и к его порту подключается кабель. Для разработки даже самой небольшой сети необходимо хорошо понимать, как работает сетевой адаптер и чем медные кабели отличаются от волоконно-оптических.

Сетевые адаптеры

Сетевой адаптер (сетевая карта) обеспечивает связь между компьютером и физической средой сети. По шине компьютера данные поступают параллельно, в то время как сетевая среда требует последовательной передачи. *Трансивер* (приемник-передатчик) сетевого адаптера способен направлять данные из параллельного канала в последовательный и наоборот.

У каждого сетевого адаптера есть уникальный адрес, «зашитый» в чип ПЗУ. Эта система адресации используется для передачи информации от одного физического интерфейса к другому (передача данных по сети сводится к разрешению логических адресов, таких как IP-адреса, в аппаратные адреса сетевых адаптеров).

Сетевые карты выпускаются для различных типов шин (например, на рис. 1.2 изображен адаптер PCI Ethernet). Прежде чем приобретать такую карту, следует открыть корпуса компьютеров, которые вы собираетесь объединять в сеть, и проверить, разъемы какого типа шин свободны. Новые модели ПК обычно имеют разъемы PCI, на материнских платах более старых машин вы обнаружите разъемы ISA и EISA. Очевидно, что при подготовке компьютера к работе в сети очень важно запастись подходящей сетевой картой. После этого останется только корректно установить адаптер и соответствующий драйвер.

Убедитесь, что у вас есть компакт-диск или набор дискет с операционной системой, установленной на вашем компьютере (например, Windows 98), и что к сетевой карте прилагаются дискеты или компакт-диск с драйвером. Чтобы подготовить компьютер к работе в сети, выполните следующие действия:

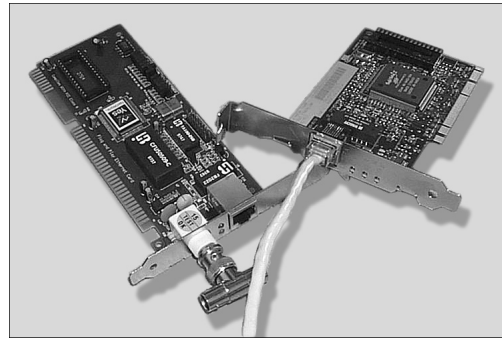


Рис. 1.2. Сетевые адаптеры обеспечивают физическое соединение компьютера с сетью

1. Откройте корпус системного блока и подключите сетевой адаптер к свободному разъему.
2. Закройте корпус и присоедините к адаптеру сетевой кабель (как правило, витую пару).
3. Включите компьютер. Если вы приобрели сетевой адаптер типа Plug-and-Play и пользуетесь ОС Windows 95/98, система сама определит сетевую карту и запустит соответствующие драйверы. Возможно, во время установки потребуется предоставить нужные драйверы (они находятся на дискетах или компакт-диске, который прилагается к сетевой карте).
4. Если ваша операционная система не распознает новые устройства, то сетевой адаптер придется инсталлировать самостоятельно. Если к карте прилагается программное обеспечение, используйте его для загрузки необходимых драйверов.
5. Некоторые ОС (например, Windows NT 4 – операционная система для сервера и рабочих станций) требуют выбрать *запрос прерывания* (Interrupt ReQuest – IRQ) и *порт ввода/вывода* (Input/Output – I/O) для нового сетевого адаптера. Укажите свободный IRQ и порт ввода/вывода и завершите установку карты согласно инструкциям операционной системы.

Если вы создаете сеть IBM Token Ring, следует приобрести сетевые карты Token Ring. Нелишне напомнить, что совершенно необходимо покупать оборудование (сетевые адаптеры и кабели), соответствующее типу сети, которую вы строите.

После подключения карты и запуска соответствующего драйвера компьютер готов к работе в сети (вероятно, вам понадобится сначала перезагрузить его). Проблемы с сетевыми адаптерами могут быть вызваны неправильной инсталляцией (карта плохо вставлена в разъем) и конфликтами запросов прерываний, которые рассматриваются в следующем разделе.

Прерывания и порты ввода/вывода

После установки нового оборудования в расширительный разъем компьютера часто возникают конфликты прерываний.

Любому аппаратному компоненту компьютера – мыши, клавиатуре, сетевому адаптеру – назначается прерывание, по которому центральный процессор оповещается о том, что конкретному устройству требуется обработка информации. У каждого такого устройства должно быть собственное прерывание, иначе возникает конфликт. Ни один из аппаратных компонентов, вероятно, не будет правильно работать, если приходится бороться за один и тот же IRQ. Зная, какие прерывания в системе уже заняты, легко назначить новому элементу – например, сетевому адаптеру – свободный IRQ.

> *В операционных системах последнего поколения установить сетевой адаптер значительно проще. ОС Windows NT 2000 Server и Windows NT 2000 Professional поддерживают технологию Microsoft's Plug-and-Play для оперативно подключаемых устройств. Это означает, что обе операционные системы в большинстве случаев определят тип аппаратуры и запустят необходимые драйверы для ряда сетевых карт, доступных на рынке. Системы Novell NetWare 4.2 и Novell NetWare 5 не работают по технологии Plug-and-Play, однако помогают инсталлировать на сервере подходящий драйвер для сетевого адаптера.*

Найти незанятый IRQ не так уж сложно: в каждой операционной системе (как в персональной, так и в серверной) есть инструмент для просмотра назначенных и свободных запросов прерываний. Пользователи DOS и Windows 3.11 могут применить программу системной диагностики Microsoft System Diagnostics (файл msd.exe). В Windows 95/98 нужно открыть меню **Пуск** ⇒ **Настройка** ⇒ **Панель управления** ⇒ **Система**, выбрать закладку **Устройства** и, выделив значок **Компьютер**, щелкнуть по кнопке **Свойства**. Появится список задействованных прерываний (см. рис. 1.3).

В системах Windows NT Workstation 4.0 и Windows NT Server 4.0 проверить свободные IRQ можно через меню **Пуск** ⇒ **Программы** ⇒ **Администрирование** ⇒ **Диагностика Windows NT**. В диалоговом окне диагностики щелкните по кнопке **Ресурсы**, чтобы просмотреть назначенные прерывания.

В табл. 1.2 приведены стандартные установки прерываний для персональных компьютеров. Обратите внимание: некоторые IRQ зарезервированы за конкретными устройствами.

В случаях, когда у компьютера нет второго порта COM или LPT2, эти прерывания окажутся свободными. В каждом ПК распределение IRQ будет различаться, поэтому с помощью вышеописанных инструментов следует определять фактическое назначение прерываний.

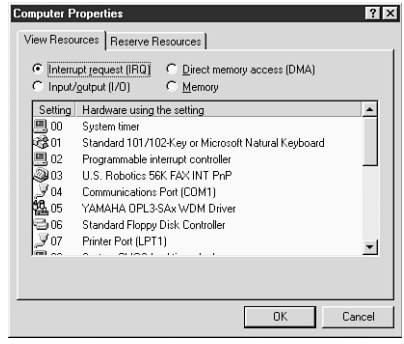


Рис. 1.3. Определение свободных IRQ

Таблица 1.2. Установки IRQ

Запрос прерывания (IRQ)	Устройство
0	Системный таймер
1	Клавиатура
2	Каскад к дополнительному контроллеру прерываний
3	Последовательные порты (COM2 и COM4)
4	Последовательные порты (COM1 и COM3)
5	Порт принтера (LPT2)
6	Контроллер устройства чтения гибких дисков
7	Порт принтера (LPT1)
8	Часы
9	Свободен
10	Основной адаптер SCSI (или свободен)
11	Дополнительный адаптер SCSI (или свободен)
12	Мышь PS/2
13	Математический сопроцессор
14	Основной контроллер жестких дисков
15	Дополнительный контроллер жестких дисков

Для связи с центральным процессором устройствам требуется не только IRQ, но и канал, по которому процессор будет направлять обработанную информацию к устройству. Базовый порт ввода/вывода служит, по существу, адресом устройства. Как и в случае с запросами прерываний, у каждого устройства имеется собственный базовый порт ввода/вывода. Для сетевых адаптеров обычно выделяются порты 220h, 280h, 300h, 320h и 360h (буква «h» указывает, что запись приводится в шестнадцатеричной (hexadecimal) системе счисления). Определяются свободные порты ввода/вывода с помощью тех же инструментов, посредством которых находят свободные IRQ.

Сетевые кабели

Чаще всего в качестве физической сетевой среды выступают медные кабели. Напомним, что существуют и волоконно-оптические кабели, которые находят все большее применение благодаря высокой пропускной способности и длине физического сегмента. Волоконно-оптический кабель задействуется в высокоскоростных сетях, таких как FDDI, и синхронных оптических сетях (synchronous optical network – SONET), передающих одновременно голос, изображение и другую информацию.

Как уже упоминалось, в локальных сетях широко используются медные кабели. И хотя выпускается несколько их разновидностей, наиболее распространена неэкранированная витая пара пятой категории (всего существует пять категорий витых пар; категории с третьей по пятую относятся к кабелям для передачи данных).

Витые пары пятой категории применяются в реализациях Ethernet со скоростями 10 Мбит/с, 100 Мбит/с (Fast Ethernet) и 1 Гбит/с (Gigabit Ethernet). Неэкранированные витые пары также подходят для сетей IBM Token Ring. Компания IBM имеет собственную классификацию витых пар. В сетях Token Ring наиболее распространен кабель типа 1. Витая пара обычно присоединяется к сетевым адаптерам, концентраторам и другим устройствам посредством разъема RJ-45.

Сети на тонком и толстом коаксиальном кабеле (RG-58 и RG-11) в последнее время становятся менее распространенными, хотя и встречаются еще в промышленных компаниях. Сеть на толстом коаксиальном кабеле характеризуется магистральной шиной, физический доступ к которой осуществляется с помощью специальных коннекторов-«вампиров», врезаемых в кабель. Коннектор связан с трансивером, который, в свою очередь, соединяется с компьютером через дополнительный кабель.

Тонкий коаксиальный кабель RG-58 был весьма популярен благодаря относительной простоте прокладки и низкой цене. Локальные сети на тонком кабеле построены по шинной топологии, где к сетевой карте каждого компьютера подключается тройниковый разъем. Затем компьютеры соединяются в цепь отрезками кабеля подходящей длины. В системах с тонким кабелем необходимо к крайним тройникам со свободной стороны прикрепить концевую заглушку-терминатор.

Медный провод, представляющий собой недорогую и простую в установке сетевую среду, имеет некоторые серьезные недостатки. Во-первых, он сильно подвержен влиянию электромагнитного излучения. Затухание (ослабление сигнала по мере распространения в кабеле) ограничивает длину провода. К тому же от медного кабеля нетрудно сделать отводку, что может оказаться существенным дефектом в защите информации, передаваемой по сети.

Волоконно-оптический кабель, изготавливаемый на основе стеклянного или пластикового волокон, – это высокоскоростная альтернатива медному проводу. Он часто служит основной магистралью в больших корпоративных сетях. Такие кабели обладают высокой пропускной способностью, большей допустимой длиной, и от них нельзя сделать ответвление. Необходимость увеличения скорости

передачи информации способствует широкому распространению волоконно-оптических сетей.

В волоконно-оптических кабелях данные переносятся световыми импульсами, в качестве источника света применяются лазеры и светодиоды (light emitting diode – LED). Такие кабели дороже медных и не так просты в установке, но способны быстрее передавать информацию, что делает их хорошей альтернативой меди.

В табл. 1.3 представлены различные типы кабелей, изображенные на рис. 1.4.

При выборе сетевого кабеля важен ряд факторов: цена, полоса пропускания (количество информации, которое можно передать по кабелю), подверженность кабеля влиянию электромагнитного излучения, величина затухания и простота установки. Выбирайте такой тип кабеля, который будет наилучшим образом соответствовать вашим требованиям и бюджету.

Таблица 1.3. Сравнение сетевых кабелей

Тип кабеля	Полоса пропускания	Максимальная длина	Стоимость
Неэкранированная витая пара пятой категории (CAT 5 UTP)	От 10 до 100 Мбит/с	100 м	Недорогой
Тонкий коаксиальный кабель	10 Мбит/с	185 м	Недорогой
Толстый коаксиальный кабель	10 Мбит/с	500 м	Дорогой
Оптоволокно	От 100 Мбит/с до 2 Гбит/с и выше	2 км	Дорогой

➢ Подробнее о шинной топологии рассказывается ниже, раздел «Шинная сеть».

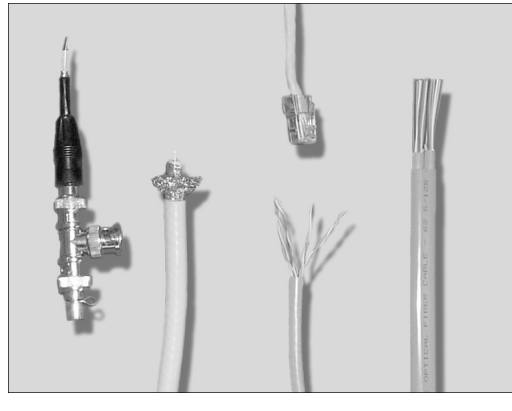


Рис. 1.4. Тонкий и толстый кабели, витая пара, волоконно-оптический кабель

Концентраторы, повторители и устройства множественного доступа

В зависимости от типа кабеля и топологии сети вам могут понадобиться устройства для соединения имеющихся узлов или добавления новых. Тип соединяющего устройства зависит от сетевой архитектуры.

Концентраторы (hubs) применяются в сочетании с витой парой и служат связующими центрами сети. Базовый концентратор не содержит активной электронной схемы и не может использоваться для расширения сети. Он, по существу, упорядочивает кабели и передает сигналы всем присоединенным к нему устройствам (рис. 1.5)[1].

Рис. 1.5. Концентратор – связующий центр сети

Технология концентраторов развивается очень быстро. Активные концентраторы содержат электронную схему и не только физически связывают узлы сети, но и действуют как повторители, благодаря чему можно расширять сеть. Существуют новые концентраторы с функциями коммутации, позволяющие увеличить пропускную способность сети. А с помощью интеллектуальных концентраторов удается даже решать проблемы со связью.

В тех случаях, когда расширение сети требует большей длины кабеля, чем максимально допустимая для данного типа, удобно использовать повторители, принимающие сигнал и воспроизводящие его. В сетях IBM Token Ring в качестве связующего центра применяется устройство множественного доступа (multistation

[1] В русскоязычной разговорной компьютерной терминологии довольно давно применяется слово «хаб» (от англ. hub – концентратор). – *Прим. научн. ред.*

access unit – MAU). Такие устройства содержат активные электронные схемы и обеспечивают не только физическую связь между сетевыми устройствами, но и логическое кольцо для циркуляции трафика.

➢ Устройства множественного доступа будут рассмотрены позже в разделе «Сети IBM Token Ring» данной главы. Подробнее о физическом уровне говорится в главе 2 (раздел «Физический уровень»).

Физическая среда соответствует физическому уровню модели OSI.

Топология сетей

Локальные сети удобно рассматривать с точки зрения их физической схемы, или *топологии*. В какой-то мере топология отдельно взятой сети отражает тип кабеля и фактическую архитектуру сети (например, Ethernet или IBM Token Ring). И хотя различным видам топологии приписаны конкретные характеристики (скажем, шинная топология считается пассивной, основанной на конкурентном доступе к среде передачи), реальное поведение той или иной сети точнее определяется ее архитектурой. Ниже представлены краткие описания и схемы основных топологий.

➢ Более подробно сетевые архитектуры рассматриваются ниже в данной главе (раздел «Виды сетевых архитектур»).

Шинная сеть

Шинная сеть характеризуется основной магистральной линией, к которой подсоединены компьютеры (рис. 1.6). Шинная топология считается пассивной, компьютеры только ждут сигналов. ПК, готовый к передаче данных, вначале прослушивает среду передачи данных, и, если полезный сигнал не обнаруживается (никто ничего не посылает), сетевая карта этого компьютера отправляет информационные пакеты. В пассивных конкурентных сетях (где узлы соперничают за доступ к среде передачи), как правило, применяется архитектура Ethernet.

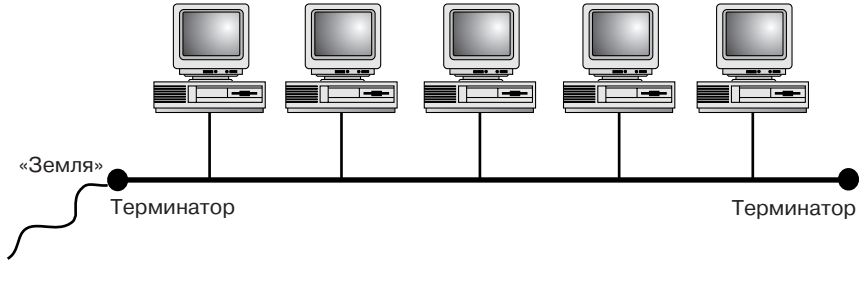


Рис. 1.6. Шинная топология

Шинные сети обычно построены на коаксиальном кабеле, к которому посредством тройников присоединены компьютеры. На концах кабеля устанавливаются терминаторы, соответствующие данному типу кабеля (с 50-омным кабелем сочетаются терминаторы в 50 Ом). Поскольку шинная сеть представляет собой набор кабелей, разъемов и терминаторов, сигнал в ней не усиливается.

Если сеть с шинной топологией не терминирована должным образом, то электрические сигналы будут отражаться от конца провода, что приведет к искажениям закодированной в сигналах информации и сбою в работе всей сети. В случае шинной топологии при обнаружении неисправностей следует сначала проверить физические компоненты сети: сети этого типа славятся проблемами с разъемами, кабелем и терминаторами.

Шины с сетевой топологией легко собирать и расширять. Для них требуется весьма небольшая по сравнению с шинами других топологий длина кабеля. В шинных сетях случаются разрывы кабеля, пропадают контакты в разъемах и происходят короткие замыкания, которые трудно находить и устранять. Одна физическая неисправность в сети (например, отсоединенный разъем) способна вывести из строя всю сеть.

Топология «звезда»

В топологии «звезда» компьютеры соединяются друг с другом через центральное связующее устройство, называемое *концентратором*. Каждый компьютер подключается к его порту отрезком кабеля – как правило, витой парой (рис. 1.7). Из-за наличия концентратора (особые концентраторы – многопортовые повторители – могут усиливать сигнал, передаваемый по сети) здесь по-прежнему используется пассивный, конкурентный метод передачи информации. Компьютеры ждут сигналов и борются за доступ к среде передачи.

Для звездообразной топологии характерно отдельное кабельное соединение для каждого ПК, поэтому такую сеть легко расширять – правда, в пределах количества свободных портов концентратора. Кроме того, новые компьютеры внедряются в сеть весьма просто: чтобы добавить устройство, достаточно протянуть от него провод к концентратору. Пользователи сети даже не заметят расширения.

Недостатки подобной топологии связаны с потребностью в кабеле и концентраторе. Поскольку каждый компьютер подключается посредством отдельного кабеля, затраты на кабель будут выше, чем в случае шинной топологии (хотя витая пара, которая применяется в «звезде», является наиболее дешевой). Приобретение концентратора также связано с дополнительными расходами, но благодаря таким выгодным сторонам звездообразной топологии, как простота обращения с физическими компонентами, затраты могут оказаться вполне оправданными.

(Цены на концентраторы настолько снизились, что даже пользователи небольших домашних сетей в состоянии использовать эти устройства для объединения своих компьютеров.)

Самый большой недостаток топологии «звезда» связан с центральным концентратором: когда в нем происходит сбой, перестает работать вся сеть. Многие сетевые администраторы на случай критических ситуаций приобретают запасной концентратор.

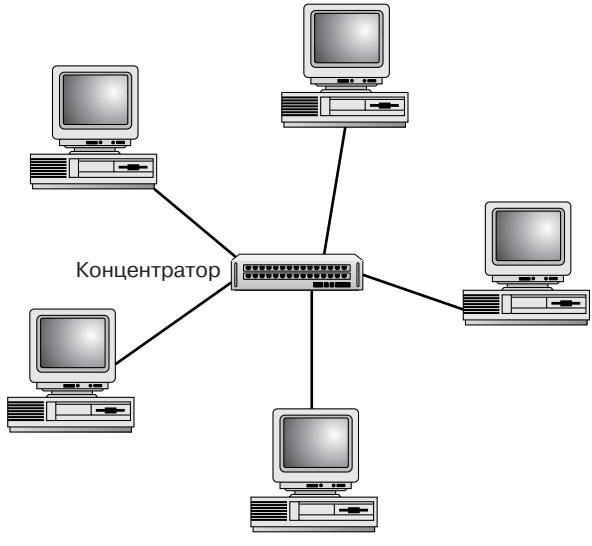


Рис. 1.7. Топология «звезда» легко расширяема

Кольцевая топология

При такой топологии компьютеры соединяются в кольцо (рис. 1.8), где информация передается в одном направлении. Каждый компьютер отсылает полученные пакеты следующему. Кольцевая топология считается активной. Примером подобной архитектуры может служить интерфейс оптоволоконной передачи (fiber distributed data interface – FDDI).

Доступ к среде передачи данных в таких сетях предоставляется каждому активному устройству с помощью специального пакета – маркера. Маркер передается по кольцу, и, если компьютеру требуется отправить информацию, он ожидает маркер. Приняв маркер, компьютер пересылает свои данные. После того как пославший информацию компьютер получает подтверждение, что его сообщение дошло до адресата, он создает новый маркер и направляет его следующему узлу в сети.

Тот факт, что компьютер для пересылки данных должен обладать маркером, означает равноправность доступа узлов к сетевой среде. Кольца с передачей маркера

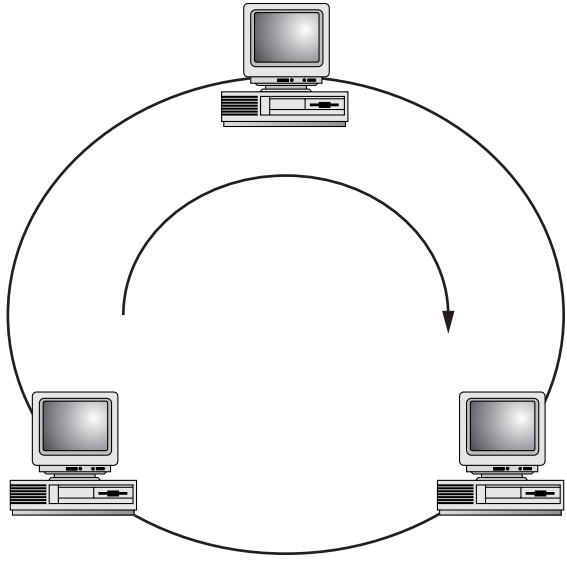


Рис. 1.8. В кольцевой топологии применяется метод передачи маркера

обеспечивают более своевременную трансмиссию информации, чем такие конкурентные сети, как шинная или звездообразная.

При высоком трафике производительность кольцевой сети падает не так сильно, как в сетях с пассивной топологией, где она значительно снижается из-за большого количества столкновений пакетов (коллизий).

Однако в сетях с кольцевой топологией очень трудно устранять неисправности. Сбой одного компьютера может прервать весь поток информации, поскольку данные передаются по кругу в одном направлении. Добавление или удаление устройств также может нарушить функционирование сети.

➢ Подробнее об архитектуре FDDI рассказывается в разделе «Архитектура FDDI».

Избыточная топология «петля»

Топология «петля» характеризуется избыточными соединениями между компьютерами в целях повышения отказоустойчивости[1]. Каждое устройство в сети связывается со всеми остальными. Иными словами, такая топология требует большого количества кабеля (рис. 1.9). В случае выхода из строя одного-двух сегментов

[1] В русскоязычной литературе также применяется термин «полносвязная сеть». – *Прим. научн. ред.*

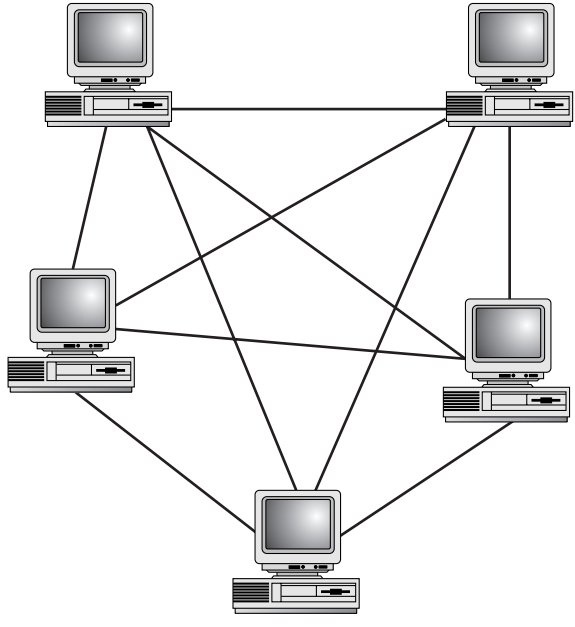


Рис. 1.9. Топология «петля»

подобная сеть будет продолжать функционировать благодаря оставшимся линиям связи.

Очевидно, что сети, построенные по топологии «петля», из-за большого количества соединений оказываются более дорогими и сложными в установке. В большинстве случаев сети, в которых применяется стратегия избыточной связи, входят в состав гибридных сетей. В последних только главные серверы и компьютеры, предназначенные для решения наиболее важных задач, используют избыточные соединения. Таким образом, защищаются лишь самые ценные части корпоративной сети, а связывать друг с другом по такому же принципу все остальные компьютеры не требуется.

Как уже упоминалось, топология – это удобный способ описания физического строения сети и стратегии передачи данных. Соединяя различные виды топологий, можно создавать гибридные сети: например, связать в цепочку несколько концентраторов и получить звездно-шинную топологию или добавить в кольцевую сеть устройство, подобное концентратору и содержащее логическое кольцо (скажем, устройство множественного доступа, используемое в качестве центрального элемента в сетях IBM Token Ring).

Виды сетевых архитектур

Сетевые архитектуры в зависимости от типа обеспечивают различные методы решения общей задачи, заключающейся в быстрой и эффективной пересылке информации. Каждая конкретная архитектура, например Ethernet, определяет не только топологию сети, но и способ доступа компьютеров к среде передачи данных. Существует несколько сетевых архитектур с различными стратегиями передачи информации.

Архитектура Ethernet

Самой распространенной сетевой архитектурой является *Ethernet*, предоставляющая множественный доступ к среде передачи данных с контролем несущей и обнаружением конфликтов (carrier sense multiple access with collision detection – CSMA/CD). Такой метод сетевого доступа означает, по существу, что узел ждет, когда линия будет свободна. Тогда он может послать кадр. Если несколько компьютеров отправляют кадры одновременно, возникают конфликты. Обнаружив конфликт, устройства прекращают передачу и снова ждут освобождения линии, после чего завершают отсылку своих кадров.

Ethernet – это пассивная архитектура. Конфликты случаются часто, и компьютеры вынуждены бороться за доступ к среде передачи. Сети Ethernet обычно построены по шинной или звездно-шинной топологии в зависимости от используемой сетевой среды. Одна из наиболее распространенных реализаций Ethernet (с различными типами сред) обладает скоростью передачи в 10 Мбит/с. Такая десятимегабитная сеть с витой парой обозначается *10BaseT*, где *10* относится к скорости (в Мбит/с), *Base* означает передачу по моноканалу (baseband), а *T* говорит о наличии витой пары (twisted pair). В табл. 1.4 приведены характеристики некоторых реализаций Ethernet.

> *Спецификации архитектур Ethernet разработаны Институтом инженеров по электротехнике и электронике (IEEE) и носят обозначение IEEE 802.3. Сеть Ethernet соответствует подуровню управления доступом к среде передачи (MAC) канального уровня в модели OSI. Модель OSI и различные спецификации подуровня MAC рассматриваются в главе 2.*

Таблица 1.4. Реализации Ethernet

Обозначение сети	Тип кабеля	Максимальная длина кабеля	Тип соединителя
10BaseT	Неэкранированная витая пара пятой категории	100 м	Концентратор
10Base2	Тонкий коаксиальный кабель	185 м	Тройники, цилиндрические соединители, терминаторы

Таблица 1.4. Реализации Ethernet (окончание)

Обозначение сети	Тип кабеля	Максимальная длина кабеля	Тип соединителя
10Base5	Толстый коаксиальный кабель	500 м	Тройники-«вампиры», ответвительные кабели, терминаторы
10BaseFL	Оптоволокно	2 км	Повторители, терминаторы

Перед отправкой по сети пакеты данных преобразуются в кадры. Ethernet включает в себя кадры разных типов, поэтому во избежание проблем все узлы сети должны быть сконфигурированы для работы с одним и тем же типом. Различают следующие виды кадров:

- Ethernet 802.3 – хотя этот тип имеет соответствующий номер IEEE, в действительности он не в полной мере отвечает спецификациям для Ethernet. Кадры такого типа применяются в сетях Novell NetWare 2.2 и 3.1;
- Ethernet 802.2 – данный вид кадра полностью соответствует спецификациям IEEE. Он используется в более поздних версиях Novell NetWare: 3.12, 4.x и 5.x[1];
- Ethernet SNAP – кадры подобного типа применяются в сетях AppleTalk;
- Ethernet II – такие кадры формируются многопротокольными сетями, такими как Internet.

Хотя десятимегабитные реализации Ethernet до сих пор довольно популярны, их стремительно вытесняют Fast Ethernet (100 Мбит/с) и Gigabit Ethernet (1 Гбит/с). В обеих версиях требуется кабель пятой категории и специальные сетевые адаптеры и концентраторы, но во многих случаях в Gigabit Ethernet применяется витая пара шестой категории.

Основное достоинство сетей Ethernet – их стоимость. Сетевые карты, кабель и концентраторы значительно дешевле оборудования, применяемого в других архитектурах (например, в сетях Token Ring). Главный недостаток связан с многочисленными конфликтами в сети. Чем больше конфликтов, тем медленнее будет работать сеть, вплоть до полной ее остановки.

> *Существует два способа избежать проблем с трафиком: сегментировать сети при помощи моста (bridge) или разбивать их на подсети и соединять через маршрутизатор. Подробнее об этом рассказывается в главе 4.*

[1] Когда фирма Novell разрабатывала стек протоколов IPX/SPX для первых версий своей операционной системы Novell NetWare, было принято решение не добавлять в заголовок кадра (канальный уровень модели OSI) информацию о протоколах верхнего уровня, которые должны обрабатывать поступивший из сети кадр, поскольку единственным таким протоколом являлся IPX. В этом состоит основное различие кадров 802.3 и 802.2, в заголовке которого такая информация присутствует. – *Прим. научн. ред.*

Архитектура IBM Token Ring

IBM Token Ring считается быстрой и надежной сетью с передачей маркера. Сети Token Ring имеют звездообразную физическую конфигурацию, центром которой служит устройство множественного доступа (multistation access unit – MAU). Фактическим кольцом, по которому посылается маркер, является логическое кольцо MAU.

Маркер переходит по кругу до тех пор, пока его не примет компьютер, желающий передать информацию. Компьютер, направляющий маркер своему соседу, называется *ближайшим активным вышестоящим узлом* (nearest active upstream neighbor – NAUN), а компьютер, получающий маркер, – *ближайшим активным нижестоящим узлом* (nearest active downstream neighbor – NADN).

После того как компьютер принял маркер и послал информацию, он создает новый маркер и передает его своему соседу.

> *В Институте инженеров по электротехнике и электронике разработаны спецификации для сетей IBM Token Ring – IEEE 802.5. Сети Token Ring соответствуют подуровню управления доступом к среде (MAC) канального уровня модели OSI. Модель OSI и различные спецификации подуровня MAC описываются в главе 2.*

Характерная черта сетей Token Ring состоит в отсутствии конфликтов и равноправном доступе к среде для всех узлов. Сети этого типа работают медленнее, чем некоторые реализации Ethernet (4 и 16 Мбит/с), но при высоком трафике их производительность ухудшается не столь заметно. (В ближайшем будущем ожидается гигабитное воплощение сети Token Ring.)

В сетях Token Ring благодаря методу обнаружения ошибок, называемому *разграничивающей сигнализацией*, обеспечивается некоторая отказоустойчивость. Когда компьютеры подсоединяются к сети, первый включившийся выполняет функции активного мониторинга и каждые 7 с посылает специальные пакеты, чтобы определить, находятся ли в сети другие узлы. Если какой-нибудь ПК не получает пакет от ближайшего активного соседнего узла, он создает пакет со своим адресом и адресом этого узла и передает его дальше. Такой пакет несет информацию, которая может быть использована сетью для автоматической реконфигурации кольца и поддержания трафика.

Архитектура FDDI

Интерфейс оптоволоконной передачи (fiber distributed data interface – FDDI) – это архитектура, предоставляющая высокоскоростную магистраль, посредством которой можно соединять сети различных типов. Сети FDDI построены на коль-

цевой топологии с применением волоконно-оптических кабелей. Способом доступа к среде служит пересылка маркера, а скорость передачи данных достигает 100 Мбит/с и выше.

Так как в основе функционирования сетей FDDI лежит взаимодействие устройств при помощи маркера, всем узлам обеспечивается надежный и равный доступ к среде. Тем не менее в архитектуре FDDI можно установить различные приоритеты и, таким образом, позволить серверам отправлять больше информационных кадров, чем клиентам.

Поскольку архитектура FDDI является настоящим кольцом[1], не исключено, что разрывы кабеля окажутся проблемой. В целях отказоустойчивости предусматривается создание вторичного кольца. Если компьютер не может связаться со своим нижестоящим соседом, он посылает информацию по вторичному кольцу, но уже в обратном направлении (рис. 1.10).

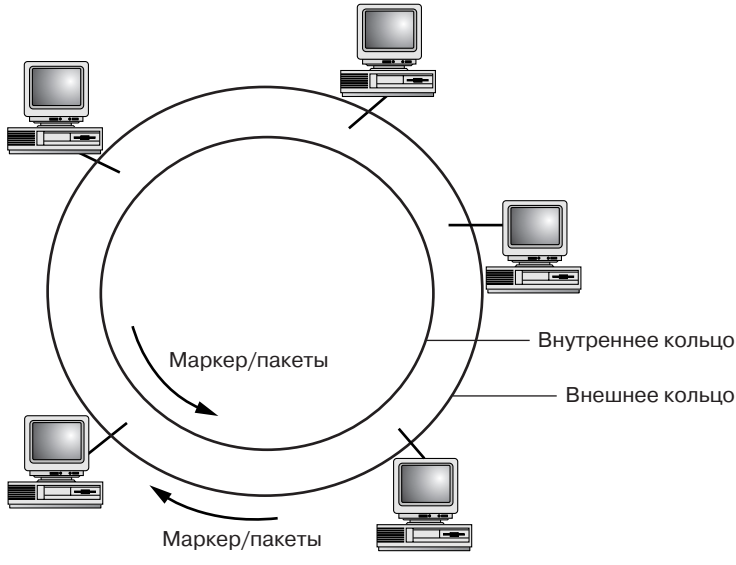


Рис. 1.10. В сети FDDI имеется два настоящих кольца с передачей данных в противоположных направлениях

Для реализации архитектуры FDDI необходимы специальные сетевые адаптеры. В станциях с двойным подключением применяется особая карта, взаимодействующая с обоими кольцами. Для связи с остальными узлами в сетях FDDI предназначены концентраторы. Поскольку другие компьютеры не входят

[1] И физическим, и логическим. – *Прим. научн. ред.*

непосредственно в кольцо FDDI, им требуется адаптер с единичным подсоединением к такому концентратору.

Архитектура AppleTalk

AppleTalk – это сетевая архитектура, применяемая машинами Apple Macintosh. Необходимое сетевое оборудование встроено в каждый такой компьютер (хотя для подключения Macintosh в сеть Ethernet требуется сетевой адаптер Mac Ethernet). Система кабелей, посредством которой соединяются компьютеры Macintosh, называется *LocalTalk* и состоит из экранированных витых пар со специальным разъемом для Macintosh.

В AppleTalk предусмотрена особая система адресации сетевых узлов. При включении Macintosh генерирует случайное число и транслирует его в сеть. Это число становится его сетевым адресом, если только он не совпадает с адресом другого компьютера. В последнем случае подключившийся компьютер продолжит генерацию случайных чисел до тех пор, пока не создаст неиспользуемый адрес.

Архитектура AppleTalk, как и Ethernet, пассивна. В AppleTalk применяется метод множественного доступа с контролем несущей и предотвращением конфликтов (carrier sense multiple access with collision avoidance – CSMA/CA). Компьютер, который собирается передавать данные, сможет это сделать, лишь когда освободится линия. Получив информацию о том, что линия свободна, он посылает специальный служебный пакет, извещая все остальные узлы о начале передачи информации, и только потом отправляет данные.

Тот факт, что компьютер оповещает другие узлы о начале передачи данных, значительно уменьшает количество конфликтов в сети CSMA/CA (особенно в сравнении с Ethernet).

Однако такие служебные пакеты снижают эффективность передачи данных: сети AppleTalk имеют скорость всего лишь в 230,4 Кбит/с. Благодаря тому, что аппаратное и программное обеспечение, необходимые для работы Macintosh в сети, поставляются в комплекте с каждым компьютером, объединение в сеть нескольких рабочих станций представляется весьма простым и недорогим.

ГЛАВА 2

Модель OSI и сетевые протоколы

При изучении любой дисциплины приходится сталкиваться с умозрительными моделями. Изобразительное искусство включает в себя теории цвета и композиции, физика охватывает почти все теоретические модели Эйнштейна. Наука о компьютерных сетях также строится на моделях, позволяющих наглядно представить сложную цепь явлений – движение данных по сети.

> *Международная организация по стандартизации (ISO) выпускает наборы правил и моделей как для технических стандартов сетевых разработок, так и для бизнес-проектов. Вы, вероятно, видели вывески деловых компаний, извещающие о том, что компания имеет сертификат ISO 9002. Это означает, что данная фирма работает в соответствии с набором правил и протоколов, составленных ISO для коммерческой деятельности на мировом рынке. Кроме того, часто встречается сертификация ISO 9660 для файловых систем на CD-ROM.*

OSI – теоретическая модель стека сетевых протоколов

В конце 70-х годов XX века ISO начала разработку эталонной модели взаимодействия открытых систем (open systems interconnection reference model – OSI/RM). В кругу людей, занимающихся сетями, обычно говорят просто о модели OSI. В 1984 году эта модель стала международным стандартом сетевых коммуникаций и теперь служит теоретической основой для изучения сетей и логического объяснения процесса передачи данных с одного узла сети на другой.

В модели OSI функционирование сетей представлено в виде семи последовательных уровней, каждый из которых отвечает за конкретную часть общего процесса передачи данных. Эта концептуальная модель позволяет изучить реальные стеки протоколов, применяемые в сетях. Например, TCP/IP и AppleTalk – два настоящих

стека сетевых протоколов. Протоколы, представляющие собой уровни в наборе протоколов, можно затем рассмотреть с точки зрения их действия на соответствующих уровнях модели OSI.

➢ Подробнее о некоторых часто используемых наборах протоколов рассказывается ниже в данной главе (раздел «Реальные сетевые протоколы»).

Модель OSI описывает ряд важных событий, происходящих при передаче данных по сетям. В ней сформулированы основные правила для различных сетевых процессов:

- как происходит преобразование данных в формат, соответствующий вашей сетевой архитектуре. Когда вы отправляете электронное письмо или файл на другой компьютер, вы работаете с таким приложением, как почтовый клиент или клиент FTP. Прежде чем передать эту информацию по сети, ее нужно перевести в более общий формат;
- как компьютеры или другие устройства устанавливают связь между собой. Для пересылки информации с одного компьютера на другой требуется механизм, обеспечивающий канал связи между отправителем и получателем;
- как передается информация и как устанавливается очередность отправки сообщений и контроль ошибок. Когда связь между компьютерами установлена, должен вступить в силу набор правил управления потоком данных;
- каким образом логические адреса пакетов преобразуются в физические адреса сетевых устройств. Компьютерные сети работают с системой логической адресации, например с IP-адресами. Для формирования сетевого кадра необходимо выполнить преобразование логического адреса в физический адрес сетевого адаптера, установленного в компьютере-получателе.

Модель OSI располагает механизмами и правилами, которые предоставляют возможность решать перечисленные задачи. Знание уровней модели OSI не только позволяет разбираться в действительных наборах протоколов, но и дает теоретическую основу, с помощью которой можно глубже изучить такие сложные устройства, как коммутаторы, мосты и маршрутизаторы.

Стеки, или наборы, протоколов – это группы протоколов, обеспечивающих при совместной работе передачу данных от одного узла к другому. Стеки протоколов похожи на бегунов в эстафете, только вместо эстафетной палочки каждому последующему протоколу вручаются пакеты данных, пока из них не сформируется битовый поток, готовый к пересылке по сети.

Сетевые администраторы обычно сталкиваются со стеками таких сетевых протоколов, как NetWare IPX/SPX и TCP/IP, однако существует вполне реальный набор протоколов, основанный на модели OSI, – стек OSI (он не входит в состав сетевых ОС наподобие Novell NetWare или Windows NT).

Наряду с такими известными сетевым администраторам стеками протоколов, как IPX/SPX и TCP/IP, существует и настоящий набор, основанный на модели OSI, – стек протоколов OSI. К сожалению, он не включен ни в одну сетевую операционную систему (Novell NetWare или Windows NT), с которой вам предстоит работать.

Уровни модели OSI

Уровни модели OSI объясняют процесс передачи данных по сети. Как пользователь компьютера, вы имеете дело только с двумя уровнями этой модели – первым (физическим) и последним (уровнем приложения):

- *физический уровень* представляет физическую сторону сети (кабели, концентраторы и т.д.). Вы, вероятно, уже сталкивались с физическим уровнем, спотыкаясь о плохо проложенный провод;
- *уровень приложения* обеспечивает интерфейс при работе с электронной почтой или передаче файлов по сети[1].

Если ограничиться обсуждением только этих двух уровней, получилась бы очень небольшая глава, однако нелишне отметить, что каждый уровень модели OSI играет важную роль в функционировании сети.

Рис. 2.1. Модель OSI – теоретическая основа для описания процесса передачи данных

На рис. 2.1 представлен список уровней модели OSI сверху вниз. Перевернутая пирамида – удачная модель, поскольку информация, изначально имеющая довольно сложную форму, в конце концов преобразуется в битовый поток, который можно пустить по проводу. Однако нумеруются уровни снизу вверх. Так, сетевой уровень иногда называют третьим. Неважно, как вы обозначаете уровень – словом или числом, надо лишь разбираться в том, какую роль он играет в общем процессе сетевых коммуникаций.

Понимать модель OSI действительно необходимо, она важна при рассмотрении как простых, так и самых сложных сетевых технологий. В каждой книге или статье, посвященной сетям, вы найдете упоминание об этой модели.

Прежде чем приступить к обсуждению уровней стека, нужно получить общее представление о том, что происходит при движении данных от уровня к уровню. До-

[1] Вообще под уровнем приложения принято понимать программное обеспечение, предоставляющее любой тип интерфейса (графическое окно или командную строку) для обращения к сети любого сетевого приложения. – *Прим. научн. ред.*

пустим, один пользователь сети хочет послать другому сообщение по электронной почте. Отправитель воспользуется почтовой программой (например, Outlook или Eudora), которая служит интерфейсом для написания и последующей передачи сообщений. Эти действия пользователя выполняются на уровне приложения.

После уровня приложения (здесь к пакету данных присоединяется заголовок уровня приложения) информация попадает на следующий уровень. Каждый уровень, в свою очередь, выполняет ту или иную задачу, устанавливая связь или должным образом форматируя данные.

Независимо от функции уровня, он добавляет к пакету данных свой заголовок (на рис. 2.2 заголовки обозначены квадратиками с соответствующей цифрой). Физический уровень – это такое аппаратное обеспечение, как, например, кабель, поэтому он не присоединяет к данным никакого заголовка.

В конце концов информация достигает физического уровня (реальной сетевой среды: кабелей, концентраторов) и передается в сеть к пункту назначения – получателю электронного письма.

Информация принимается на физическом уровне компьютера-получателя и движется снизу вверх по уровням модели OSI. При этом на каждом уровне удаляется соответствующий заголовок. Когда данные наконец поступают на

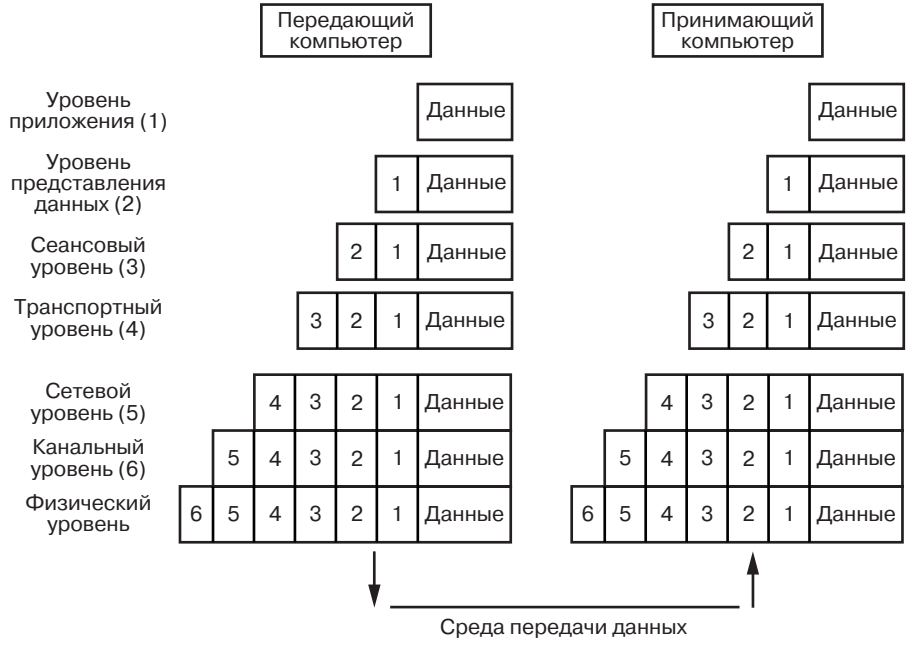


Рис. 2.2. Информация передается по стеку OSI сверху вниз в компьютере-отправителе и снизу вверх в компьютере-получателе

уровень приложения, получатель может воспользоваться почтовой программой и прочесть письмо.

Далее мы рассмотрим все уровни модели OSI от верхнего к нижнему (от уровня приложения к физическому).

Уровень приложения

Уровень приложения обслуживает пользовательские приложения и отвечает за общий доступ к сети. Он предоставляет реально видимые инструменты и сетевые службы, связанные с приложениями: обработку сообщений, передачу файлов, запросы к базам данных. Каждая из этих служб поставляется уровнем приложения различным программам, доступным для пользователя. В качестве примеров служб обмена информацией, выполняемых уровнем приложения, можно назвать World Wide Web, почтовые службы, в частности протокол пересылки почты (simple mail transfer protocol – SMTP), содержащийся в TCP/IP, и специальные службы для баз данных с архитектурой клиент/сервер.

Уровень представления данных

Уровень представления данных можно рассматривать как транслятор. Здесь пакеты принимаются от уровня приложения и преобразуются в общий формат, воспринимаемый всеми компьютерами. Скажем, данные, записанные в ASCII-коде, могут быть отображены в обобщенной форме.

Уровень представления данных отвечает также за шифрование (если того требует программа, используемая на уровне приложения) и сжатие информации.

Службы уровня приложения обеспечивают функционирование пользовательских программ в сети. Когда пользователь при работе с тем или иным приложением (например, с Excel) желает записать файл в свою директорию на сетевом сервере, уровень приложения предоставляет соответствующую службу, позволяющую передать файл с клиентской машины на сервер. Эта операция прозрачна для пользователя.

Между одинаковыми уровнями модели OSI на работающих в сети узлах устанавливается логическая связь. Когда информация (например, почтовое сообщение) сначала перемещается вниз по стеку протоколов на компьютере-отправителе, затем по сетевым коммуникациям и, наконец, вверх по уровням протокола в принимающем компьютере, связь на самом деле осуществляется между соответствующими уровнями модели OSI на обоих ПК.

Сегмент данных, созданный уровнем представления, имеет практически готовый к передаче по сети вид (хотя нижеследующие уровни внесут в него свои добавления, и сегмент может быть разбит на более мелкие части)[1].

Сеансовый уровень

Сеансовый уровень отвечает за налаживание связи, или *сеанса*, между посылающим и принимающим компьютерами, а также управляет сеансом, идущим между двумя узлами (рис. 2.3).

После того как связь между узлами налажена, сеансовый уровень вставляет в поток данных контрольные точки, что гарантирует некоторую отказоустойчивость.

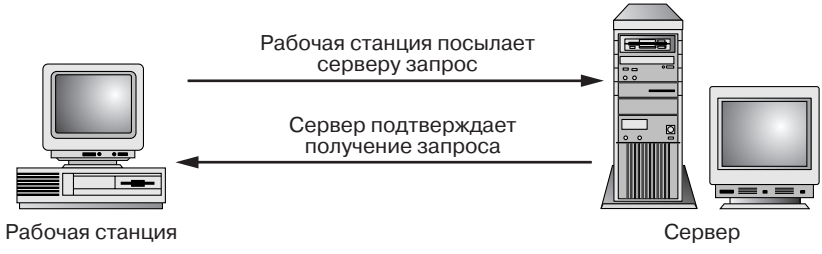


Рис. 2.3. На сеансовом уровне происходит установка связи между узлами

Если сеанс срывается и связь прекращается, то после восстановления соединения нужно заново передать только ту информацию, которая поступила после получения последней контрольной точки. Таким образом, исчезает необходимость нагружать сеть повторной пересылкой всех пакетов.

Реальные протоколы, действующие на сеансовом уровне, применяют два подхода к передаче данных: связь с предоставлением соединения и без него. Протоколы, ориентированные на установление соединения, обеспечивают сеансовое окружение, в котором связывающиеся компьютеры согласовывают параметры, относящиеся к созданию контрольных точек, поддерживают диалог во время передачи данных и одновременно заканчивают сеанс.

Протоколы с предоставлением соединения действуют как обычная телефонная связь. Вы звоните какому-либо человеку, во время разговора поддерживается прямое соединение, а в конце оба собеседника соглашаются закончить общение.

Протоколы без установления соединения функционируют аналогично почте. Они снабжают пакеты, готовящиеся к отправке, адресной информацией, и те отсылаются как обыкновенное письмо, брошенное в почтовый ящик. Предполагается, что письмо достигает пункта назначения, но от получающего компьютера не требуется никакого подтверждения доставки.

[1] Пакеты и кадры. – *Прим. научн. ред.*

Транспортный уровень

Транспортный уровень отвечает за управление потоком данных между узлами. Нужно доставить информацию не только без ошибок, но и в правильной последовательности. Транспортный уровень также обеспечивает требуемый архитектурой сети размер пакетов данных.

➢ Подробнее о сетевых архитектурах – Ethernet, Token Ring и т.п. – рассказывалось в главе 1, раздел «Виды сетевых архитектур».

Стеки протоколов у различных пользователей должны быть одинаковыми. В предыдущем примере с электронным сообщением предполагалось, что получатель и адресат на своих компьютерах пользовались одним и тем же стеком протоколов (теоретическим стеком OSI). Даже совершенно разные машины с различными операционными системами могут связываться между собой, если они работают с общим стеком протоколов. Поэтому и станции UNIX, и Macintosh, и персональные компьютеры Windows применяют стек протоколов TCP/IP для связи в Internet. Если один узел будет использовать протокол TCP/IP, а другой – IPX/SPX, им не удастся установить связь: у этих протоколов разные правила и различный формат данных, что делает коммуникацию невозможной.

Коммуникация осуществляется также между одноранговыми компьютерами (отправителем и получателем). Получатель, принявший согласованное количество пакетов от отправителя, высылает подтверждение. Например, отправитель передает связку из трех пакетов и получает подтверждение от узла назначения. Тогда он может послать еще три пакета.

Связь на транспортном уровне нужна и в тех случаях, когда отправляющий узел слишком быстро передает сообщения. Получающий узел примет столько данных, сколько сможет сохранить, и вышлет сигнал «не готов», если будет послана дополнительная информация. После обработки поступивших данных получающий узел вновь способен принимать информацию, о чем сообщает отправителю с помощью сигнала «продолжай».

Сетевой уровень

Сетевой уровень предназначен для логической адресации пакетов и их доставки. На этом уровне происходит определение маршрута и фактическая коммутация пакетов по выбранному пути. На третьем уровне логический адрес (например, IP-адрес компьютера) переводится в физический (в аппаратный адрес сетевого адаптера, установленного на данном компьютере).

Маршрутизаторы работают именно на сетевом уровне и применяют протоколы маршрутизации для определения наилучшего пути передачи данных. Ниже будет подробно рассмотрено, как маршрутизаторы выбирают пути доставки и преобразуют логические адреса в физические.

➢ Рассказ о сетевом уровне будет продолжен в последующих главах. О функционировании маршрутизаторов на сетевом уровне говорится в главе 5.

Следует помнить, что каждый уровень модели OSI (и реальных протоколов) отвечает за те или иные операции с исходящими и входящими данными. При движении данных вниз по стеку уровней в отправляющем узле уровень представления данных преобразует информацию в общий формат. На получающем узле тот же уровень приведет данные к виду, который требуется соответствующей программе уровня приложения.

Канальный уровень

Достигшие *канального уровня* пакеты данных объединяются в кадры определенного сетевой архитектурой формата. Канальный уровень отвечает за движение данных по физической среде и однозначно определяет каждый компьютер в сети по его аппаратному адресу, жестко заданному на сетевой карте. На рис. 2.4 представлен аппаратный адрес сетевого адаптера, установленного на подключенном к сети компьютере с операционной системой Windows 98.

К каждому кадру добавляется заголовок, содержащий адрес отправителя и адрес получателя. Канальный уровень обеспечивает также безошибочную доставку кадров по физическому каналу. С этой целью протоколы канального уровня добавляют к каждому кадру дополнительное поле, содержащее *контрольную циклическую сумму* (cyclical redundancy check – CRC). Она вычисляется как в отправляющем, так и в принимающем компьютере. Совпадение полученных результатов означает, что кадр доставлен в целости и сохранности.

Как уже упоминалось, тип кадра, созданного канальным уровнем, зависит от архитектуры сети. На рис. 2.5 изображен кадр спецификации Ethernet 802.2. В табл. 2.1 приводится описание каждой из его составляющих. Если вы знакомы не со всеми частями кадра, представьте его пока в виде заголовка с описанием кадра, собственно данных и информации канального уровня (например, точек доступа к службам), которая не только определяет тип кадра (в данном случае Ethernet), но и помогает доставить кадр по назначению.

Канальный уровень также контролирует доступ компьютеров к физической среде. Этот аспект будет детально рассмотрен ниже, в разделе «Подуровни канального уровня».

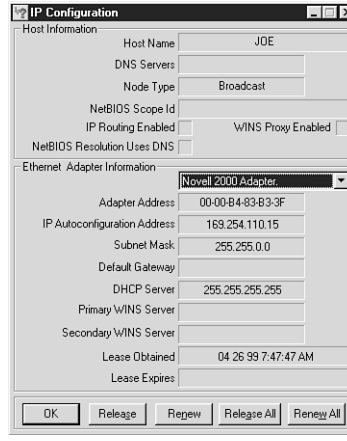


Рис. 2.4. Каждый узел сети имеет уникальный физический адрес

Реальные стеки протоколов применяют взаимодействие с установлением соединения и без него. В стеках таких сетевых протоколов, как TCP/IP и IPX/SPX, тоже используются оба метода взаимодействия. На сеансовом уровне обычно имеется несколько протоколов, работающих с помощью этих двух способов.

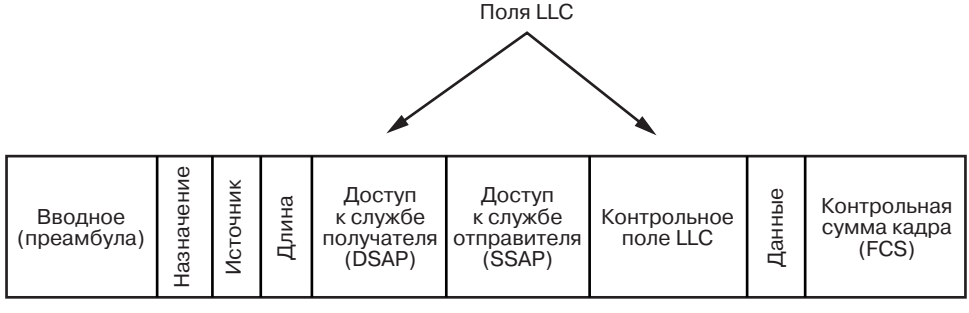


Рис. 2.5. Кадр Ethernet создается на канальном уровне модели OSI

Таблица 2.1. Поля кадра Ethernet

Сегмент	Назначение
Преамбула	Несколько битов, извещающих о посылке кадра, которые расположены в определенной последовательности
Назначение	Адрес получателя
Источник	Адрес отправителя

Таблица 2.1. Поля кадра Ethernet (окончание)

Сегмент	Назначение
Длина	Объем данных в байтах
DSAP	Точка доступа к службам получателя указывает принимающей сетевой карте место в буферной памяти, где нужно поместить кадр
SSAP	Точка доступа к службам отправителя
CTRL	Поле управления логическим каналом
Данные	Фактическая информация
FCS	Поле проверки кадра, содержащее контрольную циклическую сумму

Чтобы определить адрес сетевой карты, установленной на компьютере с операционной системой Windows, откройте меню **Пуск** ⇒ **Выполнить**. В командной строке наберите ***winipcfg*** *и нажмите* **OK**. *Появится диалоговое окно* **Конфигурация IP**, *в котором содержится адрес сетевой карты. В системе Windows NT правой кнопкой мыши щелкните по пиктограмме* **Сетевое окружение** *и откройте закладку* **Адаптеры**. *Выбрав нужный тип сетевого адаптера, щелкните по кнопке* **Свойства**. *В появившемся окне должен быть указан MAC-адрес сетевой карты.*

Физический уровень

На *физическом уровне* кадры, поступившие с канального уровня, преобразуются в битовый поток, который отправляется в среду передачи. Этот уровень определяет также реальные физические аспекты кабельного соединения. В получающем компьютере на физическом уровне принимается двоичный поток (информация, состоящая из нулей и единиц).

➢ Подробнее сетевые кабели были рассмотрены в главе 1 (раздел «Сетевые кабели»).

Подуровни канального уровня

Прежде чем завершить описание модели OSI, рассмотрим дополнительные спецификации, разработанные Институтом инженеров по электротехнике и электронике для канального уровня. Спецификации IEEE 802 подразделяют канальный уровень на два подуровня: управления логической связью (logical link control – LLC) и управления доступом к среде (media access control – MAC).

Подуровень LLC устанавливает и поддерживает связь между посылающим и принимающим компьютерами во время передачи данных по физической сетевой среде. Он также предоставляет точки доступа к службам (service access

points – SAP); другие компьютеры, отправляющие информацию, могут ссылаться на эти точки и использовать их для коммуникации с верхними уровнями принимающего узла. Подуровень управления логическим каналом описан в спецификации IEEE 802.2.

Подуровень MAC определяет, каким образом компьютеры осуществляют связь, как и когда компьютер может получить доступ к среде передачи, чтобы отправить данные. Спецификация 802 в действительности разбивает подуровень MAC на несколько категорий (способов доступа к среде), непосредственно связанных с конкретными сетевыми архитектурами, в частности Ethernet и Token Ring (рис. 2.6).

➢ О некоторых широко используемых архитектурах рассказывалось в главе 1 (раздел «Виды сетевых архитектур»).

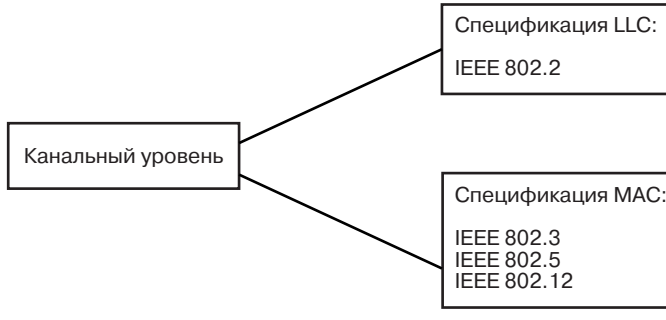


Рис. 2.6. Канальный уровень состоит из двух подуровней: LLC и MAC

Реальные сетевые протоколы

Теперь, когда мы обсудили теоретическую модель передачи данных от одного компьютера к другому, можно рассмотреть некоторые наиболее часто встречающиеся стеки протоколов и соотнести их с моделью OSI, чтобы понять, как функционируют реальные протоколы и какие протоколы того или иного стека отвечают сетевому уровню модели OSI. Эти протоколы очень важны для маршрутизации пакетов в интерсети.

Аппаратные адреса сетевых адаптеров называют также MAC-адресами. Они жестко определены в чипе ПЗУ сетевых карт и являются уникальными для каждой карты. Схема адресации была разработана IEEE. Реальный адрес имеет 48-битный формат и записывается в шестнадцатеричном виде, например 00-00-B3-83-B3-3F.

Кадры Ethernet, используемые в ранних версиях Novell NetWare (NetWare 2.x и 3.x), появились раньше, чем спецификации IEEE. Следовательно, кадр вида Ethernet 802.3 не соответствует описаниям IEEE. В новых версиях NetWare и других сетевых систем с архитектурой Ethernet применяются кадры вида Ethernet 802.2, полностью отвечающего спецификациям.

Протокол NetBEUI

Расширенный пользовательский интерфейс NetBIOS (NetBIOS extended user interface – NetBEUI) – это простой и быстрый сетевой протокол, созданный фирмами Microsoft и IBM для сетевых базовых систем ввода/вывода (network basic input output system – NetBIOS).

NetBEUI работает на транспортном и сетевом уровнях модели OSI, поэтому ему необходима NetBIOS, которая функционирует на сеансовом уровне и отвечает за установку связи между компьютерами. В сетях Microsoft есть еще два компонента: *редиректор* и *блок сообщений сервера* (server message block – SMB). Редиректор относится к уровню приложения, позволяя клиенту воспринимать все сетевые ресурсы как локальные. Блок сообщений сервера обеспечивает равноправную связь между редиректорами клиента и сервера, действуя на уровне представления данных.

Хотя NetBEUI является отличным транспортным протоколом с низкими издержками, его невозможно применять в интерсетях, где имеет место маршрутизация. Таким образом, NetBEUI годится в случае небольших, простых сетей, но не подходит для больших сетевых систем, в которых задействованы маршрутизаторы (поэтому далее в этой книге протокол NetBEUI рассматриваться не будет).

Протокол TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) стал в настоящее время стандартным протоколом для корпоративных сетей. Сети TCP/IP легко расширяемы, поэтому TCP/IP можно использовать как в малых, так и в крупных компьютерных сетях.

TCP/IP – маршрутизируемый стек протоколов, который способен функционировать на различных программных платформах (Windows, UNIX и т.д.). Многие сетевые операционные системы включают в себя TCP/IP в качестве основного протокола. Стек TCP/IP состоит из нескольких компонентов, а поскольку он был разработан до создания модели OSI, то его компоненты не точно соответствуют уровням теоретической модели. На рис. 2.7 изображен стек TCP/IP, соотнесенный с моделью OSI (это общий вид протокола TCP/IP, а не исчерпывающий список всех протоколов стека). В табл. 2.2 описаны протоколы, указанные на рисунке.

➢ Подробнее обо всех протоколах стека TCP/IP рассказывается в главе 10.

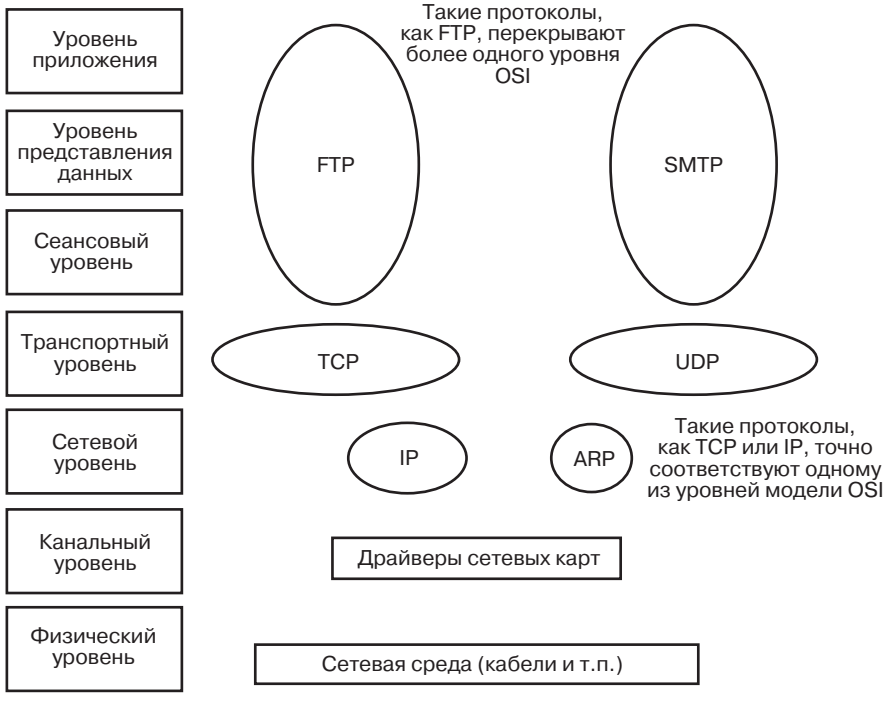


Рис. 2.7. Стек TCP/IP состоит из большого числа протоколов

Таблица 2.2. Протоколы стека TCP/IP

Протокол	Назначение
FTP	File Transfer Protocol обеспечивает интерфейс и службы для пересылки файлов по сети IP
SMTP	Simple Mail Transfer Protocol предоставляет почтовые услуги в сетях Internet
TCP	Transport Control Protocol ориентирован на установление соединения. Он управляет связью между посылающим и принимающим компьютерами
UDP	User Datagram Protocol – транспортный протокол, в отличие от TCP действующий без установления соединения
IP	Internet Protocol работает без установления соединения на сетевом уровне и предоставляет возможность логической адресации в сетях TCP/IP
ARP	Address Resolution Protocol соотносит IP-адреса с аппаратными MAC-адресами

TCP/IP располагает не только богатым набором сетевых средств (а это значит, что он требует довольно больших затрат), но и уникальной системой логической адресации. Пользователи, имеющие доступ в Internet, знакомы с 32-битным IP-адресом, который обычно записывается в виде четырех октетов (один октет состоит

из восьми бит). Типичный IP-адрес имеет формат вида 129.30.20.4, где каждое из десятичных чисел представляет собой восемь бит информации.

➢ В главе 10 IP-адресация будет рассмотрена более обстоятельно.

Поскольку TCP/IP весьма важен для интерсетей, а маршрутизация сетей TCP/IP – дело непростое, аспектам адресации TCP/IP посвящена целая глава настоящей книги. Кроме того, ниже будет подробно рассказано о командах, относящихся к маршрутизации TCP/IP в кампусной или корпоративной сети.

➢ Начать изучение TCP/IP и маршрутизации лучше всего с главы 10.

Спецификации IEEE 802 разделяются на категории, характеризующие подуровень LLC и различные виды архитектур, которые могут содержаться в подуровне MAC. Приведем полный список категорий 802:

802.1 Межсетевое взаимодействие
802.2 Управление логической связью
802.3 Локальные сети Ethernet (CSMA/CD)
802.4 Маркерные шины
802.5 Маркерные кольца
802.6 Городские сети
802.7 Консультативный технический совет по широкополосной передаче данных
802.8 Консультативный технический совет по волоконной оптике
802.9 Сети для совместной передачи данных и голоса
802.10 Защита сетей
802.11 Беспроводные сети
802.12 Сети с приоритетным доступом по запросу

Протокол IPX/SPX

Протокол межсетевого/последовательного обмена пакетами (Internetwork Packet Exchange/Sequenced Packet Exchange – IPX/SPX) разработан компанией Novell для сетевых операционных систем Novell NetWare. Стек IPX/SPX не такой емкий,

Протокол TCP/IP был разработан Управлением перспективных исследовательских программ (DARPA). Министерству обороны требовался стек протоколов, функционирующий в неоднонаправленных сетях. Подобные сети благодаря тендерам существовали среди поставщиков сетевых решений, и правительство неожиданно оказалось в ситуации, когда в различных подразделениях министерства (ВМФ, ВВС и т.д.) оказались установлены разные компьютерные системы. Поэтому TCP/IP, созданный для устранения возникшей проблемы, в шутку называют «протоколом неудачного тендера».

как TCP/IP, и не требует лишних затрат. IPX/SPX маршрутизируем и подходит не только для малых, но и для крупных сетей.

На рис. 2.8 изображены протоколы стека IPX/SPX в соотношении с моделью OSI. В табл. 2.3 представлено краткое описание каждого протокола. Наиболее интересен вопрос маршрутизации IPX/SPX в интерсетях.

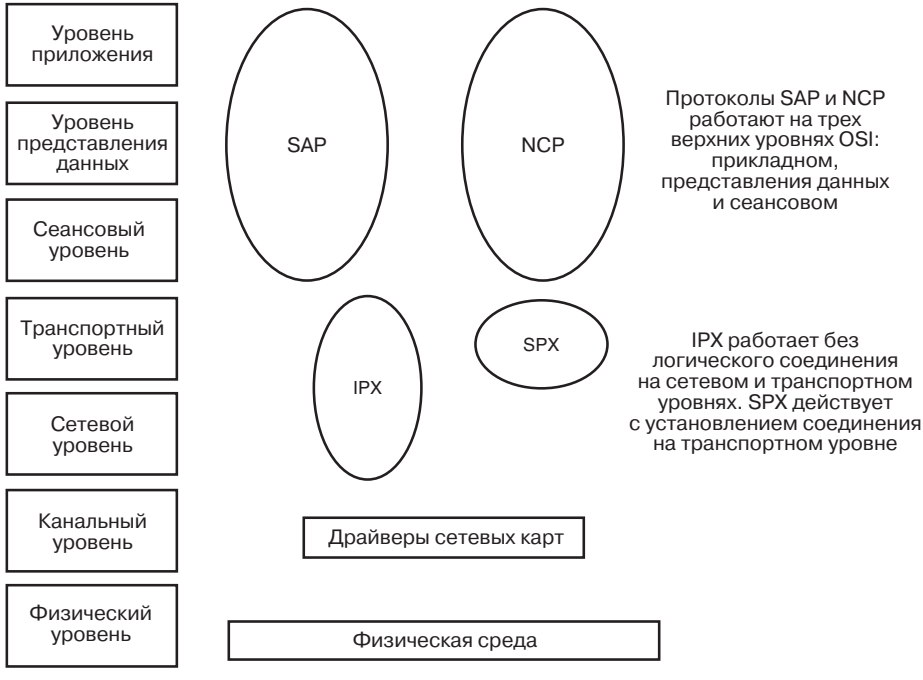


Рис. 2.8. Протокол IPX/SPX эффективно используется в малых и больших сетях

Таблица 2.3. Протоколы стека IPX/SPX

Протокол	Назначение
SAP	Service Advertising Protocol используется файловыми серверами и серверами печати NetWare для объявления адреса сервера с запущенными службами Novell
NCP	NetWare Core Protocol выполняет сетевые функции на трех верхних уровнях модели OSI (приложения, представления данных и сеансовом). Он формирует пакеты и обеспечивает соединение между клиентом и сервером
SPX	Sequenced Packet Exchange Protocol – транспортный протокол, ориентированный на установление соединения
IPX	Internetwork Packet Exchange Protocol – транспортный протокол, действующий без установления соединения и обеспечивающий адресацию и маршрутизацию

➢ Маршрутизация IPX/SPX рассматривается в главе 12.

Протокол AppleTalk

Хотя многие сетевые администраторы не считают *AppleTalk* межсетевым протоколом или протоколом для корпоративных сетей, он маршрутизируем. При наличии соответствующей сетевой карты (компьютеры Macintosh можно объединить, например, в сеть Ethernet, если оснастить их адаптером EtherTalk) протокол AppleTalk поддерживает архитектуры Ethernet, Token Ring, FDDI; его имеет смысл рассматривать как один из основных маршрутизируемых протоколов для корпоративных сетей.

AppleTalk – это не только архитектура (о ней рассказывалось в главе 1), но и стек протоколов. На рис. 2.9 представлены протоколы AppleTalk в соотношении с моделью OSI, а в табл. 2.4 приведены их краткие описания.

На рис. 2.7–2.9 изображены реальные протоколы в соответствии с моделью OSI. Чтобы понять эти рисунки, вспомните, как модель OSI описывает движение данных по семи уровням и как информация преобразуется на этом пути. Реальные протоколы выполняют все функции, описанные в модели, хотя и с помощью меньшего числа протоколов. TCP/IP, например, содержит протоколы, относящиеся сразу к нескольким уровням. Так, протокол FTP выполняет функции уровней приложения, представления данных и сеансового. Овал вокруг надписи FTP охватывает три верхних уровня модели OSI.

Прежде чем продвигаться дальше, нужно договориться о значении некоторых терминов, часто встречающихся в этой книге.
Интерсеть – сеть сетей. Локальные сети, связанные друг с другом мостом или маршрутизатором. (Межсетевое взаимодействие подробно рассматривается в главе 4.)
Internet – глобальная сеть сетей. TCP/IP фактически является стандартным протоколом для глобального соединения разнородных компьютеров.
intranet – корпоративная сеть, не подключенная к глобальной, но использующая такие межсетевые протоколы, как SMTP и HTTP для разделения информации между сотрудниками компании.
extranet – это та же сеть intranet, но предоставляющая сотрудникам компании доступ к некоторым внешним ресурсам.

Вы, вероятно, заметили, что диаграммы соответствия различных протоколов модели OSI не содержат протоколов маршрутизации. Естественно, в каждом стеке имеется свой протокол маршрутизации. Например, в стеке TCP/IP основным является информационный протокол маршрутизации (RIP), а в AppleTalk – протокол управления таблицами маршрутизации. Более детально они будут описаны при обсуждении маршрутизации в соответствующих стеках протоколов.

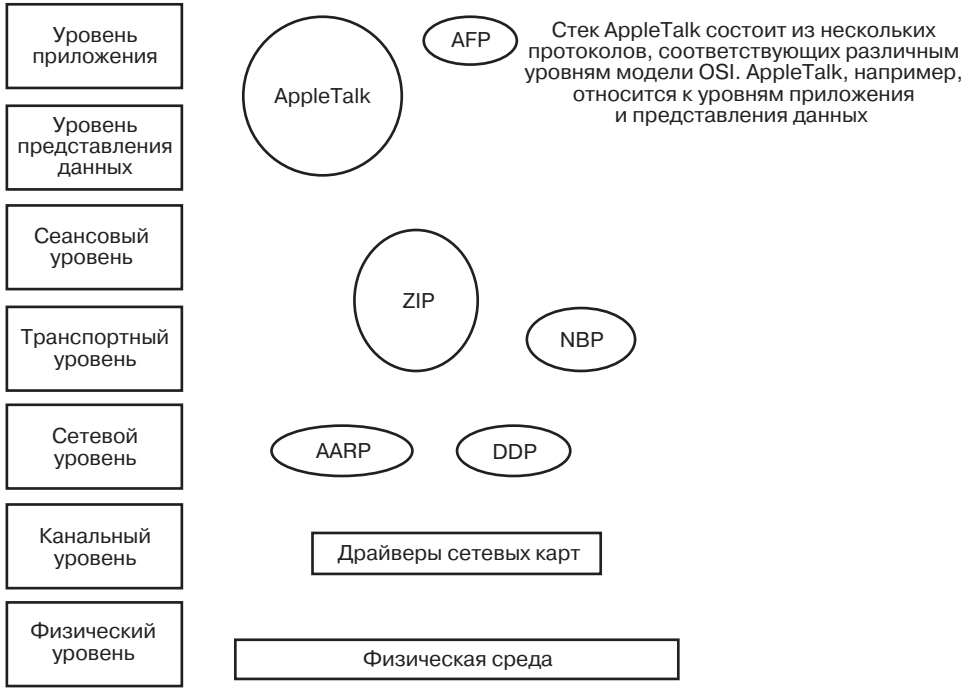


Рис. 2.9. AppleTalk – маршрутизируемый стек протоколов для сетей Macintosh

Таблица 2.4. Протоколы стека AppleTalk

Протокол	Назначение
AppleShare	Предоставляет услуги на уровне приложения
AFP	AppleTalk Filing Protocol обеспечивает совместное использование файлов узлами сети
ATP	AppleTalk Transaction Protocol связывает компьютеры на транспортном уровне
NBP	Name Binding Protocol устанавливает соответствие между именами узлов и адресами сетевого уровня
ZIP	Zone Information Protocol управляет зонами AppleTalk и соотносит их имена и сетевые адреса
AARP	AppleTalk Address Resolution Protocol устанавливает соответствие между адресами сетевого уровня и аппаратными адресами канального уровня
DDP	Datagram Delivery Protocol обеспечивает систему адресации в сети AppleTalk и производит передачу датаграмм без установления соединения

Как и в случае IPX/SPX, интерес к стеку AppleTalk связан с возможностью маршрутизировать этот протокол.

➢ Подробнее об устройстве сетей AppleTalk и маршрутизации одноименного протокола на маршрутизаторе Cisco рассказывается в главе 13.

ГЛАВА 3

Глобальные сети

По мере того как локальные компьютерные сети становились все более важными для коммерческих фирм, корпораций и организаций, возникла необходимость расширять их и соединять между собой. В пределах небольшого пространства это осуществлялось с помощью таких устройств межсетевого взаимодействия, как повторители, коммутаторы и маршрутизаторы. Однако для объединения локальных сетей, разделенных большими расстояниями, нужно иное решение. Потребность в такой технологии стала очевидной для администраторов крупных корпораций, имеющих отделения по всему миру.

Для расширения сети на большие расстояния существуют различные сетевые стандарты. Компьютерные сети могут быть связаны через коммутируемую телефонную сеть общего пользования или через частных операторов. Очень крупные компании способны развить собственную инфраструктуру глобальных сетей и вложить средства в оборудование для микроволновой и спутниковой связи.

Технология глобальных сетей подходит для объединения сетей сначала внутри города, а затем по стране и по всему миру. В глобальной сети, где решены вопросы, относящиеся к физическому уровню, передача данных также осуществляется посредством различных протоколов. Но если в локальной сети физический уровень обеспечивается кабелем и концентраторами, то в глобальной целесообразно применять выделенную линию T1 или спутниковую тарелку.

➢ Более детально межсетевое взаимодействие описывается в главе 4.

То обстоятельство, что в локальных сетях используется физическая сетевая среда (медные или волоконно-оптические кабели), не исключает применения в глобальных сетях и беспроводных технологий – микроволновой передачи, спутниковой связи, инфракрасного излучения или радиосвязи (как на одной частоте, так и в широком спектре частот).

Установка связи

В то время как физическая инфраструктура локальной сети (кабели, концентраторы, повторители и т.д.) принадлежит компании, владеть физическим оборудованием глобальных сетей слишком дорого.

Здесь существует три вида соединений: связь через коммутируемую телефонную сеть общего пользования с помощью модема, связь по выделенной линии и коммутируемая связь, предоставляющая многим пользователям одну и ту же линию.

У каждого из перечисленных способов есть свои достоинства и недостатки, и в каждом случае необходимо специальное оборудование. Ниже будут рассмотрены методы организации глобальной связи.

Один из секретов успешного администрирования глобальной сети заключается в разработке большой сети и возможной маршрутизации таким образом, чтобы данные в основном находились в сети, принадлежащей компании. Если вы платите за высокую пропускную способность выделенных линий, то главной задачей для вас станет создание экономически эффективной глобальной сети.

Соединение по телефонной линии

Проще всего организовать удаленное соединение, связав два компьютера через модем и обычную аналоговую телефонную линию. *Модем* преобразует цифровую информацию, поступающую от компьютера, в аналоговый сигнал (модулирует) и обратно (демодулирует), что отражено в его названии. Такая трансформация позволяет компьютеру посылать сообщения по аналоговой линии. Существуют модемы, обеспечивающие потенциальную скорость передачи в 56 Кбит/с, но шум в линии нередко ограничивает реальную скорость.

Маршрутизаторы иногда снабжаются интерфейсом для связи через модем (в таком случае их называют *серверами доступа*). Это означает, что две локальные сети могут соединяться через телефонную сеть, и пакеты будут маршрутизироваться (хотя скорость такого соединения весьма мала). На рис. 3.1 изображены две локальные сети, связанные через телефонную линию и маршрутизаторы.

Выделенные линии

Выделенные линии обеспечивают постоянное соединение между двумя сетями через телефонную коммутируемую сеть общего пользования или другие службы. Как правило, это цифровые линии: они обладают большей пропускной способностью, чем аналоговые, и менее подвержены шумам и помехам, характерным для обычных телефонных каналов.

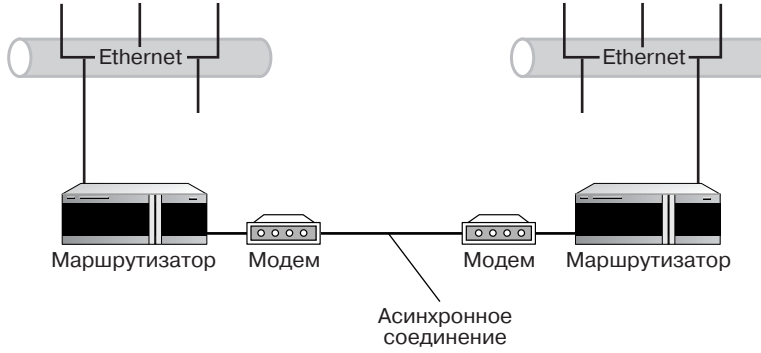


Рис. 3.1. Объединение локальных сетей через телефонную линию и модемы

Цифровые линии, применяемые для передачи данных, – это в большинстве случаев линии службы цифровой передачи данных (digital data service – DDS) и магистрали класса T (T-Carrier).

Телефонные коммутируемые сети общего пользования (PSTN) часто называют «простыми телефонными сетями» (POTS). Однако иногда им дают и другие имена, особенно если связь по выделенной линии пропадает.

Линии DDS

Линии DDS, обычно предоставляемые местной телефонной сетью, способны обеспечивать постоянное дуплексное (с одновременной передачей и получением данных) соединение с пропускной способностью до 64 Кбит/с. Поскольку линии DDS являются цифровыми, для подключения локальной сети к выделенной линии требуется устройство CSU/DSU (Channel Service Unit/Data Service Unit), которое преобразует данные, поступающие из локальной сети, в цифровой сигнал.

Локальная сеть присоединяется к порту DSU, а цифровая линия – к порту CSU. Как правило, между локальной сетью и CSU/DSU устанавливают устройство межсетевого взаимодействия, например мост или маршрутизатор (рис. 3.2).

Линии DDS – это особые цифровые выделенные линии, доступ к которым обеспечивается телефонной компанией. Цифровая сеть с предоставлением комплексных услуг (integrated services digital network – ISDN) – это технология, разработанная для уже существующих телефонных линий.

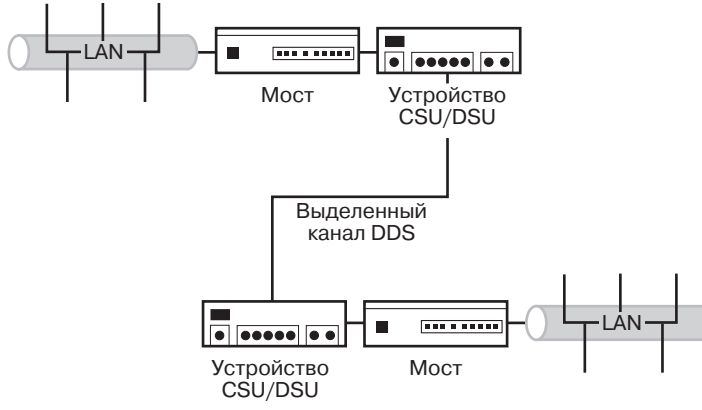


Рис. 3.2. Соединение двух локальных сетей через линию DDS

Магистрали класса T

В системах *магистралей класса T* допустимо объединять несколько различных типов данных (например, данные из локальной сети и голосовую связь) и передавать их по одному высокоскоростному каналу.

Устройство, способное объединять сигналы с разных каналов в один и распределять полученный поток по соответствующим каналам, называется *мультиплексором*, или *MUX*. На рис. 3.3 изображены две локальные сети, связанные магистралью класса T. Мультиплексоры, находящиеся на обоих концах цифровой линии, предназначены для группировки и разгруппировки различных каналов данных.

Линия T1 является основной единицей системы магистралей класса T. Она состоит из 24 каналов с пропускной способностью в 64 Кбит/с каждый, что обеспечивает общую скорость передачи, равную 1,544 Мбит/с. Существуют и другие типы магистралей класса T с большим числом каналов и большей пропускной способностью, но они значительно дороже. В табл. 3.1 представлены различные виды линий класса T.

Таблица 3.1. Системы магистралей класса T

Тип линии	Каналы	Суммарная скорость, Мбит/с
T1	24	1,544
T2	96	6,312
T3	672	44,736
T4	4032	274,76

Наиболее доступным типом магистрали является линия T1, построенная на медном проводе. Как упоминалось ранее, небольшие фирмы могут арендовать

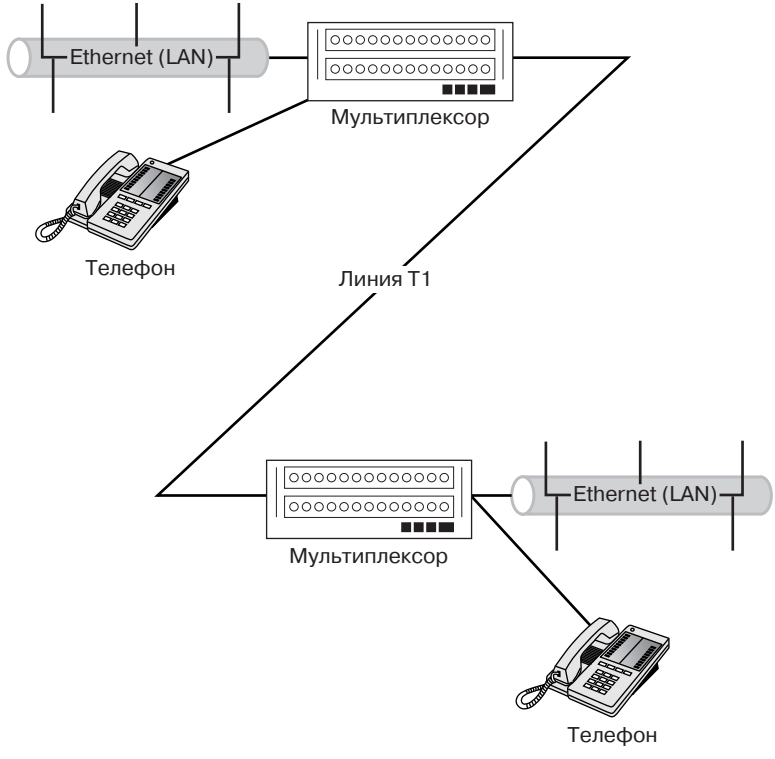


Рис. 3.3. Локальные сети, связанные магистралью класса T

лишь часть каналов. Линии T2 не предоставляются для общего доступа и функционируют лишь в пределах телефонной компании.

Магистрали с большей пропускной способностью, такие как T3 и T4, основаны на оптоволоконных кабелях; они применяются только крупными корпорациями и правительственными учреждениями (во многом из-за их высокой стоимости).

Компании, которая подключается к магистрали класса T, требуется такое же оборудование, что и для присоединения к любой другой цифровой выделенной линии. Между цифровой линией и межсетевым устройством (мостом или маршрутизатором), связанным с локальной сетью, устанавливается CSU/DSU. Как уже говорилось, при необходимости для объединения и разъединения сигналов разного вида служит мультиплексор.

Линии DDS постепенно уходят в прошлое, их замещают технологии коммутации пакетов, в частности Frame-Relay. Благодаря снижению стоимости магистралей класса T и применению дробных линий T1 (то есть выделенных частично) им отдается предпочтение в сфере глобальных сетей.

Принцип действия мультиплексора используется и в кабельном телевидении. Единый сигнал поступает в телевизор или видеомагнитофон по кабелю и попадает в мультиплексор, разбивающий этот поток на множество телевизионных каналов. Смысл широкополосной передачи состоит именно в этом – пропускать много каналов по одному кабелю.

Линия T1 является основной единицей системы магистралей класса T. Другие магистрали в действительности представляют собой объединение линий T1. Так, линия T2 состоит из четырех линий T1, T3 – из 28, а T4 – из 168.

Обзор коммутируемых сетей

Третий способ глобального объединения сетей – *коммутация*. Коммутируемые сети позволяют нескольким пользователям применять одну и ту же линию. Такие сети не столь дороги, как выделенные линии.

По существу, локальная сеть взаимодействует с глобальной через провайдера или непосредственно через телефонную компанию. Исходящие данные попадают в коммутируемую сеть, которую на схемах обычно изображают в виде облака, поскольку путь информации через нее всякий раз может быть иным (рис. 3.4).

Связь между локальной сетью и *коммутируемой сетью общего пользования* (public data network – PDN) осуществляется *оконечным оборудованием пользователя* (digital terminal equipment – DTE), таким как маршрутизатор. Между маршрутизатором и коммутируемой сетью может быть подключено *оконечное оборудование канала передачи данных* (data circuit terminating equipment – DCE), например CSU/DSU, которое обеспечивает полосу пропускания и временны е установки для передачи данных[1]. Сеть общего пользования предоставляет линии и коммутирующее оборудование для передачи данных через облако коммутируемой сети.

Существует два типа коммутируемых сетей: с коммутацией каналов и с коммутацией пакетов.

Коммутация каналов

При *коммутации каналов* между отправителем и получателем в сети общего пользования устанавливается выделенное соединение. Информация отсылается по каналу (линиям), определенному для данного сеанса. По завершении передачи связь прекращается.

[1] Оборудование DCE иначе называют *оконечным оборудованием провайдера. – Прим. научн. ред.*

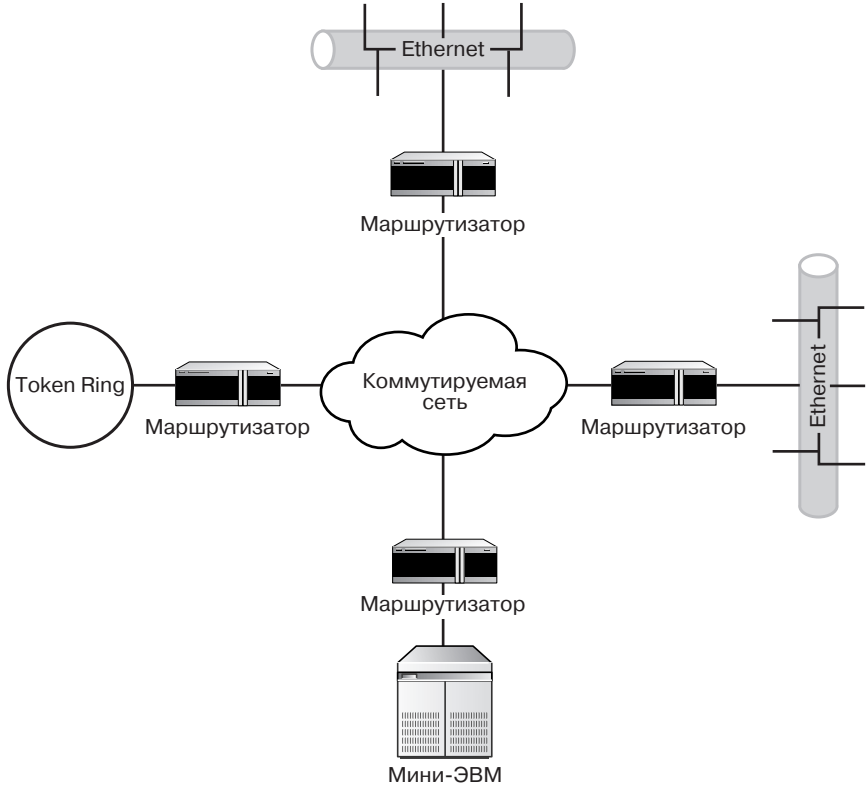


Рис. 3.4. Коммутируемые сети позволяют взаимодействовать локальным сетям, расположенным на значительном расстоянии друг от друга

Примером технологии с коммутацией каналов может служить *цифровая сеть с предоставлением комплексных услуг* (integrated services digital network – ISDN). В сетях ISDN, которые выделяются телефонными компаниями, применяются системы цифровой коммутации. Стоимость соединения ISDN зависит от частоты использования линии, а общая сумма складывается из оплаты соединения и ежемесячного абонентского взноса.

Существует две разновидности ISDN: ISDN BRI и ISDN PRI. В интерфейсе BRI (Basic Rate Interface) пользователям предоставляется три канала: два B-канала по 64 Кбит/с и D-канал со скоростью 16 Кбит/с, предназначенный для передачи контрольной информации и настроек. Интерфейс BRI допускает одновременную трансляцию голоса и данных по отдельным B-каналам. Однако обычно из двух B-каналов делают один с общей скоростью передачи 128 Кбит/с.

Интерфейс PRI (Primary Rate Interface) разработан для крупных компаний, нуждающихся в большей полосе пропускания. Он основан на линии T1, которая располагает 23 B-каналами (каждый по 64 Кбит/с). Один D-канал по-прежнему требуется для настроек и контроля соединения.

➢ Конфигурирование ISDN на маршрутизаторе обсуждается в главе 15 (раздел «Конфигурирование ISDN»).

Интерфейс передачи с базовой скоростью разрабатывался для небольших фирм и отдельных пользователей, которые нуждались в оперативном соединении локальной сети с глобальной, в особенности с Internet. Существует технология, обеспечивающая более быструю связь – цифровые абонентские линии (digital subscriber service – DSL). DSL позволяет передавать данные и голос со скоростью до 7 Мбит/с. Стоимость использования DSL, предоставленных местной телефонной компанией, может оказаться меньше, чем сумма телефонного счета и ежемесячной платы за удаленное аналоговое соединение через модем. Таким образом, DSL являются более дешевой альтернативой интерфейсу передачи с базовой скоростью.

Коммутация пакетов

В соединениях на основе *коммутации пакетов* данные разделяются на пакеты небольшого размера, благодаря чему обеспечивается их быстрая и эффективная доставка.

Каждый пакет наделен собственной контрольной информацией и коммутируется через сеть независимо от других пакетов. Это означает, что данные могут передаваться различными путями через облако коммутируемой сети и приходить к получателю в измененной последовательности. Тем не менее сведения об очередности, содержащиеся в заголовке каждого пакета, позволяют восстановить порядок поступивших сообщений.

В сетях с коммутацией пакетов возможно применение виртуальных каналов. *Виртуальный канал* устанавливает определенный путь через облако сети, по которому передаются все пакеты, предназначенные для конкретного получателя (эти пути могут служить для пересылки пакетов от многих отправителей, поскольку линии в коммутируемых сетях находятся в общем пользовании). За счет виртуальных каналов в сетях с коммутацией пакетов удается увеличить общую эффективность передачи данных.

Существует несколько технологий коммутации пакетов: X.25, Frame-Relay, ATM; они описаны в следующем разделе.

Протоколы коммутации пакетов

Сети с коммутацией пакетов появились в конце 70-х годов XX века вместе с протоколом X.25. Низкая стоимость таких сетей (в сравнении с выделенными линиями) обусловила стремительное развитие соответствующих протоколов. Далее описываются некоторые распространенные протоколы коммутации пакетов.

X.25

Протокол *X.25* предназначен для сетей общего пользования таких операторов, как AT&T и General Electric. Стек протоколов X.25 обеспечивает прямую связь между локальными сетями с помощью оконечного оборудования пользователя (DTE) и оконечного оборудования канала передачи данных (DCE). DCE предоставляет соединение DTE, например маршрутизатора, непосредственно с глобальной сетью.

Поскольку назначение всякой глобальной сети заключается в установлении связи между удаленными друг от друга локальными сетями, сеансы X.25 состоят из коммуникаций между DTE. Допустим, у вас есть локальная сеть в Чикаго, подключенная к маршрутизатору, который связывает ее с сетью общего пользования. Аналогично в Миннеаполисе имеется подобная локальная сеть, выходящая на сеть общего пользования через маршрутизатор. Протокол X.25 управляет взаимодействием между двумя DTE (маршрутизаторами), осуществляя передачу данных (рис. 3.5).

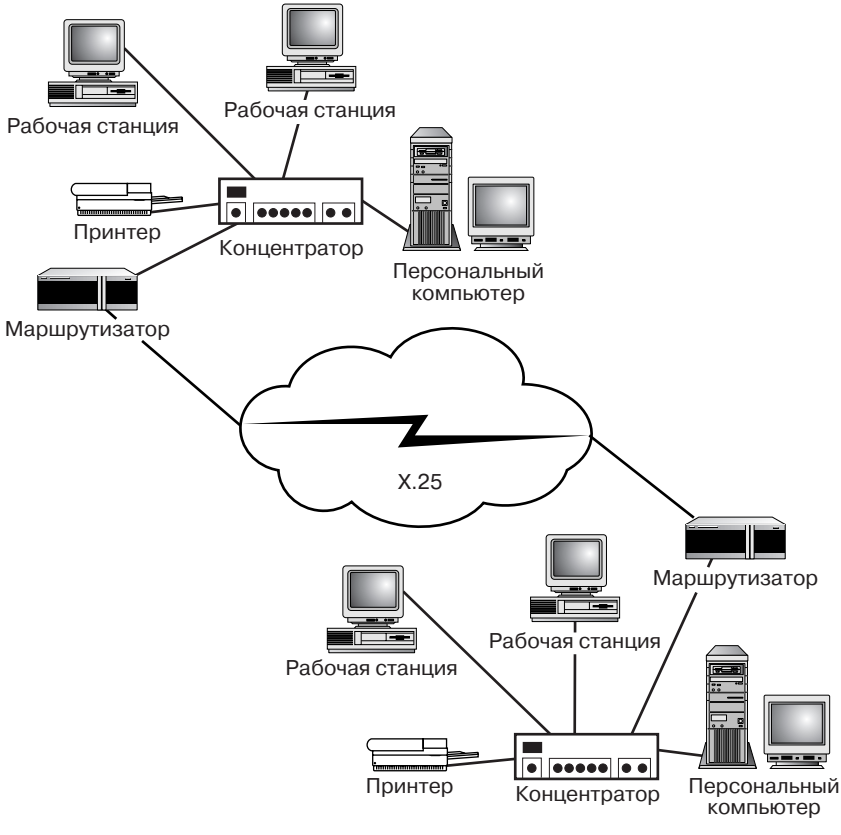


Рис. 3.5. Протокол X.25 устанавливает виртуальный канал между маршрутизаторами

Стек протоколов X.25 составлен из протоколов, работающих на сетевом, канальном и физическом уровнях модели OSI. Рассмотрим их подробнее:

- протокол пакетного уровня (Packet Layer Protocol – PLP) относится к сетевому уровню и управляет обменом пакетов между локальными сетями (между маршрутизаторами в Чикаго и Миннеаполисе в рассмотренном выше примере). PLP устанавливает виртуальный канал между устройствами оконечного оборудования данных и отвечает за сегментацию и восстановление последовательности пакетов. Кроме того, PLP закрывает виртуальный канал по завершении передачи;
- сбалансированный протокол доступа к каналу (Link Access Procedure/Balanced Protocol – LAP/B) действует на канальном уровне и обеспечивает безошибочную и упорядоченную доставку кадров;
- протокол физического уровня X.21 bis отвечает за активацию и дезактивацию физической среды, соединяющей устройства DTE и DCE.

Протокол X.25, созданный для коммутируемых телефонных сетей общего пользования с высоким уровнем шумов, выполняет множество проверок на возможные ошибки при передаче пакетов. И хотя X.25 применяется до сих пор, его скоро вытеснят скоростные протоколы коммутации пакетов – Frame-Relay и ATM.

➢ Конфигурирование X.25 на маршрутизаторе будет рассмотрено в главе 15 (раздел «Конфигурирование протокола X.25»).

С помощью протокола X.25 можно организовать виртуальное соединение двух типов: коммутируемые виртуальные каналы (switched virtual circuit – SVC) устанавливаются для данного сеанса связи и разрываются по его завершении; постоянные виртуальные каналы (permanent virtual circuit – PVC) используются для регулярной связи двух пунктов и поддерживают постоянный сеанс связи между сетями.

Frame-Relay

Frame-Relay – «наследник» протокола X.25. Он реализует высокоскоростные соединения между устройствами DTE (такими, как маршрутизаторы и мосты) через волоконно-оптические кабели. Устройства DCE в сетях Frame-Relay представляют собой коммутаторы среды передачи данных. Протокол Frame-Relay обеспечивает большую скорость, чем X.25, поскольку избавлен от некоторых функций контроля и проверок на ошибки, которые снижали скорость X.25.

Frame-Relay применяет постоянные виртуальные соединения в сеансах связи. Сетевой провайдер наделяет их идентификатором канала передачи данных (data link connection identifier – DLCI). Поскольку в интерфейсе Frame-Relay допускается существование нескольких виртуальных соединений, идентификатор каждого конкретного канала может функционировать в качестве указателя, осу-

ществляющего доставку пакетов по назначению. Это достигается отображением логических адресов (например, IP-адресов) посылающего и принимающего DTE на идентификатор используемого ими виртуального канала.

➢ Конфигурирование Frame-Relay на маршрутизаторе рассматривается в главе 15 (раздел «Конфигурирование протокола Frame-Relay»).

Асинхронная передача данных

Еще одним способом коммутации пакетов является метод *асинхронной передачи данных* (asynchronous transfer mode – ATM). ATM – это развитый протокол пакетной коммутации, работающий с пакетами фиксированного размера (53 байта), которые называются *ячейками*. Благодаря строго определенному объему пакетов увеличивается скорость передачи данных: коммутационное и маршрутизирующее оборудование быстрее пересылает единообразные ячейки, чем кадры неодинаковой величины.

Теоретически ATM в состоянии доставить информацию со скоростью до 2,4 Гбит/с, однако реальные цифры варьируются в пределах от 45 до 622 Мбит/с. Скорость в 622 Мбит/с достигается в самой быстрой сетевой среде – оптической сети ONET (разработка фирмы Bell Communications Research), которая способна передавать голос и данные.

Линии связи и ATM, и Frame-Relay предполагаются бесшумными. Таким образом, в случае ATM не требуется дополнительных средств для проверок на ошибки (что, напомним, снижало скорость коммутации пакетов в X.25). ATM подходит для магистралей FDDI городских сетей (со скоростью 100 Мбит/с) и выделенных линий T3 (45 Мбит/с).

Нет смысла рассматривать здесь технологию ATM с точки зрения конфигурирования маршрутизаторов, поскольку сети ATM оборудуются не маршрутизаторами, а специальными коммутаторами, быстро передающими данные от одного устройства к другому.

Другие протоколы глобальных сетей

При работе с маршрутизаторами важную роль играют еще два протокола: *высокоуровневый протокол управления каналом передачи данных* (High-Level Data-Link Control – HDLC) и *протокол двухточечной связи* (Point-to-Point Protocol – PPP). Они обычно конфигурируются как протоколы последовательного интерфейса маршрутизатора:

- HDLC является основным протоколом глобального сетевого взаимодействия для последовательного интерфейса маршрутизатора Cisco и применяется при синхронных последовательных соединениях (таких, как ISDN). Модификация этого протокола канального уровня, используемая в маршрутизаторах Cisco, работает, к сожалению, только с устройствами Cisco;

- протокол PPP задействуется обычно для удаленного доступа к сетям TCP/IP (например, Internet). Он может функционировать как в асинхронных (с телефонным соединением), так и в синхронных линиях. Этот протокол поддерживает сжатие данных и обеспечивает проверку прав доступа пользователя с помощью *протокола аутентификации по паролю* (password authentication protocol – PAP) или *протокола аутентификации по методу «вызов-приветствие»* (challenge handshake authentication protocol – CHAP).

Конфигурирование HDLC и PPP на маршрутизаторе рассмотрено в главе 15 (разделы «Конфигурирование протокола HDLC» и «Конфигурирование протокола PPP»).

ГЛАВА 4

Основы межсетевого взаимодействия

Строго говоря, межсетевое взаимодействие – это взаимодействие двух и более локальных сетей, при котором они функционируют как самостоятельные единицы объединенной сети. В более широком смысле под взаимодействием сетей понимают методы расширения, сегментации и объединения локальных сетей таким образом, чтобы общая пропускная способность была как можно выше. В данном случае пропускной способностью называют потенциальную скорость передачи данных по физической среде (например, 10 Мбит/с в сети 10BaseT).

В межсетевом взаимодействии применяются технологии и локальных, и глобальных сетей. Существенной особенностью является возможность объединения сетей не только с одинаковой топологией (например, локальных сетей Ethernet), но и с разными архитектурами (скажем, сетей Ethernet и Token Ring). Отличный пример реального взаимодействия сетей – Internet.

На рис. 4.1 изображена интерсеть, в основу которой положены некоторые типовые примеры межсетевого взаимодействия.

При расширении локальной сети увеличивается количество подключенных к ней рабочих станций. Если вы расширяете сеть путем объединения нескольких удаленных локальных сетей, придется воспользоваться технологиями глобальных сетей. Внедрение в локальную сеть новых серверов и рабочих станций увеличивает нагрузку на сеть и приводит к снижению ее пропускной способности. В этом случае желательно осуществить сегментацию сети и тем самым сохранить пропускную способность. Ниже рассматриваются обе представленные ситуации.

Устройства межсетевого взаимодействия

По мере роста сети вам придется решать вопросы, связанные с ее расширением, сохранением пропускной способности и объединением с удаленными сетями. Существует несколько устройств, предназначенных для этих целей: повторители, мосты, коммутаторы, маршрутизаторы, шлюзы.

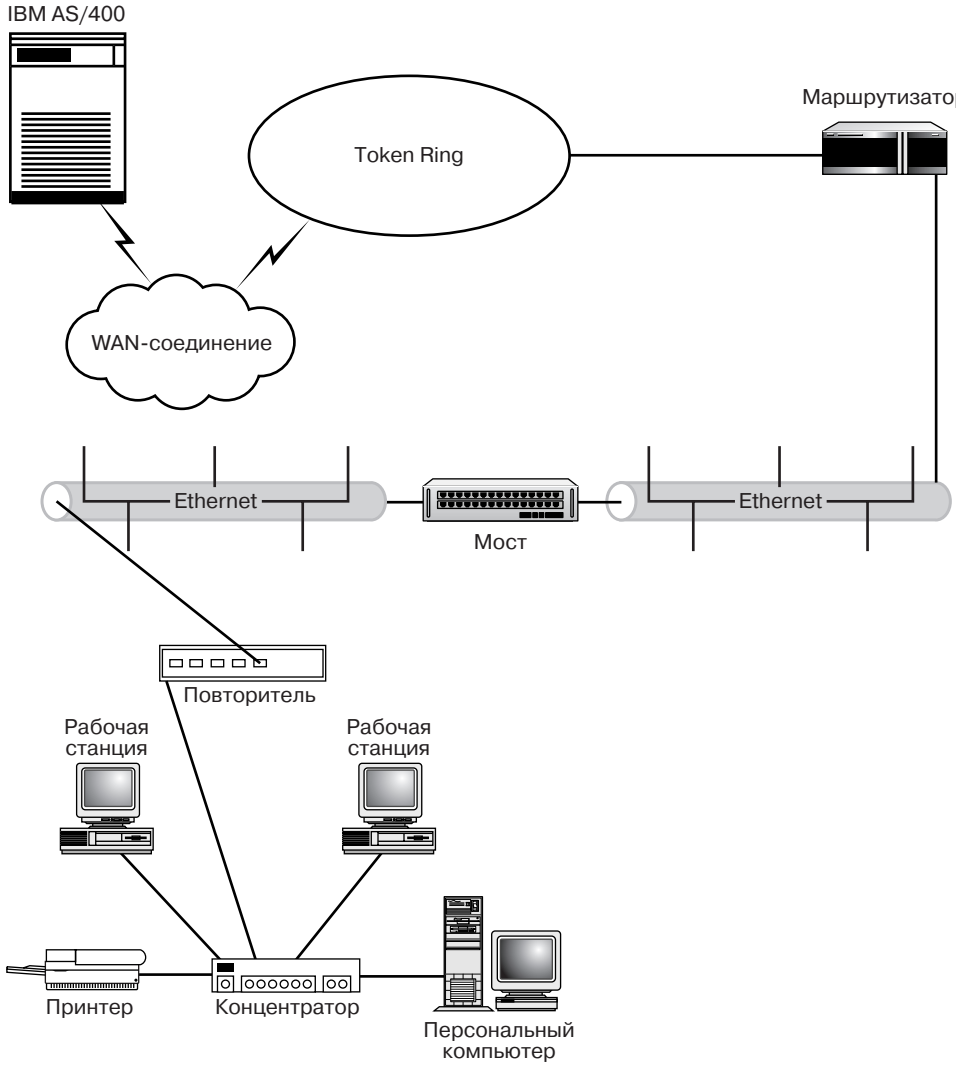


Рис. 4.1. В интерсетях применяются технологии локальных и глобальных сетей

Возможности и функции каждого устройства связаны с уровнем модели OSI, на котором оно работает. Так, повторители функционируют на физическом уровне, передавая полученный аналоговый сигнал далее по сети (что позволяет избавиться от затухания в кабеле). Шлюзы, напротив, действуют на верхних уровнях модели OSI (на уровнях приложения и представления данных) и обеспечивают связь между системами, использующими различные протоколы (например, Ethernet и мини-ЭВМ IBM AS/400).

Повторители – довольно простые устройства, а шлюзам требуется аппаратное и программное обеспечение. Другие устройства межсетевого взаимодействия – мосты и маршрутизаторы – по сложности занимают промежуточное положение.

Повторители

В рамках данной главы под межсетевым взаимодействием подразумевается расширение, сегментация и объединение локальных сетей с помощью устройств и протоколов локальных и глобальных сетей. Следовательно, устройствами межсетевого взаимодействия будут считаться не только маршрутизаторы и шлюзы, но также повторители, мосты и коммутаторы.

При обсуждении различных устройств межсетевого взаимодействия наиболее часто будет рассматриваться архитектура Ethernet, поскольку она является самой распространенной, и многие сетевые устройства разработаны именно для сетей Ethernet. Информацию о сетях Token Ring и других технологиях, относящихся к аппаратному обеспечению IBM, можно найти на страницах технической поддержки IBM по адресу http://www.networking.ibm.com/nethard.html. Эти сведения представлены в форматах HTML и PDF и способны послужить бесплатным ресурсом для сетевых администраторов. Основы FDDI хорошо изложены на странице http://www.data.com/tutorials/boring_facts_about_fddi.html. Еще один источник статей о сетях расположен по адресу www.cmpnet.com/. Здесь содержатся ссылки на различные сайты, предлагающие информацию о технологиях локальных и глобальных сетей.

Поскольку в межсетевом взаимодействии используются протоколы локальных и глобальных сетей, то имеет смысл вернуться к главам 1 и 3, если восприятие настоящей главы окажется затруднительным.

Повторители, или *репитеры* (repeaters), принимают сигнал от устройств, включенных в сеть, и воспроизводят его, благодаря чему сигнал распространяется дальше, чем по отдельному отрезку кабеля. Поскольку все виды физической среды (медные и волоконно-оптические кабели, а также беспроводные системы связи) характеризуются затуханием, ограничивающим максимальное допустимое расстояние передачи, повторители позволяют значительно расширить сеть.

Повторители являются устройствами физического уровня, поэтому они не обрабатывают полученные кадры и не занимаются их логической и физической адресацией. Таким образом, они практически не снижают скорости передачи данных, а только очищают и усиливают сигнал, полученный от одного сегмента сети, и посылают его в другой сегмент (рис. 4.2).

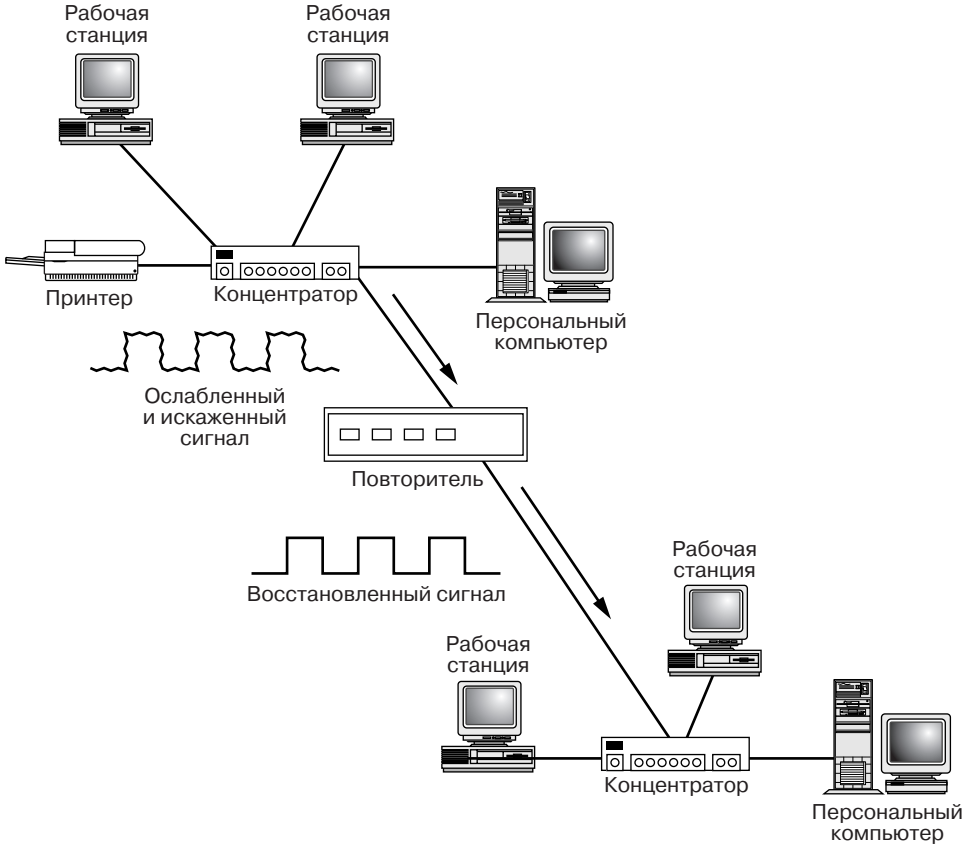


Рис. 4.2. Повторители восстанавливают полученный ослабленный сигнал и передают его в следующий сегмент сети

Повторители часто называют концентраторами, а концентраторы с функцией усиления сигнала – активными концентраторами или многопортовыми повторителями. Все эти устройства работают на физическом уровне модели OSI.

Мосты

Мосты (bridges) принадлежат к числу устройств канального уровня модели OSI и, следовательно, обладают большими возможностями, чем устройства физического уровня, такие как повторители и концентраторы. Мосты применяются для сегментации сетей, в которых из-за напряженного трафика снижается общая скорость передачи данных.

Мосты содержат специальное аппаратное обеспечение и операционную систему. Они обрабатывают MAC-адреса (то есть аппаратные адреса, жестко заданные в сетевом адаптере каждого компьютера) поступающих кадров. На основе информации о том, какие MAC-адреса относятся к тому или иному сегменту сети, мосты сортируют полученные кадры. Локальный трафик (относящийся к исходному сегменту) не проходит через данное устройство и не попадает в другие сегменты сети.

По существу, мосты обеспечивают сегментацию и способствуют сохранению высокой пропускной способности в крупной гомогенной сети (то есть в сети, построенной на принципах единой архитектуры). На рис. 4.3 изображено разделение сети с помощью моста на три отдельных сегмента.

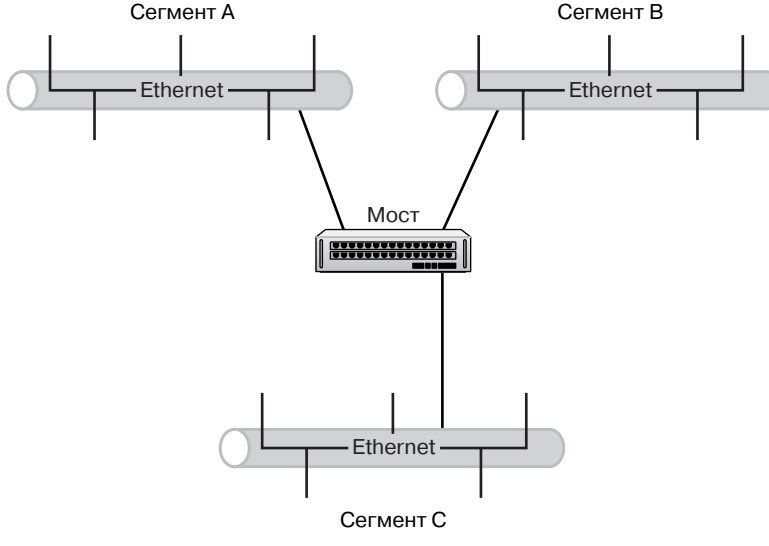


Рис. 4.3. Мосты отделяют локальный трафик от глобального

Допустим, компьютер в сегменте A передает данные другому компьютеру в этом же сегменте. Мост обрабатывает полученные кадры, выявляя аппаратные адреса отправителя и получателя, затем определяет, что информация должна остаться в сегменте A, и не ретранслирует ее в другие сегменты. Следовательно, пропускная способность незадействованных сегментов сохраняется высокой: их линии не загромождаются лишними данными.

Если компьютер из сегмента A отправляет сообщение компьютеру в сегменте C, то мост, изучив MAC-адреса кадров, передаст их именно в сегмент C. В сегмент B данные не попадут.

Может показаться, что мосты прекрасно справляются с задачей максимизации общей производительности сети. Однако они обладают рядом недостатков: направляют широковещательные пакеты (например, пакеты системы NetBIOS) всем узлам сети, а при невозможности определить принадлежность MAC-адреса тому или иному сегменту сети, пошлют такие кадры во все сегменты.

В сетях Ethernet применяются так называемые прозрачные мосты, которые при передаче или игнорировании поступающих кадров руководствуются специальной таблицей. Мост анализирует получаемые кадры и строит таблицу соответствия адресов и сегментов сети, которой пользуется в дальнейшем.

В сетях Token Ring имеются специальные мосты, фиксирующие кадры, которые содержат информацию о пути их следования. Мосту остается только выполнять полученные указания и направлять кадры в нужный сегмент.

Коммутаторы

Еще одно межсетевое устройство канального уровня, позволяющее сохранить пропускную способность сети за счет сегментации, – это *коммутатор* (switch). Коммутаторы, как и мосты, посылают кадры в соответствующие сегменты посредством аппаратной адресации, но поскольку они построены с использованием специального аппаратного оборудования, передача информации производится здесь значительно быстрее.

Коммутаторы различаются по способу передачи кадров. Существуют коммутаторы с буферизацией кадров и со сквозной передачей (без буферизации).

Коммутаторы с буферизацией кадров (store-and-forward) полностью обрабатывают кадры, в том числе проверяют контрольную циклическую сумму и определяют адрес назначения кадра. На все это время кадр записывается в буфер. При такой коммутации значительно уменьшается количество поврежденных кадров, переправленных коммутатором, но снижается и скорость передачи.

Коммутаторы без буферизации кадров (cut-through) функционируют быстрее, поскольку при обработке поступившего на коммутатор кадра считывается только MAC-адрес получателя.

Маршрутизаторы

Маршрутизаторы (routers) работают на сетевом уровне модели OSI. Они предназначены для соединения сетей и нуждаются в аппаратном и программном обес-

печении (маршрутизаторы Cisco функционируют с операционной системой Cisco IOS). Маршрутизаторы могут связывать различные сети: Ethernet, Token Ring, FDDI – для этого необходим только соответствующий интерфейс.

Будучи устройствами сетевого уровня модели OSI, маршрутизаторы пользуются логической адресацией для передачи кадров между различными сетями. Они разделяют корпоративную сеть на логические подсети, за пределы которых их локальный трафик не выходит. Благодаря тому, что маршрутизаторы не посылают широковещательные пакеты по всем направлениям, широковещательные штормы не оказывают влияния на все узлы.

> *Мосты пересылают широковещательные пакеты, которые действительно в состоянии «заполонить» сеть, так что в этом случае защиты от широковещательных штормов нет. Неисправные сетевые карты и другие устройства могут производить большое количество широковещательных пакетов, что приводит к широковещательным штормам, распространяющимся на всю сеть.*

➢ Поскольку данная книга посвящена маршрутизаторам и маршрутизации (в особенности маршрутизаторам Cisco и операционной системе Cisco IOS), подробности работы этих устройств и соответствующие протоколы будут рассмотрены в главе 5.

Шлюзы

Шлюзы (gateways) используются для соединения сетей с различными сетевыми протоколами, то есть там, где необходимо выполнять преобразование протоколов между несовместимыми сетями. Например, посредством шлюза можно связать мини-ЭВМ IBM AS400 с локальной сетью персональных компьютеров.

Шлюзы работают на верхних уровнях модели OSI: транспортном, сеансовом, уровне представления данных и уровне приложения. Как правило, шлюзом служит компьютер, снабженный специальным программным обеспечением, которое преобразует данные из формата одной сети в формат другой. В примере с IBM AS400 и локальной сетью ПК шлюз должен быть оборудован операционной системой Windows NT Server и специальным программным обеспечением для трансформирования данных.

Обычно шлюзы устанавливаются на таких высокоскоростных магистралях, как сети FDDI, для соединения больших ЭВМ и мини-ЭВМ с локальными сетями, подключенными к магистрали FDDI через маршрутизаторы (рис. 4.4). Хотя шлюзы необходимы для связи сетей, требующих преобразования данных, они могут снижать скорость передачи (в особенности при пересылке данных в объединенных сетях). Поскольку шлюзы соединяют различные системы, их конфигурирование бывает относительно более сложным, чем у других сетевых устройств (именно *относительно*: не стоит говорить человеку, конфигурирующему маршрутизаторы, что шлюз настроить труднее).

Шлюзы часто выполняют функции трансляторов различных стандартов электронной почты. Примером может служить шлюз, преобразующий данные из формата Lotus Notes Mail Server в формат Microsoft Exchange Server.

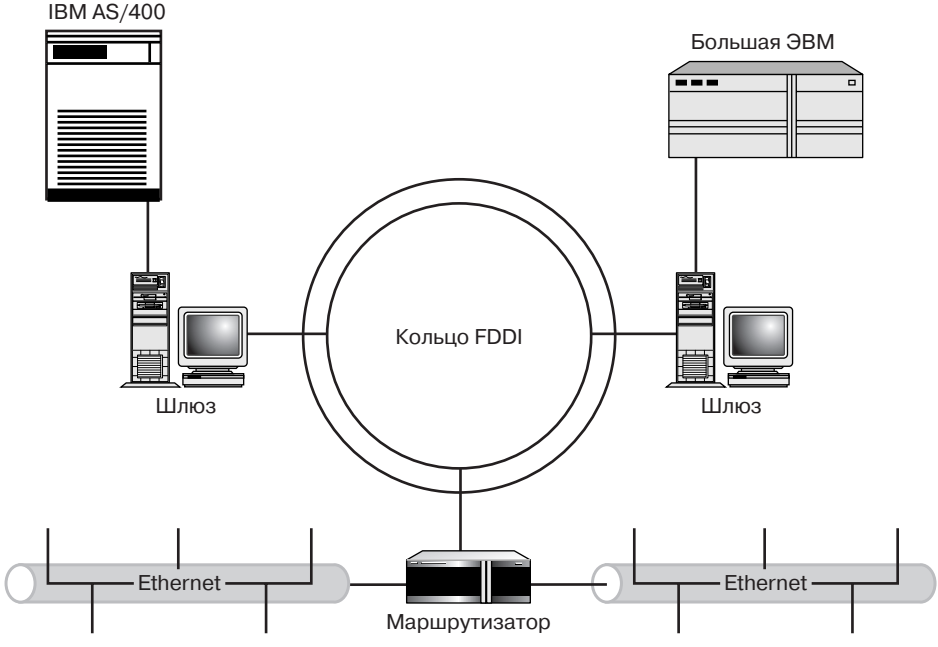


Рис. 4.4. Шлюзы обеспечивают соединение высокоскоростных магистралей с большими и малыми ЭВМ

Создание кампусной сети

Прежде чем закончить обсуждение проблем межсетевого взаимодействия, нужно сказать несколько слов о масштабе сети. Кампусная сеть определяется как часть корпоративной. Обычно кампусные сети ограничены одним или несколькими зданиями и в основном имеют архитектуру локальной сети: Ethernet, Token Ring или FDDI.

Чтобы создать сеть размером со студенческий городок и поддерживать ее функционирование, необходимо соединять различные сетевые архитектуры с помощью маршрутизаторов и применять устройства межсетевого взаимодействия (например, коммутаторы и мосты), защищающие от появления «узких мест» в сети.

Формирование корпоративной сети – объединение нескольких кампусных – требует использования технологий глобальных сетей, в которых также обязательны устройства межсетевого взаимодействия, в особенности маршрутизаторы с соответствующим интерфейсом.

В следующей главе мы рассмотрим принципы работы маршрутизатора. Это поможет понять, как локальные сети становятся глобальными и почему построение корпоративной сети теоретически не является сложным.

При настройке компьютера в сети (особенно в сети TCP/IP) вы должны сконфигурировать шлюз по умолчанию для своего узла. Шлюз по умолчанию – это, как правило, логический адрес порта маршрутизатора, к которому подключается данный узел и вся подсеть. Не нужно путать интерфейсы маршрутизатора (называемые шлюзами) с настоящими шлюзами, преобразующими данные из одного формата в другой.

ГЛАВА 5

Принципы работы маршрутизатора

Для передачи информации из одной сети в другую предназначен маршрутизатор (вы уже познакомились с этим устройством в главе 4). Чтобы выполнить маршрутизацию данных в межсетевом пространстве, следует определить подходящий путь передачи кадров и переслать кадры к пункту назначения.

И определение маршрута, и отправка по нему данных (ее еще называют коммутацией, поскольку кадры коммутируются с входного интерфейса маршрутизатора на выходной) осуществляются на сетевом уровне модели OSI. Другим важным событием, происходящим на этом уровне, является преобразование логических адресов (таких, как IP-адреса в случае протокола TCP/IP) в аппаратные физические адреса. Рассмотрим названные события подробнее.

Основы маршрутизации

Как было отмечено в главе 4, маршрутизаторы позволяют разделить большую сеть на логические подсети. Таким образом, локальный трафик каждой подсети остается в ее пределах, и общая пропускная способность не уменьшается. Передачу данных между подсетями осуществляют маршрутизаторы. Они также служат связующим звеном между вашей и другими сетями, при этом для всех узлов сеть будет представляться единой, или, как говорят, прозрачной, хотя она разделена на части. Лучшим примером объединения различных сетей в единую крупную сеть является Internet.

➢ Прежде чем продолжить изучение материала данной главы, вернитесь к описанию модели OSI (глава 2).

Для установки маршрутизатора сеть необходимо разбить на подсети. Пока можно считать, что подсети являются логическими разделами большой корпоративной сети. Создание подсетей в среде TCP/IP будет подробно описано в главе 10.

Определение маршрута

Рассмотрим гипотетическую сеть с разбиением на подсети, соединенные маршрутизатором, и создадим логическую адресную систему.

На рис. 5.1 изображена сеть, разделенная на две подсети с помощью маршрутизатора. Не будем пока обращать внимание на архитектуру подсетей (Ethernet, Token Ring и т.д.), приняв, что подсети соединяются с маршрутизатором посредством соответствующих протоколов и интерфейсов.

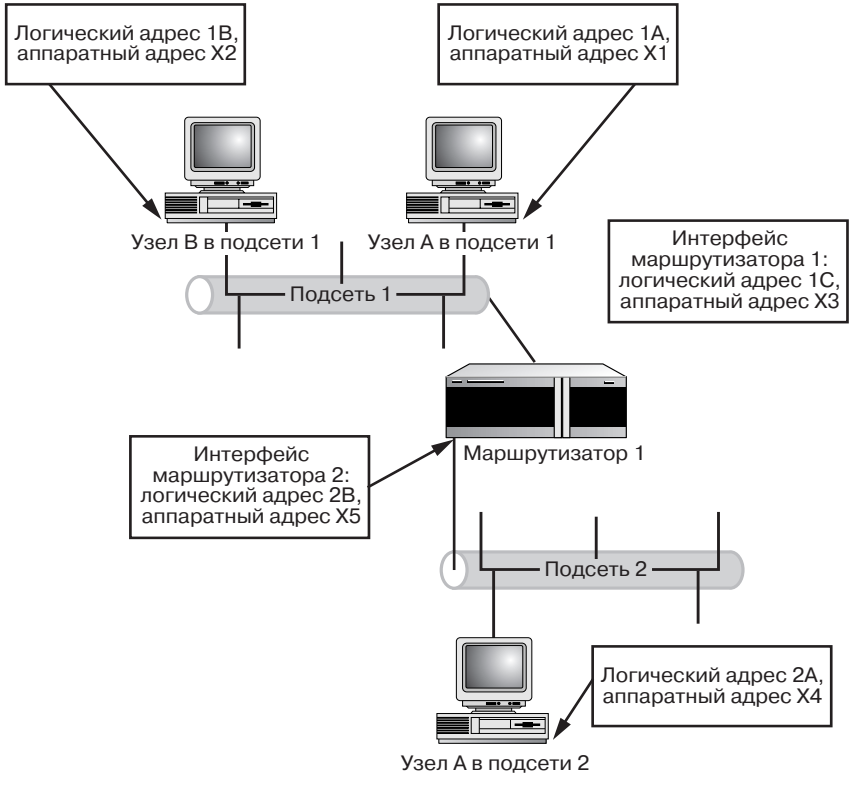


Рис. 5.1. Сеть с разделением на две логические подсети

В этом примере у маршрутизатора есть два интерфейса: 1 и 2. К ним присоединены подсеть 1 и подсеть 2 соответственно. Логическим адресом в данном случае является номер подсети и буквенное обозначение (интерфейсы маршрутизатора также имеют логические адреса). Так, логический адрес узла A подсети 1 – 1A.

Каждый узел характеризуется также аппаратным адресом (он жестко задан в любом сетевом адаптере заводом-изготовителем; интерфейсы маршрутизатора

тоже имеют аппаратные адреса). Для простоты обсуждения будем обозначать аппаратные адреса буквой «X» и цифрой. Например, аппаратный адрес узла A подсети 1 выглядит так: X4.

Посмотрим теперь, что произойдет в нашей небольшой интерсети, когда один из компьютеров соберется отправить данные другому.

Следует иметь в виду, что логические адреса, принятые в нашей книге, не являются настоящими. В реальных сетях используются истинные логические адреса (в частности, IP-адреса). В качестве примера реальных адресов приведем список IP-адресов класса B для узлов и интерфейсов сети:
Подсеть 1: 130.10.16.0
Узел A: 130.10.16.2
Узел B: 130.10.16.3
Интерфейс маршрутизатора 1: 130.10.16.1
Подсеть 2: 130.10.32.0
Узел A: 130.10.32.2
Интерфейс маршрутизатора 2: 130.10.32.1
Обратите внимание, что в адресах узлов и интерфейсов подсети 1 в третьем октете стоит 16, а в случае подсети 2 – 32. Именно эти числа и отличают одну подсеть от другой (см. также главу 10).

Логические и аппаратные адреса

Когда несколько сетей объединяются при помощи маршрутизатора, возникает два вида трафика. Информация, передаваемая в пределах одной подсети, составляет локальный трафик. А если связь осуществляется между узлами из разных подсетей, то трафик проходит через маршрутизаторы. В двух следующих разделах будет рассказано, как реализуется связь в пределах одной подсети и между подсетями.

Связь в пределах подсети

Рассмотрим случай, когда данные передаются между двумя компьютерами одной подсети. Требуется, чтобы узел A подсети 1 направил сообщение узлу B подсети 1. Узлу A известно, что пакеты данных следует доставить по логическому адресу 1B, который находится в той же подсети. В этих условиях маршрутизатор не будет активно задействован при пересылке информации. Тем не менее логический адрес 1B должен быть разрешен в аппаратный адрес узла. Разрешение адреса означает, что на основе информации о логическом адресе получателя (в нашем случае это 1B) узел-отправитель (узел A) должен получить данные об аппаратном адресе узла-получателя (узел B).

Допустим, узел А получил информацию о том, что логический адрес 1В узла В соответствует аппаратному адресу Х2. Компьютеры хранят сведения такого рода в небольшой кэш-памяти. Если узлу А неизвестен аппаратный адрес узла 1В, он пошлет в сеть запрос о преобразовании логического адреса 1В в аппаратный адрес и, получив эту информацию, сможет отправить данные узлу В, который их примет, поскольку они помечены его аппаратным адресом – Х2. Как видите, связь между узлами одной сети осуществляется непосредственно, без участия маршрутизатора.

Связь между подсетями

Рассмотрим теперь, как происходит передача данных из одной подсети в другую.

Узел А подсети 1 собирается переслать данные узлу А подсети 2. Иными словами, он отправит данные по логическому адресу 2А. Зная, что адрес 2А относится к другой подсети, узел А подсети 1 отошлет данные на *шлюз по умолчанию* (default gateway), то есть на интерфейс маршрутизатора, соединенный с подсетью 1. В данном случае логический адрес этого интерфейса – 1С. Его надо разрешить в MAC-адрес – реальный аппаратный адрес интерфейса маршрутизатора 1.

В ответ на широковещательный запрос узел А подсети 1 получает информацию об аппаратном адресе Х3, относящемся к логическому адресу 1С, и посылает данные на интерфейс маршрутизатора 1. Приняв пакеты, маршрутизатор должен определить, как перенаправить их узлу назначения. Для этого он обращается к таблице маршрутизации и коммутирует пакеты на интерфейс, подсоединенный к той подсети, где находится узел назначения.

> *Компьютеры используют свои широковещательные запросы (а также широковещательные запросы других компьютеров) для того, чтобы определить, какие адреса являются локальными, а какие находятся в другой сети.*

Коммутация пакетов

После того как маршрутизатор получил пакеты данных, происходит их коммутация: маршрутизатор перенаправляет данные с того интерфейса, куда они поступили, на интерфейс, с которого они будут посланы в другую подсеть. Однако бывают случаи, когда пакеты проходят через несколько маршрутизаторов, прежде чем достигнут узла назначения. В нашем примере действует только один маршрутизатор. Маршрутизатор 1 знает, что логический адрес 2А принадлежит подсети 2. Поэтому пакеты будут переключены с интерфейса 1 на интерфейс 2.

Как и прежде, для разрешения логического адреса 2А конечного адресата в реальный аппаратный адрес Х4 используются широковещательные запросы. Пакеты данных снабжаются соответствующим аппаратным адресом получателя и отправляются в подсеть 2. Когда узел А подсети 2 отслеживает пакеты с аппаратным адресом Х4, он принимает их.

Таким образом, при маршрутизации применяются как логические, так и аппаратные адреса. Каждый маршрутизируемый протокол преобразовывает логические адреса в аппаратные по своей схеме, хотя теоретически все они действуют одинаково.

Таблицы маршрутизации

Расскажем теперь, как маршрутизатор определяет, на какой порт переключить полученные пакеты (этого вопроса мы коснемся еще раз при рассмотрении маршрутизации IP в главе 11). Для создания таблиц маршрутизации предназначено специальное программное обеспечение. Таблицы маршрутизации содержат сведения о том, на каком интерфейсе начинается маршрут, который в конечном счете приведет к пункту назначения.

При построении таблиц маршрутизаторы не учитывают адреса узлов, им нужно только доставить тот или иной набор кадров в соответствующую сеть. Например, таблица маршрутизации в случае сети, изображенной на рис. 5.1, будет иметь вид, представленный в табл. 5.1. Обратите внимание на то, что каждый интерфейс маршрутизатора относится к той или иной подсети. Поэтому маршрутизатор, изучив логические адреса кадров, может определить, в какую подсеть их перенаправить.

Таблица 5.1. Базовая таблица маршрутизации для маршрутизатора 1

Логическое обозначение подсети	Интерфейс маршрутизатора
1	1
2	2

По существу, таблица маршрутизации указывает, что пакеты, адресованные какому-либо узлу подсети 1, должны направляться на интерфейс маршрутизатора 1. Пакеты, посланные узлу подсети 2, коммутируются на интерфейс 2. Конечно, в реальной сети логическое обозначение подсети будет неким IP-адресом (например, 129.10.1.0 относится к подсети IP класса B).

Интерфейс маршрутизатора обозначается типом поддерживаемой архитектуры (E0 в случае основного интерфейса Ethernet, S0 – для основного последовательного интерфейса маршрутизатора).

В больших сетях, где применяются несколько маршрутизаторов, таблицы маршрутизации содержат больше информации. Разобьем, например, нашу сеть (с одним маршрутизатором и двумя подсетями) на пять подсетей с двумя маршрутизаторами (рис. 5.2). Казалось бы, здесь только четыре подсети. Но в действительности всякое последовательное соединение между двумя маршрутизаторами также является подсетью и должно иметь собственный логический адрес.

В новой, расширенной сети у маршрутизатора 1 будет совершенно другая таблица маршрутизации. Теперь ему придется пересылать пакеты в подсети 4 и 5. Однако, как отмечалось выше, маршрутизатор не обеспечивает доставку данных непосредственно узлам назначения. Он только направляет их по пути, ведущему в соответствующую подсеть.

Табл. 5.2 представляет собой таблицу маршрутизации для маршрутизатора 1, основанную на системе адресов из нашего примера. Обратите внимание на то,

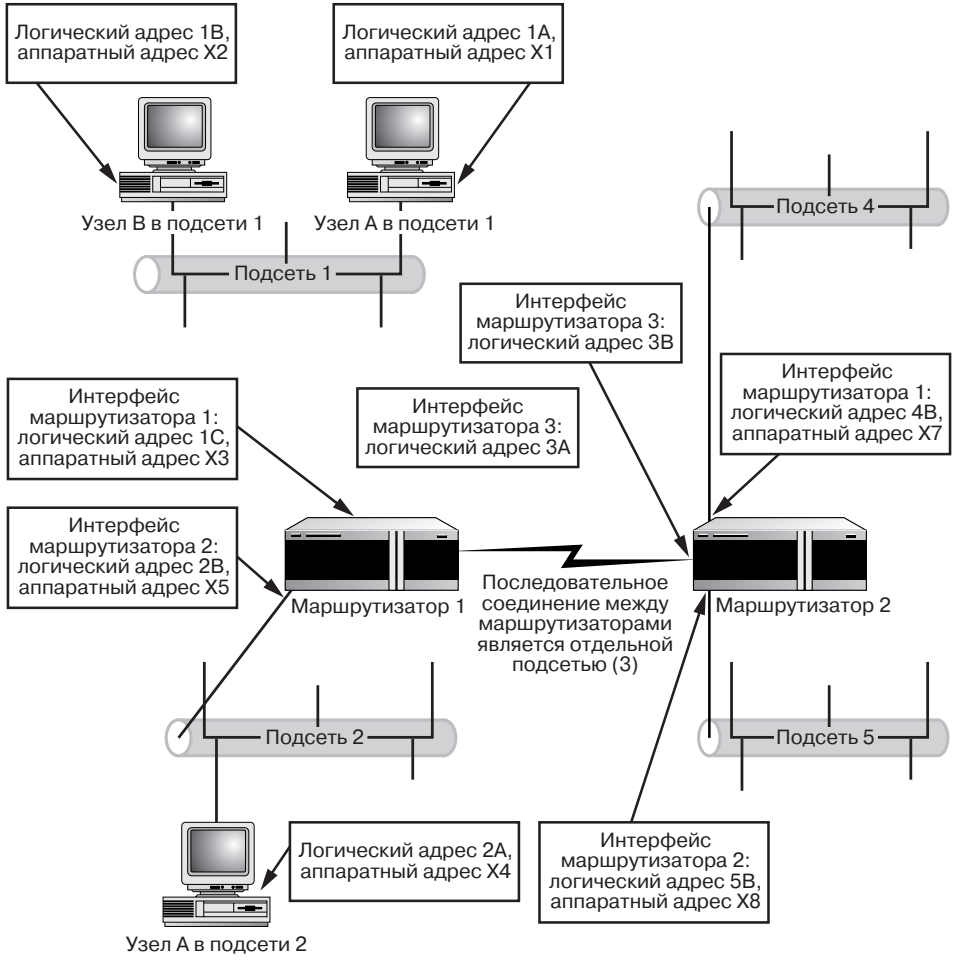


Рис. 5.2. Сеть, разделенная на пять логических подсетей с двумя маршрутизаторами

что маршрутизатор 1 пересылает пакеты в подсети 4 и 5 через один и тот же интерфейс 3. Иными словами, маршрутизатору 1 достаточно отправить эти пакеты маршрутизатору 2: за дальнейшую передачу данных в ту или иную подсеть, подключенную к соответствующему интерфейсу, будет отвечать он.

Таблица 5.2. Расширенная таблица маршрутизации для маршрутизатора 1

Логическое обозначение подсети	Интерфейс маршрутизатора
1	1
2	2
4	3
5	3

Похожую таблицу маршрутизации имеет маршрутизатор 2. В ней указывается, что все пакеты, адресованные в подсети 1 и 2, должны переправляться через интерфейс 3 на маршрутизатор 1. Отправкой данных в конечные подсети займется маршрутизатор 1.

Для выработки всех этих решений предусмотрено программное обеспечение, отвечающее за передачу информации по сети (это сетевые, или *маршрутизируемые*, стеки протоколов, в частности TCP/IP, IPX/SPX, AppleTalk) и позволяющее маршрутизатору выбрать наилучший путь для пересылки пакетов. Такое программное обеспечение носит название *маршрутизирующего протокола* (routing protocol). В следующих двух разделах будут рассмотрены маршрутизируемые и маршрутизирующие протоколы (иначе называемые *протоколами маршрутизации*).

Таблицы маршрутизации могут создаваться двумя способами. При статической маршрутизации сетевой администратор сам вводит информацию о возможных путях между сегментами сети. С помощью некоторых команд маршрутизатора можно построить таблицу, подобную табл. 5.1. Другой способ формирования таблиц – динамический. В этом случае ими занимаются такие протоколы маршрутизации, как RIP и IGRP (они описаны ниже). Динамические таблицы маршрутизации в конечном итоге по виду также напоминают табл. 5.1.

➢ Подробнее о маршрутизации IP и таблицах маршрутизации рассказывается в главе 11.

Маршрутизируемые протоколы

Прежде чем приступить к рассмотрению протоколов, определяющих путь для маршрутизируемых пакетов и обслуживающих таблицу маршрутизации, следует сказать несколько слов о маршрутизируемых протоколах (routable, routed protocol). В главе 2 обсуждались распространенные сетевые протоколы: TCP/IP, IPX/SPX, AppleTalk и NetBEUI. Из этих четырех протоколов маршрутизируемы только первые три, поскольку в заголовки сетевого уровня они вносят информацию, позволяющую пересылать пакеты данных от отправителя к получателю, даже если пакеты передаются через различные сети.

Протокол NetBEUI также выполняет адресацию кадров. Он применяет имена NetBIOS (данные компьютеру пользователем при настройке), которые затем, после серии широковещательных запросов системы NetBIOS, преобразуются в MAC-адреса. К сожалению, система именования NetBIOS не включает в себя систему логической адресации сетевого уровня. Имена NetBIOS не предоставляют достаточной информации (а точнее, вообще не содержат никаких сетевых данных) для передачи кадров из одной сети в другую. К тому же в теке протоколов NetBEUI/NetBIOS нет протокола маршрутизации.

➢ Чтобы вернуться к описанию сетевых протоколов (например, TCP/IP), откройте главу 2, раздел «Реальные сетевые протоколы».

Протоколы маршрутизации

Если маршрутизируемые протоколы обеспечивают логическую адресацию, благодаря которой маршрутизация становится возможной, то протоколы маршрутизации обслуживают таблицы маршрутизации. Эти протоколы позволяют маршрутизаторам устанавливать связь между собой и обмениваться информацией, необходимой для построения и обслуживания таких таблиц.

Существует несколько протоколов маршрутизации: RIP (Routing Information Protocol), OSPF (Open Shortest Path First) и EIGRP (Enhanced Interior Gateway Protocol). Несмотря на то что все они применяют различные методы определения наилучшего пути из одной сети в другую, цель у них одна – накопление информации, относящейся к тому или иному маршрутизируемому протоколу, например IP (IP – это маршрутизируемый компонент стека протоколов TCP/IP).

В локальных и глобальных сетях серверы и узлы зачастую работают с несколькими протоколами. Так, сервер NT в *домене NT* (домен NT – это сеть, управляемая NT-сервером, который называется *контроллером домена*) может посредством TCP/IP осуществлять коммуникацию со своими клиентами.

Но он также способен служить шлюзом для различных файловых серверов и серверов печати, функционирующих в старых системах Novell NetWare, следовательно, сервер NT применяет и стек IPX/SPX. Протоколы этих стеков действуют одновременно, не мешая друг другу (рис. 5.3).

Принцип одновременно и независимо исполняемых протоколов распространяется и на протоколы маршрутизации. На одном маршрутизаторе могут независимо работать несколько протоколов маршрутизации, создающих и обновляющих таблицы маршрутизации для разных маршрутизируемых протоколов. Таким образом, одна и та же сетевая среда в состоянии поддерживать различные виды сетевого взаимодействия.

➢ Подробнее о различных протоколах маршрутизации рассказывается в главе 5, раздел «Типы протоколов маршрутизации».

Основы протоколов маршрутизации

Протоколы маршрутизации должны не только предоставлять информацию для таблиц маршрутизации и обновлять их соответствующим образом при изменении структуры путей, но и определять наилучший путь передачи данных от одного компьютера к другому. Поскольку эти протоколы создаются для оптимизации маршрутов, необходимо, чтобы они были устойчивыми и гибкими.

Протоколам маршрутизации не требуется больших вычислительных ресурсов для обработки информации о маршрутах. Иными словами, маршрутизатор не

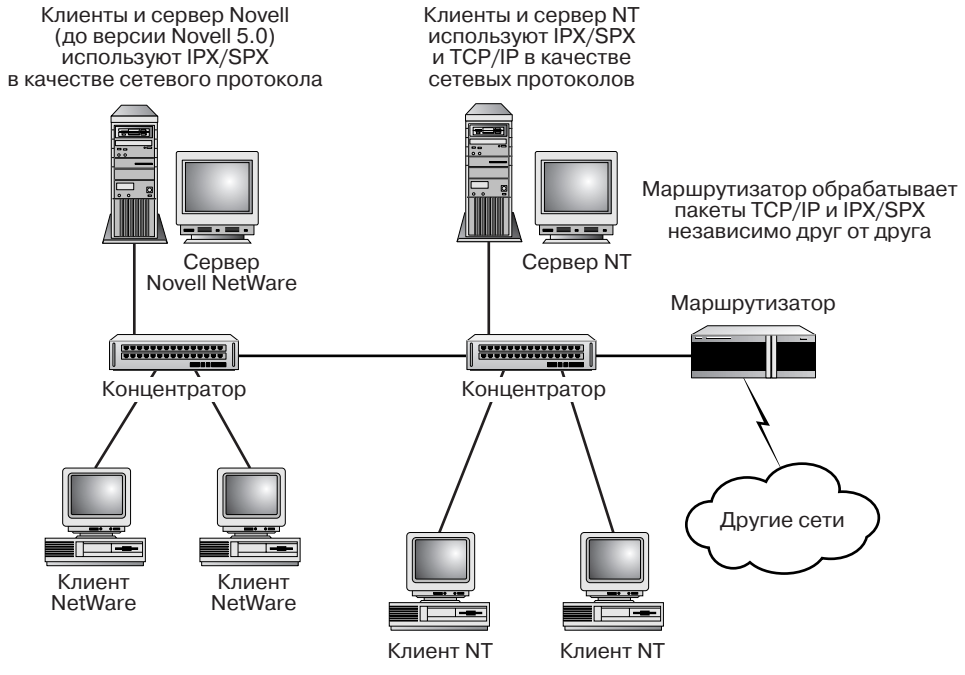


Рис. 5.3. Сети могут использовать несколько протоколов, а маршрутизаторы – одновременно маршрутизировать несколько сетевых протоколов с помощью различных протоколов маршрутизации

должен быть мощным компьютером с несколькими процессорами. В следующем разделе мы рассмотрим механизм определения наилучшего пути.

Хотя здесь рассматриваются теоретические аспекты работы маршрутизатора и взаимосвязи между маршрутизируемыми протоколами и протоколами маршрутизации, следует иметь в виду, что именно с этими вопросами вы столкнетесь при конфигурировании маршрутизатора. Операционная система Cisco IOS предоставляет команды и функции, позволяющие настроить необходимые протоколы на данном маршрутизаторе. Подробнее о Cisco IOS говорится в главе 9.

Алгоритмы маршрутизации

Алгоритм – это математическая процедура, позволяющая прийти к искомому решению. В случае маршрутизации алгоритм можно представить как набор правил, которыми протокол маршрутизации руководствуется при выборе того или иного пути. Такие алгоритмы применяются для построения таблиц маршрутизации.

Существует два вида алгоритмов маршрутизации: статические и динамические. *Статический алгоритм* не является процедурой, а содержит информацию соответствия, внесенную в таблицу маршрутизации сетевым администратором. Эта таблица указывает, как нужно передавать данные от одного пункта к другому. Все пути в таком случае будут статическими, то есть неизменными.

Проблема со статическими алгоритмами (помимо того, что приходится вручную вводить информацию в несколько маршрутизаторов) заключается в том, что маршрутизатор не может сам приспосабливаться к изменениям топологии сети. Если какой-нибудь маршрут становится недоступным или перестает работать часть сети, маршрутизатор не сумеет обновить свою таблицу в соответствии с этими переменами.

Динамические алгоритмы создаются и обслуживаются сообщениями об обновлении маршрутов. Эти сообщения, несущие информацию об изменениях в сети, обращаются к программе, запрашивая пересчет алгоритма, и соответствующим образом обновляют таблицу маршрутизации.

Алгоритмы маршрутизации (и протоколы маршрутизации, применяющие тот или иной алгоритм), различаются также по способу доставки маршрутизаторам информации об обновлениях. *Алгоритм дистанционно-векторной маршрутизации* направляет сообщения об обновлении через определенные промежутки времени (например, через каждые 30 с, как это делает протокол RIP). Маршрутизатор, основанный на данном алгоритме, передает всю таблицу ближайшему соседу, соединенному с ним напрямую. Таким образом, реагирование на изменения в сети происходит по принципу домино.

Допустим, маршрутизатор 1 получает информацию, что связь с сетью A оборвалась (рис. 5.4). В своем сообщении об обновлениях, отправляемом каждые 30 с, он передает исправленную таблицу маршрутизатору 2, извещая его о том, что путь к сети A более недоступен. Маршрутизатор 2 соответственно посылает маршрутизатору 3 обновленную таблицу, где указывается, что маршрутизатор 2 уже не обслуживает путь к сети A. Процедура обновления продолжается до тех пор, пока все маршрутизаторы не будут проинформированы, что пути к сети A на этом участке теперь не существует.

> *На самом деле маршрутизаторы передают обновления всем своим соседям. Таким образом, маршрутизатор 2 отправит обновленную таблицу не только маршрутизатору 3, но и обратно маршрутизатору 1.*

Недостаток описанного способа состоит в том, что маршрутизаторы строят свои таблицы на основе непроверенной информации, не контролируя реальное состояние соединений. Им приходится полагаться только на сведения, полученные от других маршрутизаторов.

Другим способом обновления таблиц маршрутизации является *алгоритм маршрутизации с учетом состояния каналов*. Протоколы, действующие по этому

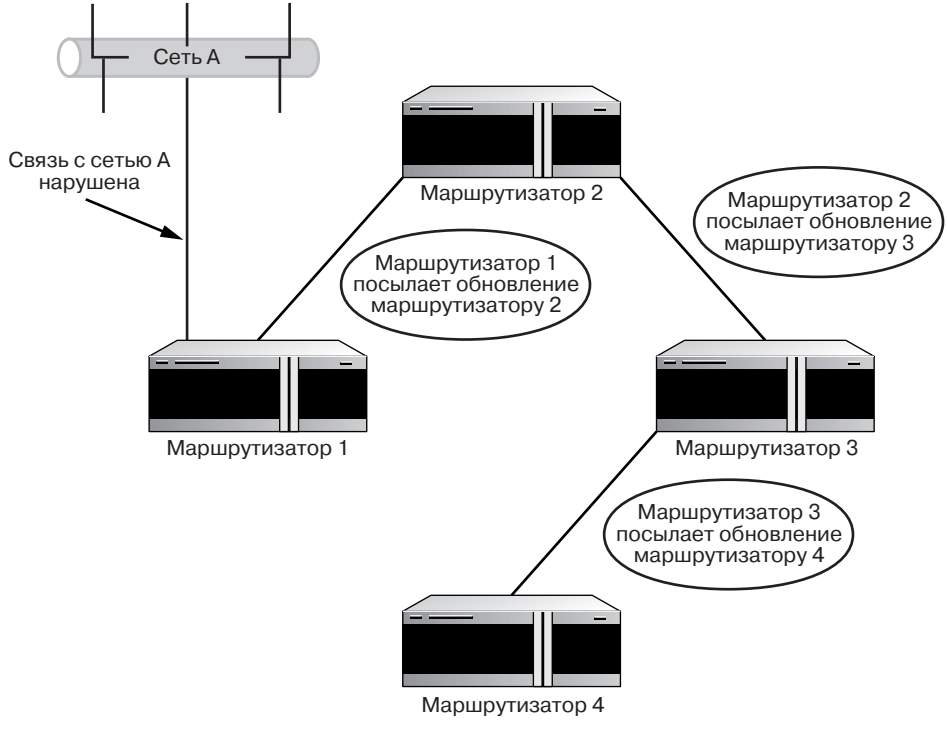


Рис. 5.4. При дистанционно-векторной маршрутизации обновленная таблица направляется ближайшему маршрутизатору

алгоритму, не только определяют ближайший маршрутизатор, но и обмениваются информацией о состоянии каналов со всеми маршрутизаторами. Таким образом, в отличие от дистанционно-векторного метода, передается не вся таблица, а только данные о непосредственных соединениях маршрутизатора.

Следовательно, маршрутизаторы, на которых работают протоколы с алгоритмом маршрутизации по состоянию каналов, способны создавать исчерпывающую картину всей сети и принимать более правильные решения при выборе путей.

Когда в сети обрывается связь или возникают другие неполадки, очень важно, чтобы таблицы маршрутизации были должным образом обновлены. Время, необходимое для обновления таблиц на всех маршрутизаторах, называется сходимостью. Чем дольше маршрутизаторы обновляют свои таблицы, тем выше вероятность, что пакеты данных будут направлены по нефункционирующим путям. Та же проблема имеет место и в Internet; именно поэтому электронные письма иногда попадают на тупиковый путь и не доходят до адресата.

Может показаться, что динамические алгоритмы гораздо лучше справляются с задачами маршрутизации. Однако динамическая маршрутизация требует дополнительных вычислительных затрат и пропускной способности для широковещательных сообщений и редактирования таблиц. Так что в некоторых случаях применение статических таблиц маршрутизации обеспечивает более быструю передачу данных.

Некоторые протоколы маршрутизации, например протокол с выбором кратчайшего маршрута, считаются гибридными, поскольку используют как дистанционно-векторный алгоритм, так и алгоритм маршрутизации с учетом состояния каналов.

Кроме того, эти алгоритмы учитывают состояние каналов и обеспечивают более быструю *сходимость*, чем алгоритмы дистанционно-векторной маршрутизации.

Метрика маршрутизации

Мы рассказали о различных видах алгоритмов маршрутизации (статических и динамических) и о способах обновления таблиц маршрутизации (дистанционно-векторном и с учетом состояния каналов), обсудим теперь, каким образом протоколы маршрутизации выбирают наилучший путь доставки данных из нескольких возможных.

Алгоритмы маршрутизации определяют преимущества одного маршрута перед другим с помощью метрики. Метрикой может служить длина пути, стоимость передачи данных по нему, надежность того или иного маршрута между отправляющим и получающим компьютерами.

Например, протокол RIP, основанный на дистанционно-векторном алгоритме, применяет в качестве метрики *счетчик переходов*. Переход – это передача данных от одного маршрутизатора к другому. Если существует несколько вероятных путей, протокол выберет тот, где наименьшее число переходов. На рис. 5.5 изображена сеть, в которой возможны два пути пересылки данных от отправляющего компьютера к принимающему. Поскольку маршрут А содержит только один переход, он и будет считаться оптимальным.

Протоколы, работающие только с одной метрикой (например, счетчик переходов), рассматривают проблему выбора наилучшего маршрута лишь с одной стороны. В частности, протокол RIP не учитывает скорость передачи и надежность линий. Из рис. 5.5 видно, что путь А, наилучший по количеству переходов, содержит медленную 56-килобитную выделенную линию, за пользование которой к тому же приходится платить. Путь В проходит по магистралям, принадлежащим компании, и является более быстрым (100 Мбит/с). Однако, поскольку учитывается только количество переходов, будет выбран маршрут А.

Большую гибкость при выборе оптимального маршрута обеспечивают протоколы маршрутизации, располагающие более развитой системой метрик. Например, протокол IGRP применяет от 1 до 255 метрик в зависимости от установок сетевого администратора. Этими метриками могут быть пропускная способность (емкость задействованных линий), нагрузка (количество трафика, управляемого тем или иным маршрутизатором), стоимость передачи. Когда несколько метрик учитываются одновременно, выбор пути не так очевиден. В примере, представленном на рис. 5.5, протокол маршрутизации, применяющий в качестве метрики стоимость передачи, выберет путь более дешевый, хотя и с большим количеством переходов.

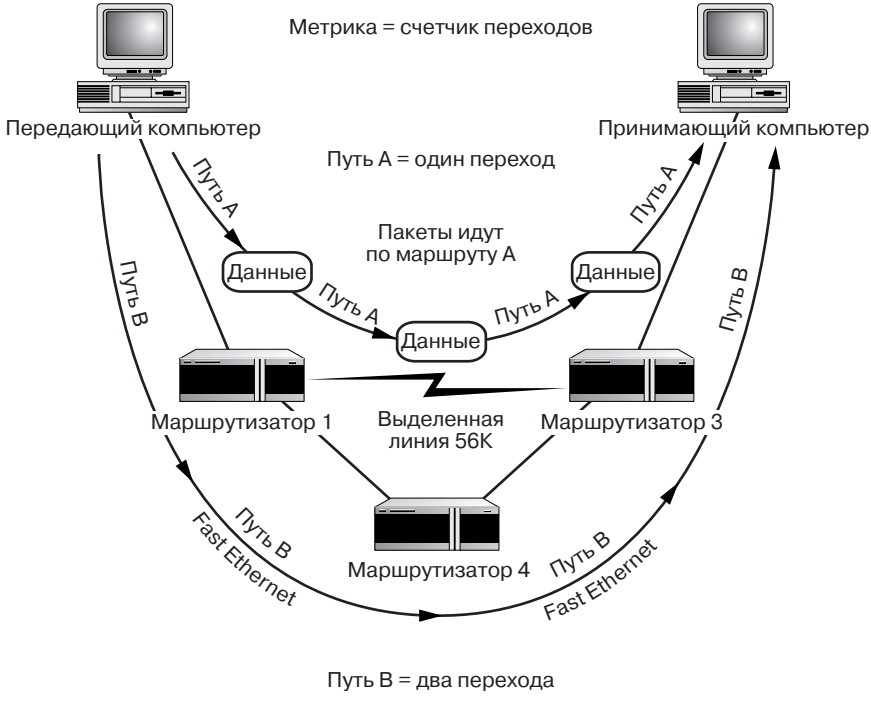


Рис. 5.5. Алгоритмы маршрутизации пользуются метрикой для определения оптимального пути

Типы протоколов маршрутизации

В реальных крупных сетях, в особенности корпоративных, устанавливается несколько маршрутизаторов. Для эффективной передачи данных маршрутизаторы нередко собирают в группу, называемую *областью* (area). Различные области,

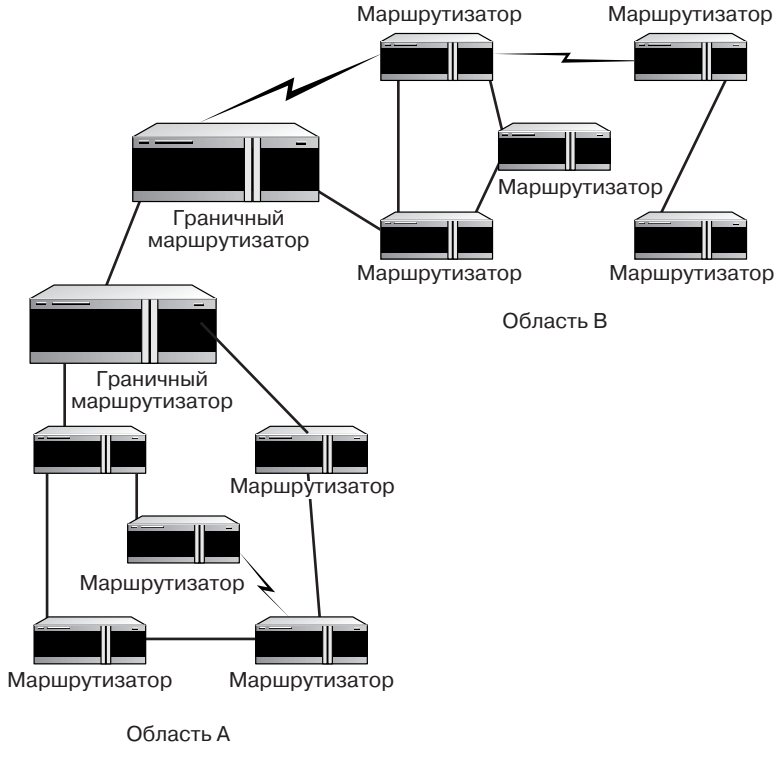


Рис. 5.6. Граничные маршрутизаторы соединяют различные автономные системы

объединенные в группу более высокого уровня, образуют *домен маршрутизации* (routing domain), который именуется также *автономной системой*.

На рис. 5.6 изображена сеть, разделенная на области. Каждая область заканчивается маршрутизатором высокого класса – *граничным*. Два граничных маршрутизатора, соединенные между собой, обеспечивают связь между доменами (или автономными системами в сети IP).

Поскольку интерсети можно разделять на логические группы (домены или автономные системы), существует два типа протоколов маршрутизации: одни обеспечивают маршрутизацию в пределах домена, другие – между доменами.

Протоколы внутренней маршрутизации (interior gateway protocols – IGP) относятся к первому типу. Такие протоколы, как RIP или *протокол внутренней маршрутизации между шлюзами* (interior gateway routing protocol – IGRP), конфигурируются на каждом маршрутизаторе в домене.

Протоколы внешней маршрутизации (exterior gateway protocols – EGP) отвечают за передачу данных между доменами, в качестве примера можно назвать *протокол граничной маршрутизации* (border gateway protocol – BGP).

Протоколы внутренней маршрутизации

Протоколы внутренней маршрутизации работают с дистанционно-векторными алгоритмами и алгоритмами маршрутизации с учетом состояния каналов. Существует несколько протоколов IGP, различающихся количеством метрик, с помощью которых определяется оптимальный путь. Самым первым протоколом внутренней маршрутизации был протокол RIP – он рассмотрен в следующем разделе наряду с другими распространенными протоколами IGP.

При использовании алгоритмов, учитывающих состояние каналов и требующих больших вычислительных затрат, сети нередко разбивают на домены маршрутизации, которые связываются между собой через граничные маршрутизаторы. В сетях IP такие домены называют автономными системами.

Сеть небольшой компании можно рассматривать как один домен, где применяются протоколы внутренней маршрутизации. Связь такой сети с Internet осуществляется посредством протокола внешней маршрутизации. Протоколам внутренней и внешней маршрутизации (IGP и EGP) посвящена оставшаяся часть данной главы.

Информационный протокол маршрутизации

В *информационном протоколе маршрутизации* (RIP), основанном на дистанционно-векторном алгоритме и предназначенном для маршрутизации IP, в качестве метрики используется счетчик переходов. Будучи самым старым протоколом IGP, он все еще находит применение.

RIP – это протокол маршрутизации IP. Сети IP логически подразделяются на подсети. Правильное разбиение и согласованное применение масок подсетей очень важно для работы RIP.

Протокол RIP передает обновления каждые 30 с (по умолчанию). Эти сообщения содержат полную таблицу маршрутизации. RIP функционирует с протоколом пользовательских датаграмм (user datagram protocol – UDP), входящим в стек TCP/IP, для инкапсуляции извещений об обновлении. Однако RIP ограничен максимально возможным количеством переходов: оно не должно превышать 15. Таким образом, этот протокол удобен для небольших однородных сетей, но не в состоянии обеспечить гибкий выбор оптимального маршрута в крупных сетях.

➢ Конфигурированию RIP на маршрутизаторе Cisco посвящен раздел «Конфигурирование протокола RIP» (глава 11).

Протокол IGRP

Протокол IGRP был разработан компанией Cisco в 80-х годах. Он основан на дистанционно-векторном алгоритме маршрутизации и применяет составную метрику, учитывающую несколько переменных. Кроме того, в отличие от RIP, IGRP не ограничивается маршрутами, содержащими максимум 15 переходов.

Протокол IGRP обновляет таблицы реже, чем RIP, и располагает более эффективным форматом кадра. Он поддерживает автономные системы, поэтому управляемые им маршрутизаторы можно помещать внутрь доменов, где весь трафик, приходящий на маршрутизатор, остается локальным. Таким образом снижается количество широковещательной информации, расходующей пропускную способность всей сети.

Метрика IGRP учитывает пропускную способность, задержку, степень загрузки и надежность линий следующим образом:

- *пропускная способность* – это емкость интерфейса, измеренная в килобитах. У последовательного интерфейса она может составлять 100000 Кбит (такой скоростью обладает последовательный интерфейс коммутатора ATM). К сожалению, пропускная способность измеряется не динамически, не в данный момент времени, а установлена администратором с помощью команды `bandwidth`. Подробнее о настройке последовательных интерфейсов рассказывается в главе 15;
- *задержка* – это промежуток времени, необходимый для доставки кадра от интерфейса до пункта назначения. Задержка измеряется в микросекундах и также является статической величиной, заданной администратором при помощи команды `delay`. Для некоторых распространенных интерфейсов, в частности Fast Ethernet и IBM Token Ring, такие временные интервалы уже рассчитаны. Например, задержка интерфейса Fast Ethernet составляет 100 мс;
- *надежность* – это отношение количества ожидаемых сообщений, подтверждающих активность, к действительно пришедшим на тот или иной интерфейс маршрутизатора. Этот параметр измеряется динамически и при выполнении команды `show interface` изображается в виде дроби. Например, дробь 255/255 означает стопроцентную надежность связи;
- *степень загрузки* – это текущий объем трафика на данном интерфейсе. Нагрузка измеряется динамически и также представляется в виде дроби. Например, дробь 1/255 означает интерфейс с минимальным количеством трафика, а 250/255 говорит о загруженном интерфейсе. Оценить данную величину позволяет команда `show interface`.

Итак, IGRP учитывает различную информацию при обновлении таблиц маршрутизации. Он часто применяется в крупных сетях, где протокол RIP был бы неэффективен.

Поскольку IGRP разработан компанией Cisco и является ее собственностью, он применяется только на маршрутизаторах Cisco. Протокол RIP более универсален, его можно использовать в сетях IP как с маршрутизаторами Cisco, так и с устройствами других производителей.

Cisco также предоставляет усовершенствованный IGRP (EIGRP), который, располагая теми же метриками, что и простой IGRP, уведомляет об изменениях не регулярно, а лишь тогда, когда они происходят. Для таких – более редких – сообщений выделяется меньшая доля общей пропускной способности.

Вы, вероятно, обратили внимание, что показатели надежности и нагрузки основаны на числе 255. Причина проста: хотя IGRP не работает со счетчиком переходов в качестве метрики, он может передавать данные в сетях с количеством переходов, не превышающим 255. Теоретически кадры разрешается пересылать через 255 устройств, поэтому данное число и фигурирует в оценке надежности и нагрузки.

➢ Подробнее о конфигурировании IGRP на маршрутизаторе Cisco рассказывается в главе 11, раздел «Конфигурирование протокола IGRP».

Протокол маршрутизации с выбором кратчайшего пути

Протокол маршрутизации с выбором кратчайшего пути (OSPF) применяет алгоритм, учитывающий состояние каналов. Он создан Рабочей группой инженеров Internet (Internet Engineering Task Force – IETF) в качестве альтернативы протоколу RIP. По существу, OSPF использует алгоритм предпочтения кратчайшего пути, позволяющий вычислить наиболее выгодный маршрут от источника к пункту назначения.

Протокол приветствия (Hello Protocol) служит здесь в качестве механизма идентификации соседних маршрутизаторов. Интервалы между кадрами приветствий можно сконфигурировать для каждого интерфейса, функционирующего с OSPF (по умолчанию этот промежуток составляет 10 с). Устанавливается значение интервала посредством команды `ip ospf hello-interval`.

Протокол OSPF подходит и для автономных систем, где локальные маршрутизационные сообщения не выходят в другие сети. Граничные маршрутизаторы соединяют автономные системы в одну сеть.

Протоколы внешней маршрутизации

Как упоминалось ранее, протоколы внешней маршрутизации (EGP) предназначены для передачи данных между автономными системами (доменами маршрутизации). *Протокол граничной маршрутизации* BGP широко используется как протокол междоменной маршрутизации. Это стандартный EGP для Internet.

BGP управляет маршрутизацией между несколькими граничными маршрутизаторами доменов. По существу, граничные маршрутизаторы разных доменов являются соседями и обмениваются таблицами маршрутизации друг с другом, что позволяет им создать список всех путей в ту или иную сеть.

BGP применяет единственную метрику для определения наилучшего пути. Каждому каналу администратором сети назначается число, определяющее степень предпочтительности этого канала.

ЧАСТЬ II

Устройство маршрутизатора и основная конфигурация

ГЛАВА 6

Интерфейсы маршрутизатора

Интерфейс маршрутизатора обеспечивает физическое соединение маршрутизатора с той или иной сетевой средой. Интерфейсы Cisco часто называют *портами*, причем каждый порт предназначен для подключения к среде определенного вида. Так, интерфейс локальной сети, например порт Ethernet, представляет собой розетку коннектора RJ-45, к которой с помощью витой пары подсоединяется концентратор Ethernet.

Интерфейсы маршрутизатора

Встроенные порты характеризуются типом соединения и номером. Например, первый порт Ethernet обозначается E0, второй – E1 и т.д. (В некоторых случаях интерфейсы Ethernet организованы в виде концентратора.) Последовательные порты обозначаются буквой «S» и цифрой: так, S0 – первый последовательный порт. На рис. 6.1 изображены два последовательных порта маршрутизатора Cisco 2505 и порты концентратора Ethernet (от первого до восьмого).

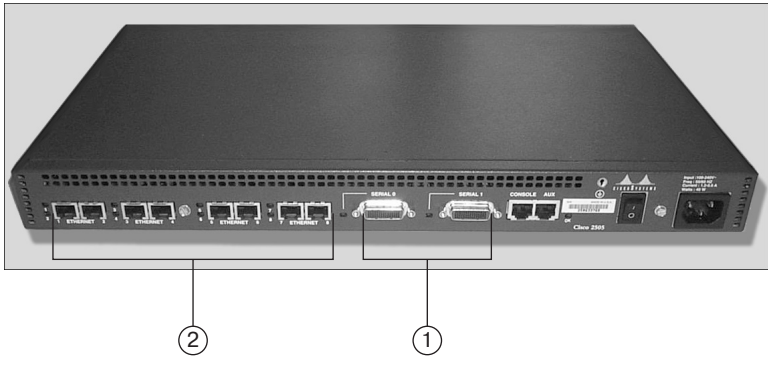


Рис. 6.1. Интерфейсы Ethernet могут представлять собой порты концентратора: 1 – последовательные порты; 2 – порты концентратора Ethernet

Маршрутизаторы Cisco серии 2500 выпускаются с определенным количеством портов для локального, глобального и последовательного соединений. Маршрутизаторы более высокого класса, такие как Cisco 4500, являются модульными, что дает возможность устанавливать в них карты различных интерфейсов. Более того, разрешается задавать количество портов на карте. Например, в один из трех свободных разъемов маршрутизатора 4500 допустимо вставить карту Ethernet с шестью портами. На рис. 6.2 показано окно конфигурации аппаратного обеспечения для маршрутизатора Cisco 4500 (с программой конфигурирования Cisco ConfigMaker вы познакомитесь в главе 16). Три свободных разъема, представленные в правой части окна, могут быть заполнены различными картами, перечисленными слева.

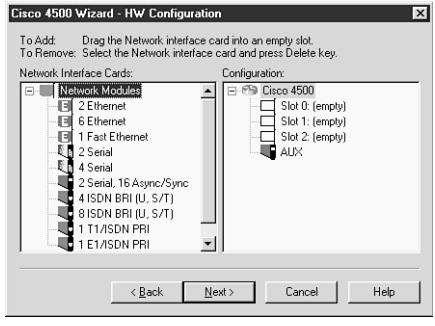


Рис. 6.2. В свободные разъемы модульных маршрутизаторов можно устанавливать карты различных интерфейсов

В модульных маршрутизаторах наименование порта включает в себя тип интерфейса, номер разъема и номер порта. Так, первый порт карты Ethernet, помещенной в первый разъем, обозначается как Ethernet 1/0 (номер разъема/номер порта).

Информация об интерфейсах и их статусе выводится с помощью команды `show interfaces`. На рис. 6.3 показан результат выполнения данной команды на маршрутизаторе 2505, имеющем один порт Ethernet (E0) и два последовательных порта (S0 и S1). Под статусом порта понимается его конфигурация и наличие физического подключения к сетевой среде.

Настройка интерфейса зависит от типа сетевого протокола той сети, которая подведена к данному порту. Например, порт Ethernet, подсоединенный к сети IP, будет сконфигурирован для маршрутизации IP. Если же в порт Ethernet включена сеть AppleTalk, он настраивается для маршрутизации AppleTalk.

➢ Конфигурирование интерфейсов описывается в главах 11–13. Подключение локальных и последовательных портов к сетевой среде рассматривается в разделе «Соединение маршрутизатора с сетью» (глава 7).

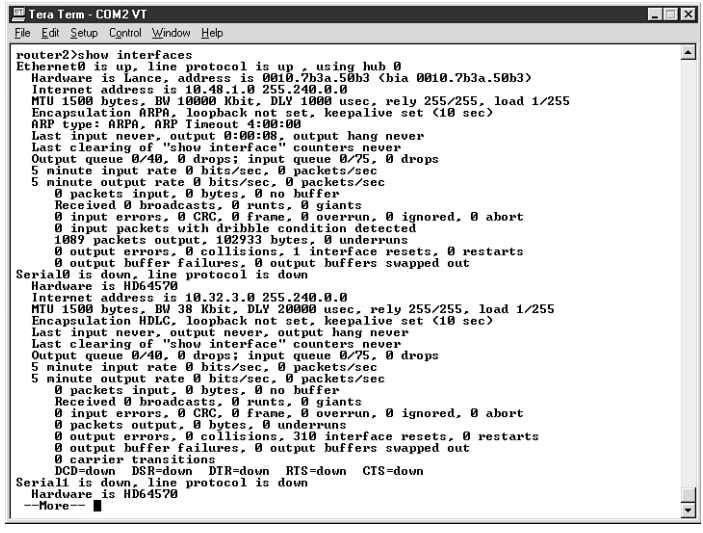


Рис. 6.3. Получение информации об интерфейсах маршрутизатора

Маршрутизаторы самого высокого на сегодняшний день класса (например, Cisco 12000) используют карты с процессором универсального интерфейса (versatile interface processor – VIP). Каждая VIP-карта имеет два разъема для интерфейсных карт. Маршрутизаторы этого типа изготавливаются для конкретной сети. В маршрутизаторах серии 12000 также имеются оперативно заменяемые интерфейсы, которые позволяют добавлять карты, не прерывая работу маршрутизатора и обслуживаемой им сети.

Интерфейсы локальных сетей

Маршрутизаторы Cisco поддерживают несколько распространенных типов локальных сетей. Наиболее часто применяются интерфейсы Ethernet, Fast Ethernet, IBM Token Ring, FDDI.

Все названные протоколы содержат одну и ту же систему физической адресации на канальном уровне (аппаратный адрес, жестко заданный в сетевой карте или контроллере интерфейса маршрутизатора). Каждое устройство имеет уникальный физический адрес.

Рассмотрим основы технологии локальных сетей:

- сети Ethernet обеспечивают скорость передачи данных до 10 Мбит/с. Это пассивная сетевая архитектура, использующая множественный доступ с контролем несущей и обнаружением конфликтов (CSMA/CD). Маршрутизатор

Cisco может применяться для разделения сети на логические подсети (например, подсети IP). Как правило, маршрутизатор подсоединяется к сети посредством неэкранированной витой пары с разъемом RJ-45. В некоторых маршрутизаторах, в частности Cisco 2505, разъемы Ethernet представляют собой порты концентратора, к которым непосредственно подключаются рабочие станции (рис. 6.4);

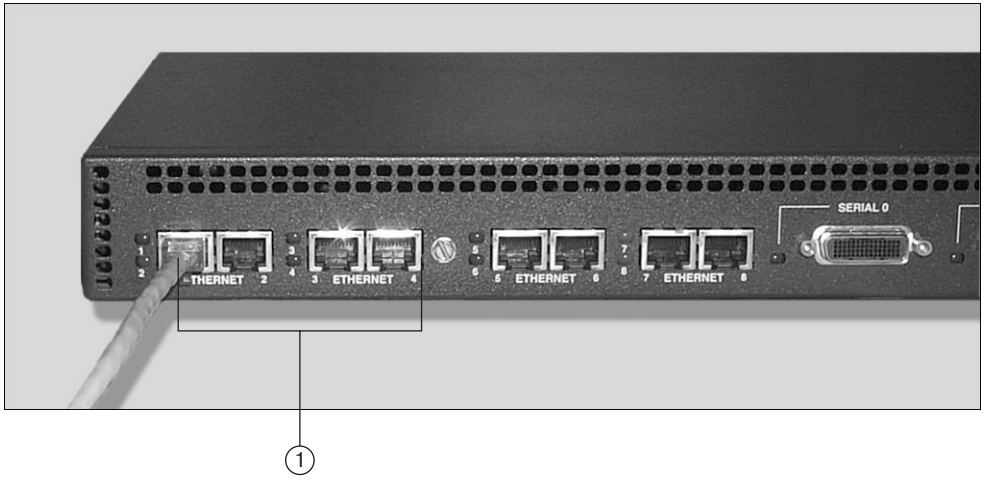


Рис. 6.4. Интерфейс маршрутизатора 2505 играет роль концентратора при подсоединении сети Ethernet: 1 – порты концентратора

- интерфейс Fast Ethernet позволяет передавать информацию со скоростью до 100 Мбит/с. Он основан на том же методе допуска, что и простой Ethernet (CSMA/CD), и в нем также применяется неэкранированная витая пара. Для работы с Fast Ethernet маршрутизатор должен обладать интерфейсом Fast Ethernet, а узлы – сетевыми адаптерами Fast Ethernet. Концентраторы, используемые в этой архитектуре, должны ей соответствовать;
- архитектура Token Ring разработана компанией IBM. Сети Token Ring построены по принципу логического кольца, которое образуют устройства множественного доступа (MAU), применяемые для соединения узлов. Методом доступа к среде является передача маркера. Маршрутизаторы, используемые в этих сетях, должны быть снабжены специальным интерфейсом Token Ring. Скорость передачи (4 или 16 Мбит/с) для интерфейса необходимо установить в соответствии со скоростью сети;
- архитектура FDDI представляет собой два кольца с передачей маркера в противоположных направлениях. Если связь в одном из колец разрывается, сеть продолжает функционировать в оставшемся кольце. Архитектура FDDI, часто применяемая в крупных волоконно-оптических сетях в качестве основной

магистрали, обеспечивает скорость передачи до 100 Мбит/с. Маршрутизаторы, задействованные в этой архитектуре, должны иметь интерфейс FDDI.

Таким образом, для всех протоколов локальных сетей требуется соответствие интерфейса маршрутизатора и архитектуры сети. Например, сеть Token Ring может быть подключена к маршрутизатору только при наличии у него интерфейса Token Ring.

➢ Спецификации некоторых маршрутизаторов Cisco рассматриваются в приложении 2, а также на сайте компании Cisco, расположенном по адресу www.cisco.com.

Проектируя интерсеть, нужно позаботиться о том, чтобы маршрутизатор содержал все необходимые интерфейсы для различных соединений с локальными сетями. На рис. 6.5 изображена интерсеть, которая состоит из локальных сетей с архитектурами Token Ring и Ethernet, соединенных маршрутизаторами.

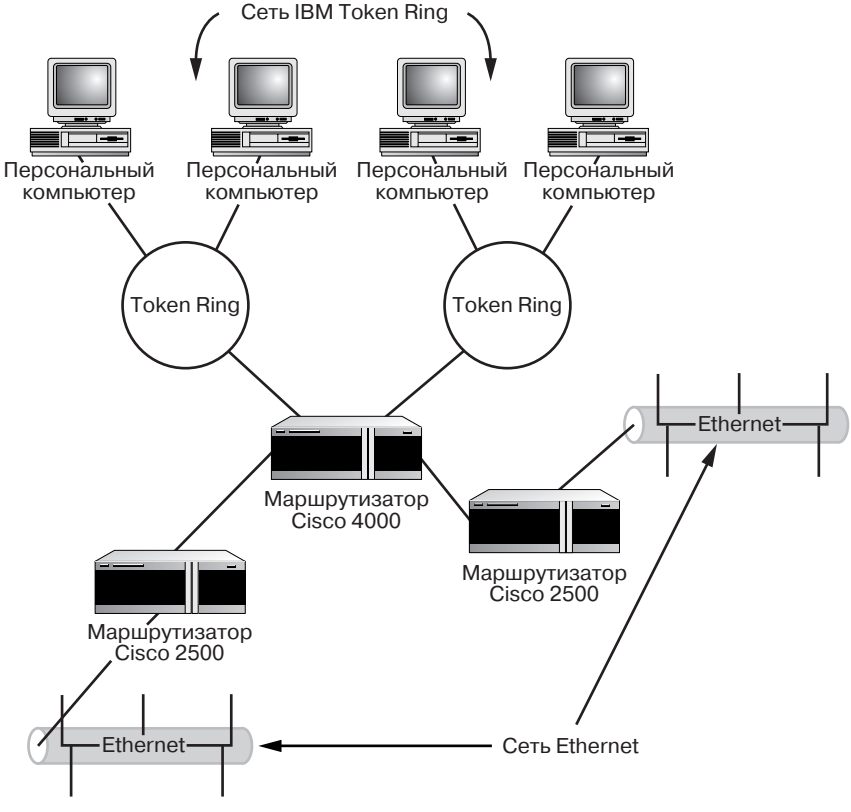


Рис. 6.5. Соединение различных архитектур посредством маршрутизаторов

➢ Аппаратные адреса (MAC-адреса) описываются в главе 2, раздел «Канальный уровень». Подробнее об архитектурах локальных сетей рассказывается в главе 1, раздел «Виды сетевых архитектур».

Маршрутизаторы могут использовать несколько маршрутизируемых (например, IP и IPX) и маршрутизирующих протоколов одновременно (см. главу 5).

Интерфейсы локального соединения маршрутизатора, как и сетевые карты, обладают уникальными MAC-адресами. Для просмотра MAC-адреса интерфейсов можно использовать команду ***show interfaces*** *(см. рис. 6.3).*

Интерфейсы последовательного соединения

Интерфейс последовательного соединения (Serial) позволяет соединять локальные сети с помощью технологий глобальных сетей. Протоколы глобальных сетей пересылают данные через синхронные и асинхронные последовательные интерфейсы маршрутизаторов, подключенные к выделенным линиям и другим устройствам передачи, которые выполняют функции посредников.

Наиболее часто используются такие технологии глобального взаимодействия на канальном уровне, как HDLC, X.25, Frame-Relay, ISDN и протокол связи «точка-точка» (PPP), которые конфигурируются на соответствующих интерфейсах маршрутизатора в режиме конфигурации.

➢ Процедура конфигурации протоколов глобальных сетей на маршрутизаторе Cisco рассматривается в главе 15.

Рассмотрим названные технологии подробнее:

- HDLC – протокол канального уровня, обеспечивающий инкапсуляцию информации, которая поступает по синхронным соединениям. Иными словами, *аппаратура передачи данных* (data communication equipment – DCE) предоставляет выход в сеть и тактовый сигнал, синхронизирующий пересылку сообщений между последовательными устройствами. К последовательным портам посредством кабеля V.35 подключается модем или другое устройство обслуживания канала/данных (CSU/DSU). HDLC считается двухточечным протоколом, который обеспечивает прямое соединение между посылающим и принимающим устройствами (например, между маршрутизаторами). Он принят по умолчанию для маршрутизаторов Cisco. Следует учитывать, что

Cisco использует собственную версию HDLC, несовместимую с аналогичными версиями других производителей, поэтому при попытке использовать маршрутизаторы разных марок могут возникнуть проблемы;

- PPP также является двухточечным протоколом, действующим на канальном уровне и поддерживаемым маршрутизаторами Cisco. Не будучи собственностью компании Cisco, он может применяться в устройствах любых производителей. PPP работает как в синхронном, так и в асинхронном режимах (иными словами, предоставляет инкапсуляцию обоих видов). Для обозначения конца и начала кадра используется *разграничитель* (flag) – несколько битов, вставляемых в поток данных. Протокол PPP служит для связи сетей IP, AppleTalk и IPX. Он конфигурируется на последовательном порте маршрутизатора, подключенном к выделенной линии. Этот протокол вам, вероятно, уже знаком, поскольку он задействован при соединении с Internet через модем;
- X.25, протокол с коммутацией пакетов, применяется в коммутируемых телефонных сетях общего пользования. Данные передаются по таким сетям посредством виртуальных каналов. X.25 работает медленнее, чем другие протоколы глобального взаимодействия, из-за выполнения большого количества проверок на ошибки. Протокол X.25 обычно используется между оконечным оборудованием пользователя (DTE) и оконечным оборудованием канала передачи данных – оборудованием провайдера (DCE). Устройством DTE, как правило, служит маршрутизатор Cisco, а в качестве DCE выступает коммутатор, принадлежащей сети. На рис. 6.6 изображена связь двух маршрутизаторов через облако X.25;

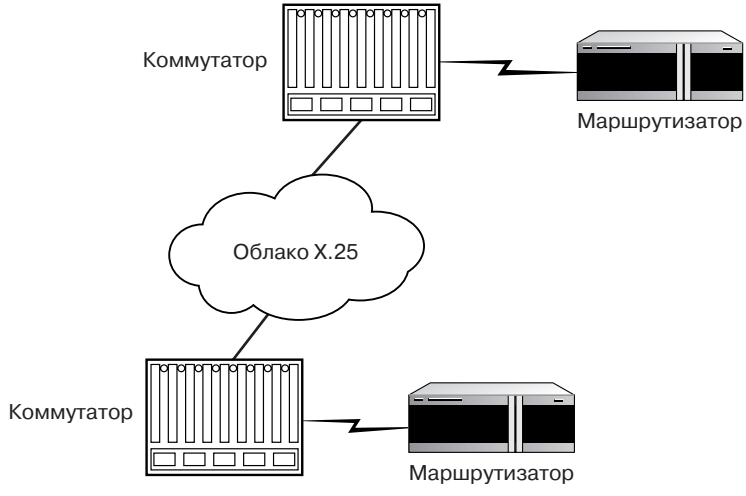


Рис. 6.6. Маршрутизаторы можно подключить к коммутаторам и сконфигурировать под протокол X.25

- Frame-Relay – протокол канального уровня с коммутацией пакетов, разработанный для применения в сетях ISDN. В настоящее время он вытесняет протокол X.25, поскольку также использует виртуальные каналы для определения наилучшего пути между двумя узлами глобальной сети. В соединениях Frame-Relay устройство DTE (маршрутизатор) подключается к оконечному оборудованию канала передачи данных (например, CSU/DSU). Большинство устройств CSU/DSU взаимодействуют с маршрутизатором посредством кабеля V.35. Кроме того, маршрутизатор можно подсоединить непосредственно к коммутационному оборудованию. Структура сети Frame-Relay, по существу, такая же, как сети X.25 (см. рис. 6.6);
- в сетях ISDN для передачи данных, голоса и изображений по существующим телефонным линиям используются цифровые технологии. Протокол ISDN является асинхронным, для него необходимо специальное оборудование – *модем ISDN*.

Допустимо также задействовать маршрутизатор с интерфейсом BRI, который подключается непосредственно к телефонной линии. Если такого интерфейса у маршрутизатора нет, можно либо подсоединить модем ISDN к одному из свободных последовательных портов, либо приобрести другой маршрутизатор.

В синхронных последовательных соединениях используется тактовое устройство, обеспечивающее синхронизацию передачи данных. При асинхронном подключении начало и конец передачи определяются стартовым и стоповым битами.

В протоколах X.25 и Frame-Relay применяется оконечное оборудование канала передачи данных (CSU/DSU или телефонные коммутаторы), подведенное к последовательным портам маршрутизатора. Даже простейший маршрутизатор низкого класса (например, 2505) может быть сконфигурирован для этих протоколов. В случае ISDN, как правило, необходим соответствующий порт, имеющийся только в особых моделях маршрутизаторов.

➢ Протоколы глобального взаимодействия рассматриваются в главе 3.

Логические интерфейсы

Прежде чем завершить обсуждение интерфейсов маршрутизаторов, рассмотрим их логические интерфейсы, реализующиеся исключительно программными средствами, а именно операционной системой маршрутизатора.

Логические интерфейсы не входят в предмет обсуждения данной книги, но об их существовании нужно знать. Они иногда конфигурируются на маршрутизаторах высокого класса, таких как Cisco 4000 и 7500, служащих центральными маршрутизаторами в крупных сетях, и применяются для пропуска или ограничения трафика в ту или иную часть сети.

➢ ОС маршрутизатора Cisco подробно описывается в главе 9.

Логический интерфейс – это *виртуальный интерфейс*, созданный командами системы. Виртуальные интерфейсы воспринимаются устройствами в сети как реальные. Можно сконфигурировать несколько различных логических интерфейсов: интерфейс кольцевой проверки, нулевой и туннельный.

Интерфейс кольцевой проверки

Интерфейс кольцевой проверки (loopback interface) эмулирует реальный физический интерфейс маршрутизатора и, как правило, конфигурируется на маршрутизаторах высокого класса, соединяющих корпоративную сеть с Internet или другой корпоративной сетью. Такие маршрутизаторы конфигурируются протоколами внешней маршрутизации, например протоколом граничной маршрутизации (BGP).

Поскольку маршрутизатор является важным звеном связи между интерсетями, он должен сохранять пакеты данных, даже если какой-либо физический интерфейс выходит из строя. Для этого создается виртуальный интерфейс кольцевой проверки, который конфигурируется как конечный адрес для сеансов протокола BGP. Трафик обрабатывается маршрутизатором, что гарантирует доставку сообщения получателю.

Нулевой интерфейс

Нулевой интерфейс (null interface) настраивается соответствующими командами и является своего рода стеной, не пропускающей заданную часть трафика. Например, если требуется, чтобы трафик из определенной сети не проходил через данный маршрутизатор (но мог идти через другие маршрутизаторы), можно сконфигурировать нулевой интерфейс, который будет сбрасывать все пакеты, приходящие из этой сети. Однако чаще для фильтрации трафика в интерсети и определения допустимых путей для конкретных сетей используются списки доступа (см. главу 14): нулевой интерфейс – это довольно грубый подход к процессу, требующему ювелирного мастерства.

Туннельный интерфейс

Туннельный интерфейс (tunnel interface) используется для передачи кадров определенного типа через соединение, которое, как правило, не поддерживает данный

тип. Например, такой интерфейс можно настроить на двух маршрутизаторах, передающих кадры AppleTalk каждый из своей локальной сети через последовательное соединение (рис. 6.7). Туннельный интерфейс конфигурируется и для маршрутизации протокола IP. И хотя обычно AppleTalk не маршрутизируется через интерфейс IP, кадры AppleTalk будут инкапсулированы (запакованы в кадры общего формата) и переданы по туннелю в виде кадров IP. Маршрутизаторы Cisco предоставляют *протокол обобщенной инкапсуляции* (generic route encapsulation protocol – GRE), который выполняет инкапсуляцию кадров для передачи через туннельный интерфейс.

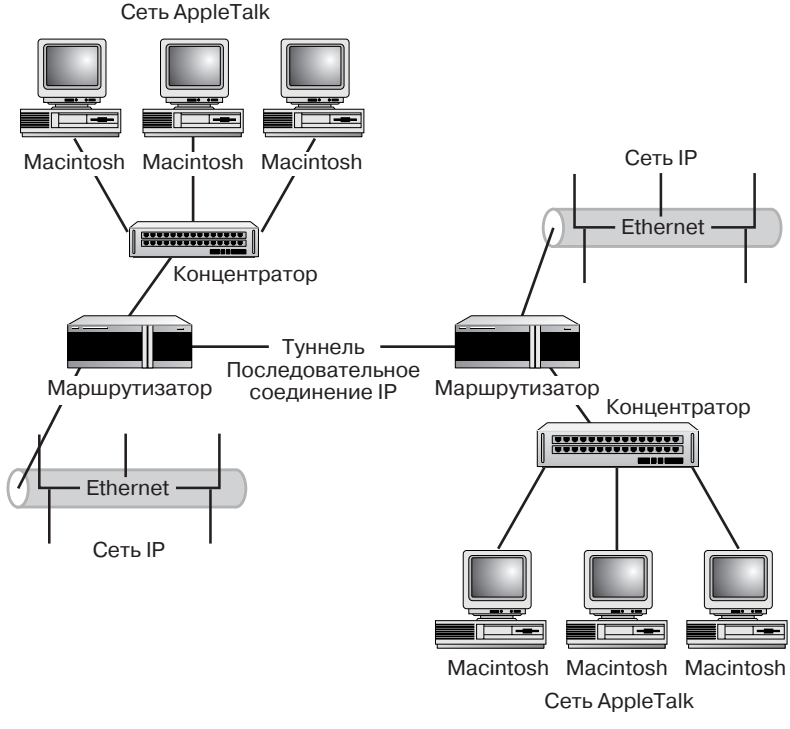


Рис. 6.7. Кадры AppleTalk маршрутизируются через виртуальный туннель IP

ГЛАВА 7

Установка маршрутизатора

Маршрутизаторы представляют собой аппаратное и программное обеспечение для маршрутизации. Они являются важными устройствами для связи подсетей в локальных сетях и объединения локальных сетей в глобальные. В главе 5 рассматривались теоретические аспекты маршрутизации, а здесь мы расскажем, как маршрутизатор применяется на практике. На рис. 7.1 показаны передняя и задняя панели маршрутизатора Cisco 2505, оснащенного тремя интерфейсами: интерфейсом локального соединения и двумя последовательными. Как правило, маршрутизаторы 2505 используются в ISDN, выделенных линиях T1 и других видах глобальной связи.

Знакомство с маршрутизатором

Существует несколько моделей маршрутизаторов Cisco, причем количество портов у них может быть различным, так как в каждом конкретном случае необходимо определенное число соединений заданного типа. Во многих маршрутизаторах высокого класса предусмотрена возможность самостоятельной настройки типа и количества интерфейсов.

> *На сайте www.cisco.com приведены сведения о продукции компании, на основе которых вы сможете выбрать подходящий маршрутизатор. В приложении 2 также представлены описания и технические характеристики некоторых моделей маршрутизаторов.*

Устройство маршрутизатора Cisco

В число функций маршрутизаторов Cisco входит составление таблиц маршрутизации, выполнение команд и передача пакетов данных через сетевые интерфейсы с помощью соответствующих протоколов. Следовательно, такие маршрутизаторы

Рис. 7.1. Маршрутизатор Cisco 2505 связывает локальные сети через последовательный интерфейс: 1 – концентратор портов Ethernet; 2 – порты последовательного соединения

должны обладать определенными вычислительными способностями и емкостью для хранения данных, иметь свободную оперативную память. Для конфигурирования протоколов маршрутизации и маршрутизируемых протоколов необходима операционная система (она будет рассмотрена в главе 9).

Центральный процессор

Маршрутизаторы, как и компьютеры, содержат микропроцессор, причем разные модели маршрутизаторов оснащены различными процессорами. Например, в маршрутизаторе Cisco 2505 используется процессор Motorola 68EC030 с тактовой частотой 20 МГц. А такой маршрутизатор высокого класса, как Cisco 7010, содержит процессор Motorola MC68040 с тактовой частотой 25 МГц. (Во многих маршрутизаторах низкого класса применяются те же процессоры, что и в компьютерах Apple Macintosh; в маршрутизаторах высокого класса чаще используются процессоры Risc, характерные для мини-ЭВМ или серверов высшего класса.)

➢ Характеристики моделей маршрутизаторов Cisco представлены в приложении 2.

Компоненты памяти

Как уже было сказано, маршрутизаторам необходимо место для содержания конфигурационных сведений, загрузки операционной системы (internetworking operating system – IOS) и хранения динамической информации в процессе работы. Маршрутизаторы Cisco имеют несколько видов памяти для хранения данных и динамического кэширования.

Рассмотрим различные типы памяти, применяемые в маршрутизаторе Cisco:

- *ПЗУ* (ROM) содержит процедуру начального самотестирования (Power On Self Test – POST) и программу начальной загрузки. В чипах ПЗУ хранится либо часть IOS, либо она вся. Так, ПЗУ маршрутизатора 2505 включает в себя только часть операционной системы, в то время как в моделях серии 7000 IOS содержится полностью. Благодаря тому, что операционная система IOS находится в ПЗУ, после крупных аварий (например, после очистки Flash RAM) удается все восстановить. Чипы ПЗУ легко заменять и модернизировать;
- *энергонезависимое ОЗУ* (Non-Volatile Read-Only Memory – NVRAM) содержит стартовую конфигурацию маршрутизатора. NVRAM можно очистить и записать в него текущую конфигурацию. Являясь энергонезависимым устройством, NVRAM сохраняет информацию даже после выключения маршрутизатора, поэтому нет необходимости всякий раз заново его конфигурировать;
- *флэш-память* (Flash RAM) является особым видом ПЗУ, которое можно очистить и перепрограммировать. Во флэш-памяти хранится операционная система Cisco IOS, но можно записать другие версии операционной системы, например обновление текущей версии IOS, что значительно упростит модернизацию маршрутизатора. Память Flash RAM имеет вид модулей SIMM, в зависимости от модели маршрутизатора можно установить дополнительные модули;
- *оперативная память* (Random Access Memory – RAM) похожа на динамическую память персонального компьютера. Она предоставляет место для временного хранения данных (в RAM помещаются пакеты данных во время анализа их адресной информации) и текущей таблицы маршрутизации. Кроме того, в RAM содержится активная конфигурация и сведения о ее изменении. Принятые изменения заносятся в NVRAM.

Различные компоненты памяти играют важную роль в процессе загрузки маршрутизатора. В следующей главе рассматривается, как происходит загрузка системы и где расположены операционная система и конфигурационная информация.

➢ Подробнее о роли различных компонентов памяти рассказывается в главе 8. Другая важная аппаратная часть маршрутизатора – его интерфейсы – описана в главе 6.

Нужно не только выбрать приемлемую модель маршрутизатора,, но и решить, какую версию Cisco IOS использовать. На сайте компании Cisco, расположенном по адресу www.cisco.com, представлена информация обо всех существующих версиях этой операционной системы. Планировщик поможет вам определить наиболее подходящую систему для вашего маршрутизатора. В частности, она должна поддерживать маршрутизацию того протокола, который вы хотите задействовать. Если вам потребуется только IP, можно выбрать версию, которая маршрутизирует исключительно протокол IP; если же вы собираетесь маршрутизировать IP, IPX и AppleTalk, вам необходима другая версия IOS. Не забывайте: операционная система не входит в комплект маршрутизатора, ее нужно приобретать отдельно.

Подсоединение к консоли

В главе 6 были описаны внутренние компоненты и интерфейсы маршрутизатора, а теперь мы рассмотрим процедуру подсоединения маршрутизатора к сети: локальное подключение через порт Ethernet и связь локальных сетей посредством глобального соединения.

➢ О конфигурировании маршрутизатора рассказывается в главе 8, а некоторые системные команды обсуждаются в главах 9, 11–13 и 15.

Прежде чем подключать маршрутизатор к сети, следует изучить документацию Cisco, предоставленную компанией Cisco или ее дилером. Проверьте спецификацию кабеля, указанную на нем вблизи от разъемов, тип операционной системы (маршрутизатор не будет работать с не соответствующей ему версией IOS), удостоверьтесь, что получены все заказанные компоненты и интерфейсы. Если комплект окажется неполным или выяснится, что маршрутизатор снабжен неподходящими интерфейсами (или, в случае маршрутизаторов высокого класса, неподходящими адаптерами интерфейсов), свяжитесь с местным дилером компании Cisco.

Проверив комплектность маршрутизатора, кабелей и программного обеспечения, можно приступать к сборке устройства. Убедитесь, что устройство выключено, и подсоедините шнур питания к маршрутизатору и источнику питания. Затем подключите к маршрутизатору ПК, который будет выполнять функцию консоли. Консолью может быть любой компьютер с портом для последовательного соединения, поддерживающий эмуляцию терминала. Компьютер, по сути, становится в таком случае терминалом ввода/вывода и предоставляет интерфейс для конфигурирования и контроля маршрутизатора.

Компьютер-консоль и маршрутизатор связываются посредством кабеля, поставляемого в комплекте с маршрутизатором. С обеих сторон кабель оканчивается разъемом RJ-45 (рис. 7.2).

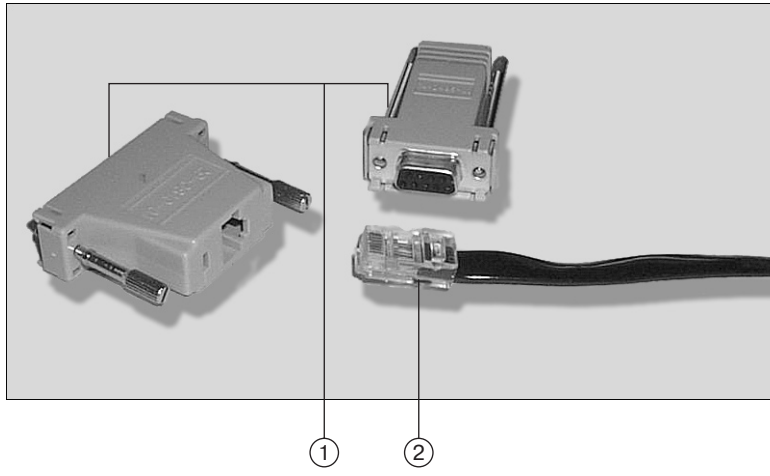


Рис. 7.2. Для соединения маршрутизатора с компьютером-консолью используется кабель: 1 – адаптеры для последовательного порта; 2 – кабель

В комплект также входят несколько различных *адаптеров для последовательного соединения*, имеющих гнездо для разъема RJ-45. К ним можно подвести кабель, а затем подключить этот кабель к последовательному порту компьютера-консоли (см. рис. 7.2). Выбрав подходящий адаптер, приступайте к соединению маршрутизатора с консолью:

1. Подключите кабель с разъемом RJ-45 к порту на задней панели маршрутизатора с надписью CONSOLE (рис. 7.3).
2. Другой конец кабеля (с адаптером) присоедините к последовательному порту компьютера-консоли.

После этого разрешается переходить к установке программы эмуляции терминала на персональном компьютере (программа эмуляции терминала и установки для коммуникации с маршрутизатором рассматриваются в следующем разделе).

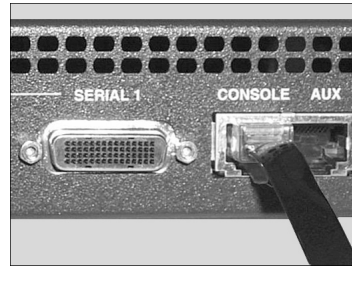


Рис. 7.3. Кабель с разъемом RJ-45 подводится к порту CONSOLE

Для того чтобы маршрутизатор можно было подсоединить к различным локальным сетям, его надо разместить в серверном шкафу или там, где его легко подключить к выделенной линии, предоставленной провайдером. Маршрутизатор Cisco обычно поставляется с монтажными скобами, с помощью которых он легко устанавливается в стойку для концентраторов или другого оборудования. Если же вы предполагаете разместить это устройство в труднодоступном месте, удобнее сначала сконфигурировать его (см. главу 8) и лишь потом обеспечивать физические соединения.

Конфигурирование консоли

Компьютер, выполняющий функции консоли, обменивается информацией с маршрутизатором благодаря *программе эмуляции терминала*. Существует несколько таких программ, например HyperTerminal, поставляемый в комплекте с операционными системами Windows 9x и 2000, и ProComm Plus, – коммерческий продукт, позволяющий отправлять факс, эмулировать терминал и т.п. В сети Internet можно найти другие бесплатные или условно бесплатные программы, в частности Tera Term Pro – очень простой в использовании и настройке эмулятор терминала (рис. 7.4).

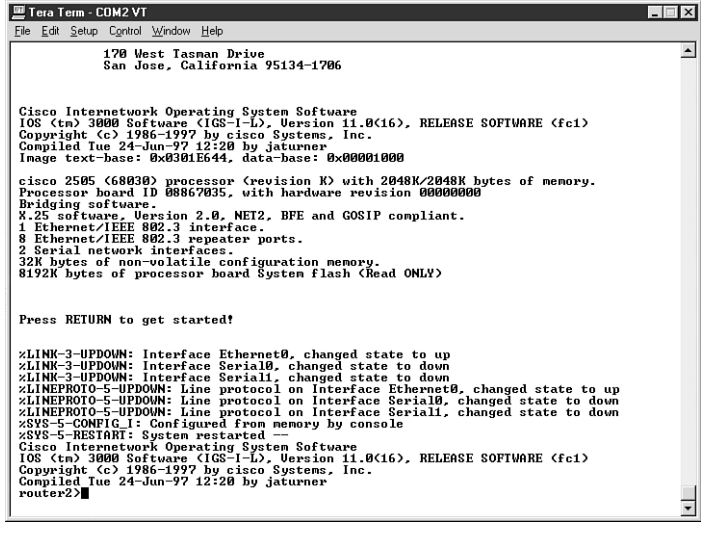


Рис. 7.4. Эмулятор терминала используется для связи между компьютером и маршрутизатором

После того как программа эмуляции терминала установлена, необходимо настроить параметры связи для последовательного порта. В табл. 7.1 приведены значения, которые должен использовать эмулятор терминала.

Таблица 7.1. Настройки связи для терминала

Параметр	Значение
Эмуляция терминала	VT100
Скорость передачи, бод	9600
Четность	Нет
Биты данных	8
Стоповые биты	1 (2 для маршрутизаторов серии 2500)

Скорость передачи (в бодах) определяется как количество элементов сигнала в секунду. Если каждый бит представляет собой один элемент, то 1 бод равняется 1 бит/с.

Проверка четности используется для обнаружения ошибок. Нечетное значение этого параметра означает, что каждое слово данных должно состоять из нечетного количества битов, а четное значение предполагает четное число битов. Если слово данных не соответствует заданному требованию, его нужно передать заново.

Биты данных – количество битов в каждом кадре.

Стоповые биты – количество битов, обозначающих окончание кадра.

Многие программы эмуляции терминала, которые можно найти в Internet, служат для связи между компьютерами через глобальную сеть. Это означает, что они не подходят для последовательных соединений. Прежде чем скачать и становить эмулятор терминала, убедитесь, что он пригоден для подключений по последовательному порту. Программа HyperTerminal, включенная в операционную систему Windows, может использоваться в последовательных соединениях (с установками, приведенными в табл. 7.1).

Эмулируя терминал, компьютер работает как устройство ввода/вывода, отправляющее и принимающее данные через последовательный порт. Терминал DEC VT 100 был стандартным терминалом ввода/вывода в больших и алых ЭВМ, а теперь используется в качестве образца для последовательных соединений в ПК.

Работа с эмулятором терминала

Каждая программа эмуляции терминала работает по-своему, но все они позволяют задавать значения некоторых параметров в диалоговом окне. На рис. 7.5 изображено диалоговое окно настройки порта Serial в программе Tera Term. Значения параметров выбираются в открывающихся списках.

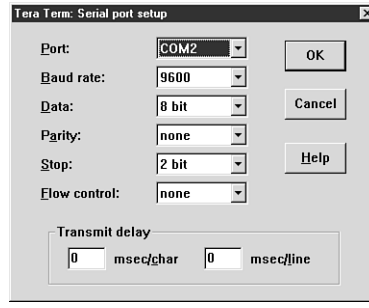


Рис. 7.5. Настройки параметров связи для последовательного порта в ОС Windows

После того как эмулятор терминала сконфигурирован, связь с маршрутизатором устанавливается следующим образом:

1. Запустите программу эмуляции терминала и удостоверьтесь, что выбран правильный порт и заданы соответствующие значения параметров (см. табл. 7.1).
2. Включите питание маршрутизатора.

На экране должна появиться титульная страница маршрутизатора (см. рис. 7.4). Если этого не произошло, проверьте соединения в портах и убедитесь, что в эмуляторе терминала указан правильный последовательный порт.

Новый маршрутизатор еще не сконфигурирован, то есть на нем не установлены соответствующие протоколы и ни один из интерфейсов не подготовлен к связи (процедура конфигурирования маршрутизатора описана в главе 8).

Соединение маршрутизатора с сетью

Установив взаимодействие маршрутизатора и консоли, вы получаете возможность конфигурировать различные его параметры. (Существуют и другие методы конфигурирования маршрутизатора, о них будет рассказано в главе 8.) Следующий шаг – подключение маршрутизатора к сети, которую он будет обслуживать.

Как говорилось в главе 6, маршрутизатор в состоянии иметь несколько различных интерфейсов в зависимости от модели и выбранной конфигурации. Рассмотрим основные возможности сетевых соединений на примере маршрутизатора Cisco 2505.

Локальные соединения

Локальные соединения обычно производятся через порты Ethernet или Token Ring маршрутизатора, а затем через концентратор или устройство множественного доступа (MAU), предоставляющее связь с разными компьютерами сети.

Допустим, требуется наладить взаимодействие маршрутизатора с локальной сетью Ethernet. Для этого концентратор соединяют с портом Ethernet маршрутизатора посредством витой пары пятой категории, а потом подключают к нему компьютеры.

Чтобы применять прямоточную витую пару пятой категории, переключатель MDI/MDI-X на маршрутизаторе необходимо установить в положение MDI-X. Если такого переключателя нет (как, например, в моделях Cisco 2505 и 2507), следует использовать кабель с перекрестным током, в котором получаемые и отправляемые сигналы ревертированы.

В некоторых маршрутизаторах, например в Cisco 2505, интерфейс Ethernet реализован в виде концентратора (рис. 7.6), что позволяет обойтись без отдельного концентратора и подсоединять компьютеры непосредственно к маршрутизатору. Если же требуются дополнительные порты, то концентратор можно подключить через витую пару с перекрестным током.

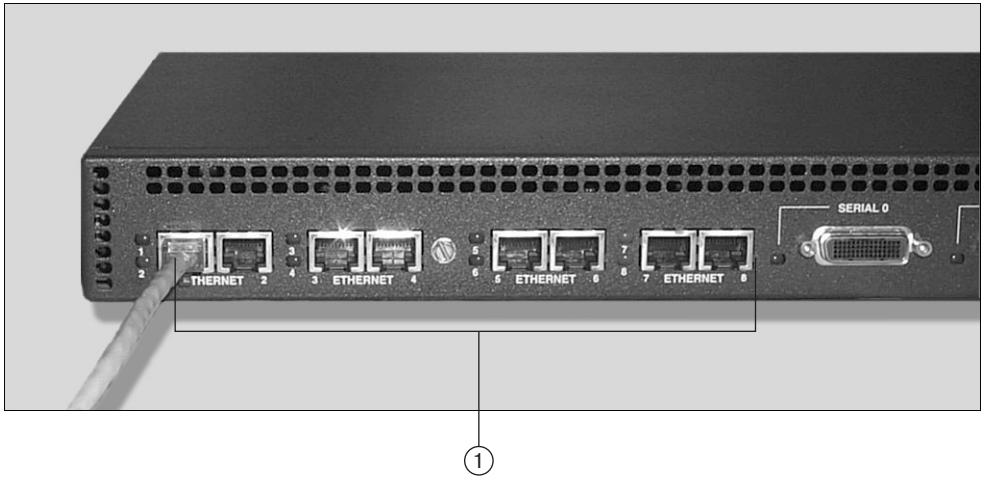


Рис. 7.6. Интерфейс Ethernet маршрутизатора Cisco 2505 имеет вид восьмипортового концентратора: 1 – порты концентратора

➢ Подробнее о витых парах рассказывалось в главе 1, раздел «Сетевые кабели».

Подключая концентраторы к порту Ethernet маршрутизатора цепочкой, не забывайте, что между устройствами Ethernet может располагаться не более четырех концентраторов.

Последовательные соединения

Последовательные соединения можно сконфигурировать для различных протоколов глобальных сетей. Порт последовательного соединения в маршрутизаторах Cisco представляет собой разъем на 60 контактов (рис. 7.7).

Рис. 7.7. Последовательный порт маршрутизатора Cisco

Маршрутизатор Cisco 2505 имеет два порта Serial. Порт последовательного соединения поддерживает различные стандарты передачи сигналов, в частности V.35, X.21 bis, EIA-530. На рис. 7.8 изображен кабель V.35 с 60-штырьковым разъемом. Другим концом такой кабель обычно подключается к CSU/DSU или иному устройству глобального сетевого взаимодействия. В табл. 7.2 перечислены сигнальные стандарты, которые поддерживаются интерфейсами последовательного соединения маршрутизаторов Cisco.

Таблица 7.2. *Сигнальные стандарты для последовательных соединений*

Стандарт	Спецификация
V.35	Синхронные соединения между сетями с коммутацией пакетов
X.21 bis	Связь между DTE и DCE в глобальных сетях с протоколом X.25
EIA-530	Стандарт RS232 для несбалансированного последовательного соединения

Если вы правильно подключили интерфейс, то маршрутизатор подтвердит соединение. Например, при подключении какого-нибудь устройства к последовательному порту маршрутизатор отметит, что интерфейс активен, даже если соответствующий протокол еще не сконфигурирован.

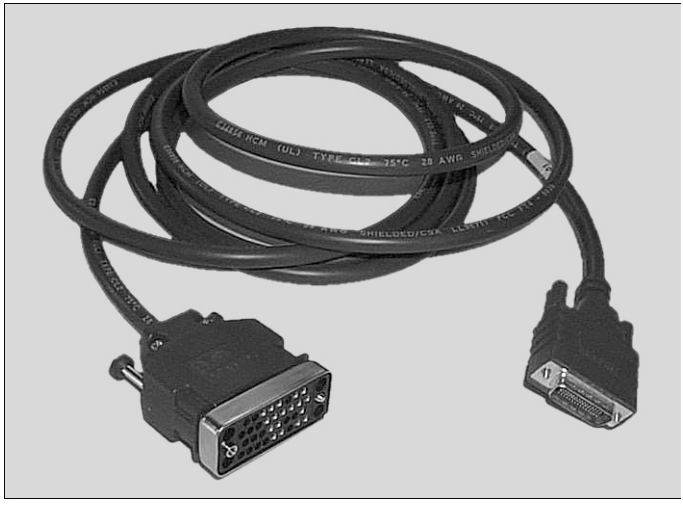


Рис. 7.8. Кабель V.35 для подключения к порту Serial устройств, аналогичных CSU/DSU

Резюме

На вопрос, в каком порядке следует действовать: сначала конфигурировать маршрутизатор, а потом присоединять его к сети, или наоборот, – однозначно ответить невозможно. Установив на маршрутизаторе самую простую конфигурацию и убедившись, что устройство обнаруживается в сети, допустимо активизировать все его физические соединения и завершить конфигурирование через сеть посредством виртуального терминала (такие терминалы будут рассматриваться в следующей главе).

Если маршрутизатор подключили к устройствам глобального и локального взаимодействия несконфигурированным, то сразу после подключения можно провести полную конфигурацию и проверить связь. Однако когда маршрутизатор помещен в труднодоступное место, то может оказаться достаточно сложным подсоединить к нему компьютер для настройки.

В следующей главе будет рассказано, как сконфигурировать новый маршрутизатор.

При покупке кабеля для последовательного соединения маршрутизатора с другими устройствами убедитесь, что у него подходящие разъемы. Кабели только кажутся одинаковыми, поэтому нужно быть внимательным.

ГЛАВА 8

Базовая конфигурация маршрутизатора

Базовое конфигурирование маршрутизатора состоит в активизации различных интерфейсов и настройке параметров протоколов маршрутизации и маршрутизируемых протоколов. Например, для маршрутизации протокола IP следует задать интерфейсам соответствующие IP-адреса. Необходимо настроить протоколы маршрутизации, в частности протоколы RIP или IGRP. Интерфейсы последовательных соединений тоже нужно конфигурировать для использования соответствующего протокола второго уровня (допустим, HDLC или Frame-Relay). В основную конфигурацию может входить установка полосы пропускания и настройка интервалов времени и других параметров для соединений с глобальными сетями.

Конфигурирование маршрутизатора

Конфигурационный файл маршрутизатора задействует необходимые программные установки (все команды, применяемые для настройки, встроены в систему Cisco IOS). Существует несколько способов настройки маршрутизатора: либо напрямую через консоль, либо при помощи загрузки конфигурационного файла с сервера TFTP (Trivial File Transfer Protocol):

- консоль маршрутизатора. Маршрутизатор можно сконфигурировать непосредственно с компьютера, подсоединенного к его порту CONSOLE кабелем, который поставляется в комплекте с устройством. На компьютере должен быть установлен эмулятор терминала, позволяющий связываться с маршрутизатором через последовательный порт. Можно также подключиться к маршрутизатору через дополнительный вход (AUX), расположенный, как правило, рядом с входом CONSOLE на задней панели;
- виртуальный терминал. Если на маршрутизаторе уже создана базовая конфигурация и активизированы некоторые интерфейсы (например, порт Ethernet), то с ним можно связаться при помощи программы Telnet, работающей как *виртуальный терминал*, и сконфигурировать устройство (для этого нужно знать соответствующие пароли – о них речь пойдет позже);

- управляющая рабочая станция. Маршрутизатор допустимо сконфигурировать и с рабочей станции, на которой установлены специальные программы управления, например CiscoWorks или аналогичный продукт компании Hewlett Packard – HP OpenView;
- графическая программа Cisco ConfigMaker. Эта программа (рис. 8.1) позволяет создавать конфигурацию для одного или нескольких маршрутизаторов и затем устанавливать ее на маршрутизаторах, подсоединенных к консоли (то есть к компьютеру с программой ConfigMaker) или к сети. Для загрузки конфигурации на маршрутизаторы, подключенные к сети, необходимо, чтобы их сетевые интерфейсы уже были сконфигурированы. Программа ConfigMaker будет подробно рассмотрена в главе 16;
- сервер TFTP. Можно загрузить конфигурационный файл с сервера TFTP, предварительно его туда записав. О серверах TFTP речь пойдет в главе 17.

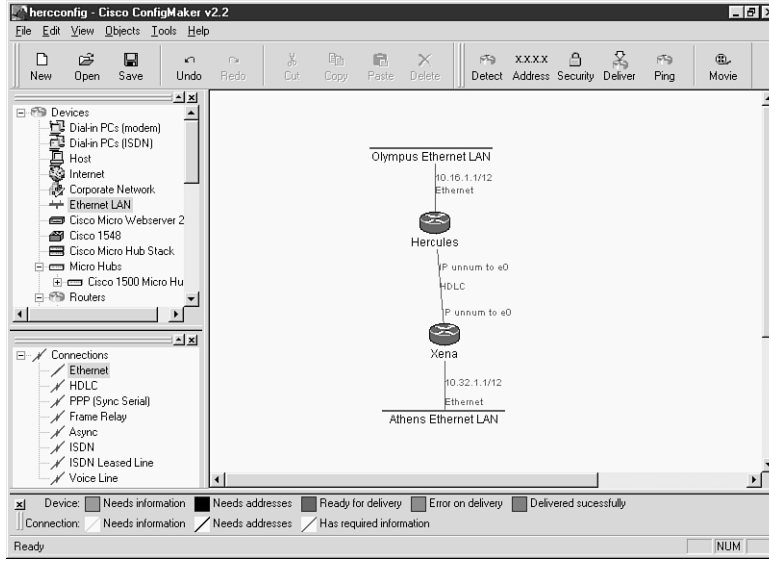


Рис. 8.1. Программа ConfigMaker позволяет создать схему сети и загружать файлы конфигурации на маршрутизаторы

Проще всего действовать непосредственно через порт CONSOLE (рис. 8.2). Такой подход позволяет не только быстро установить базовую конфигурацию с помощью диалогового окна системной конфигурации, но и детально настроить ее в режиме конфигурации маршрутизатора.

Прежде чем изучать способы создания базовой конфигурации в диалоговом режиме системной конфигурации, рассмотрим процедуру загрузки маршрутизатора.

➢ Подробнее об основных командах маршрутизатора и конфигурировании рассказывается в главе 9.

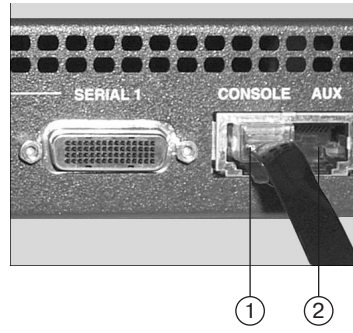


Рис. 8.2. Компьютер можно подключить непосредственно к портам маршрутизатора: 1 – порт CONSOLE; 2 – порт AUX (вспомогательный)

Установка правильной конфигурации – важнейший аспект работы с маршрутизатором. В этой главе вы узнаете, как сохранять и защищать конфигурационные файлы.

Процесс загрузки маршрутизатора

Выше уже говорилось о различных видах памяти маршрутизатора: RAM, NVRAM, Flash RAM, ROM, каждый из которых играет определенную роль в процессе загрузки устройства. Прежде чем приступить к описанию этапов конфигурирования, необходимо рассмотреть процедуру загрузки и узнать, где находится конфигурационный файл.

Когда вы включаете маршрутизатор, чип ПЗУ запускает *тест POST* (Power On Self Test), контролирующий аппаратное обеспечение маршрутизатора: процессор, интерфейсы и память. Этот тест подобен проверке, которая выполняется сразу после включения персонального компьютера.

Далее запускается программа самозагрузки, записанная в ПЗУ (ROM), которая производит поиск системы Cisco IOS. Операционная система может быть загружена из ПЗУ (маршрутизаторы хранят в ПЗУ либо всю IOS, либо ее часть), из Flash RAM или с сервера TFTP (команды загрузки IOS будут рассмотрены в следующей главе). Как правило, IOS находится во флэш-памяти.

Когда операционная система загружена, маршрутизатор ищет конфигурационный файл. Обычно он располагается в памяти NVRAM, но, как и в случае с IOS, его можно загрузить с сервера TFTP.

Из файла конфигурации считывается информация о запуске интерфейсов и о параметрах, связанных с маршрутизируемыми и маршрутизирующими протоколами (рис. 8.3). Следует иметь в виду, что для загрузки операционной системы не из флэш-памяти, а из другого источника необходима запись в реестре конфигурации ПЗУ; кроме того, для получения файла конфигурации не из NVRAM требуется,

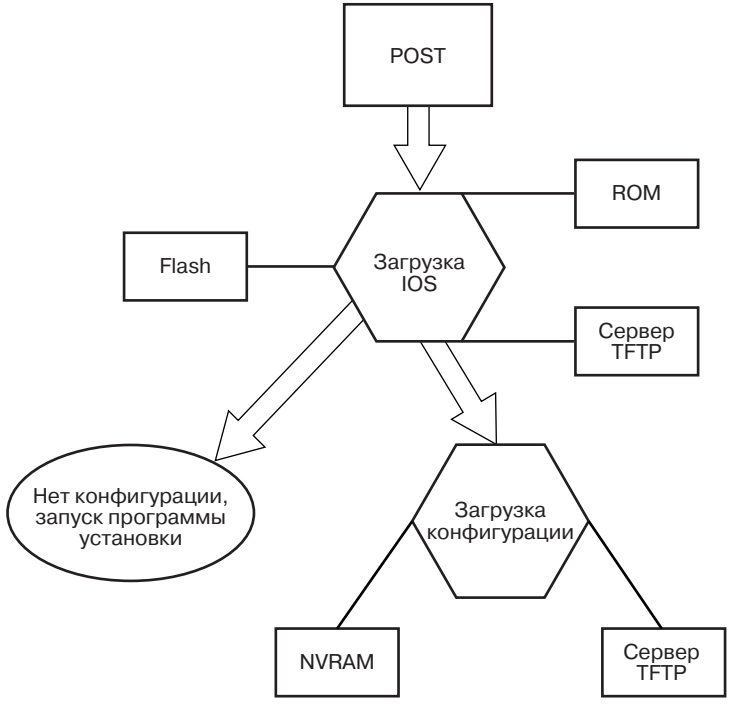


Рис. 8.3. Загрузка операционной системы и конфигурационного файла

чтобы в NVRAM содержалась информация, указывающая местоположение этого файла.

Если файл конфигурации не удается обнаружить ни в NVRAM, ни в другом заданном месте, маршрутизатор переходит в режим установки, и на экране консоли появляется диалоговое окно системной конфигурации. В следующем разделе мы расскажем, как создать основную конфигурацию в режиме диалога.

➢ Компоненты памяти маршрутизатора рассматриваются в главе 7 (раздел «Устройство маршрутизатора Cisco»). Подробнее о наборе команд системы Cisco IOS говорится в главе 9.

Файл конфигурации можно удалить и заново создать с помощью диалогового окна установки. В режиме установки введите ***`erase startup-config`*** *и нажмите* **Enter***: конфигурация будет удалена из NVRAM. Для перезагрузки маршрутизатора воспользуйтесь командой* ***`reload`*** *и снова нажмите* **Enter***. После перезапуска на экране консоли появится диалоговое окно системной конфигурации.*

Работа в режиме системной конфигурации

Когда вы включаете маршрутизатор в первый раз (или впервые после удаления файла конфигурации), запускается программа системной конфигурации (рис. 8.4). В режиме установки вам предлагаются вопросы, ответы на которые позволят создать базовую конфигурацию.

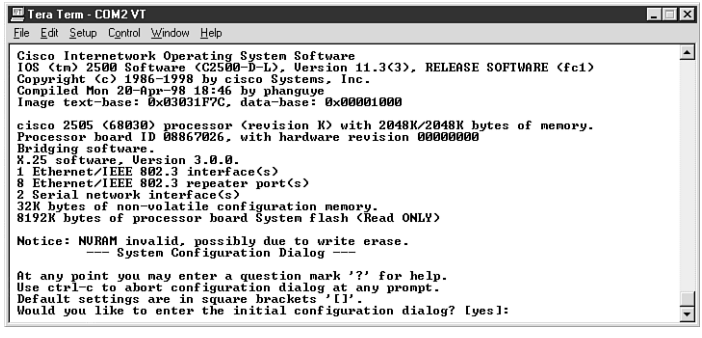


Рис. 8.4. В диалоговом окне установки можно сконфигурировать новый маршрутизатор

Для работы с данной программой необходимо представлять, какие протоколы предполагается маршрутизировать (IP, IPX, AppleTalk), и располагать информацией о параметрах, относящихся к интерфейсам. Например, для маршрутизации IP нужно знать IP-адреса соответствующих интерфейсов (ниже будут приведены примеры).

➢ Подробнее об IP-адресации рассказывается в главе 11.

Ниже описывается процесс конфигурации для маршрутизатора 2505 с системой Cisco IOS 11.3, которая поддерживает маршрутизацию IP, IPX, AppleTalk и DECnet. В этой книге обсуждается маршрутизация трех наиболее распространенных протоколов: IP, IPX и AppleTalk.

Запуск программы установки

Программа предлагает пользователю ответить на вопросы, связанные с установкой различных паролей и конфигурированием интерфейсов маршрутизатора. Сначала задаются пароли для входа в режим конфигурации и для работы с виртуального терминала (Telnet):

1. В качестве ответа на вопрос `Would you like to enter the initial configuration dialog?` (Начать диалог базовой конфигурации?) нажмите **Enter** (по умолчанию принимается ответ «да») – см. рис. 8.4.
2. После этого программа спросит, показывать ли текущие данные об интерфейсах. Нажав **Enter**, вы сможете просмотреть информацию об интерфейсах маршрутизатора (рис. 8.5). Обратите внимание, что Ethernet 0 активизирован, а оба интерфейса Serial отключены. Кроме того, никакие IP-адреса еще не назначены.

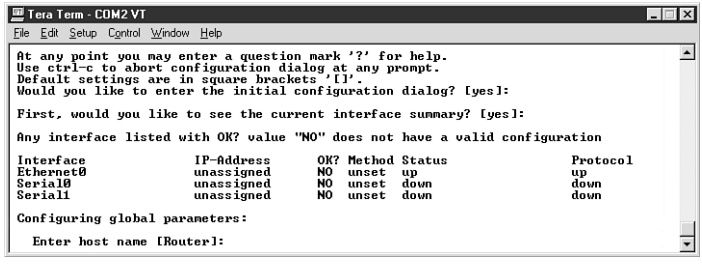


Рис. 8.5. Программа установки предоставляет текущие данные по физическим интерфейсам маршрутизатора

3. Далее программа предложит присвоить маршрутизатору имя. Введите любое имя (например, `ciscokid`) и нажмите **Enter**.
4. Следующий этап – выбор секретного пароля `enable secret`. Этот пароль зашифровывается и служит для предоставления доступа к режиму конфигурации (Enable), позволяющему производить изменения в настройках маршрутизатора. Впишите какой-нибудь пароль и нажмите **Enter**.
5. Затем требуется указать простой пароль для настроек. Он может показаться излишним, поскольку аналогичный пароль уже был предоставлен. Дело в том, что второй пароль относится к старым версиям Cisco IOS, в которых не было возможности шифрования пароля для режима настроек. Так как оставить пустой пароль нельзя, введите простое, но неочевидное для постороннего человека значение (скажем, `password`) и нажмите **Enter**.
6. Теперь необходимо определить пароль для виртуального терминала. Этот пароль используется виртуальными терминалами, связывающимися с маршрутизатором через Telnet. Он дает возможность следить за состоянием маршрутизатора и даже конфигурировать его с удаленной рабочей станции. Задайте пароль и нажмите **Enter**.
7. Далее программа спросит, разрешать ли использование *простого протокола управления сетью* (simple network management protocol – SNMP). Этот протокол включает в себя основные сетевые операции и позволяет отслеживать изменения в сети с помощью станции управления, для которой требуется программа CiscoWorks. Если вы не собираетесь работать с программами

управления маршрутизаторами, запретите применение SNMP: введите `no` и нажмите **Enter**.

Конфигурирование маршрутизируемых протоколов

Следующий этап установки касается конфигурирования протоколов, которые будут применяться на маршрутизаторе. Программа спросит, какие маршрутизируемые протоколы, поддерживаемые данной версией IOS, включить, а также работу каких протоколов маршрутизации разрешить:

1. В случае маршрутизатора 2505 будет задан вопрос, разрешать ли использование протокола DECnet (DECnet – это стек протоколов фирмы Digital Equipment Corporation). По умолчанию предлагается ответ «нет»; если вы согласны, нажмите **Enter**.
2. Далее (для маршрутизатора 2505) нужно решить, конфигурировать ли протокол AppleTalk. Сейчас лучше сказать «нет» (это ответ по умолчанию; о маршрутизации протокола AppleTalk речь пойдет в главе 13). Нажмите **Enter**.
3. На вопрос, конфигурировать ли IPX (эта тема будет рассматриваться в главе 12), ответьте «нет» (нажмите **Enter**).
4. Теперь следует указать, нужно ли конфигурировать IP. По умолчанию предлагается ответить «да» (рис. 8.6). Хотя протокол IP детально описывается ниже, в главах 10 и 11, имеет смысл включить его уже на данном этапе: в таком случае маршрутизатор сможет работать в сети, а дальнейшее конфигурирование допустимо будет произвести с виртуального терминала или посредством загрузки готовой конфигурации из ConfigMaker или с сервера TFTP. Нажмите **Enter**.

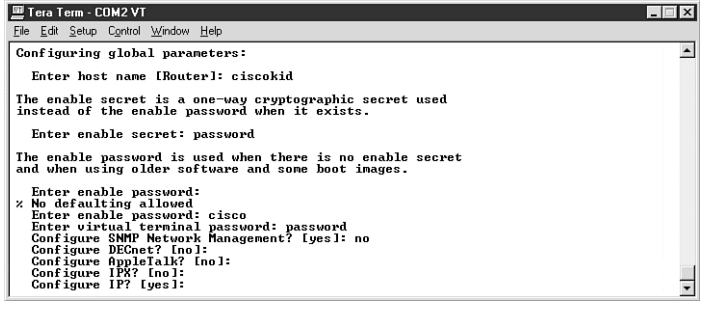


Рис. 8.6. Когда IP сконфигурирован, маршрутизатор готов к дальнейшему конфигурированию через сеть

5. Далее программа спросит, конфигурировать ли IGRP – один из протоколов маршрутизации IP. О конфигурировании IGRP и RIP будет рассказываться

в главе 11, а сейчас лучше отключить эту опцию. Введите `no` и нажмите **Enter**.

6. Этот вопрос связан с конфигурированием RIP. По умолчанию принимается ответ «не конфигурировать», поэтому просто нажмите **Enter**.
7. И наконец, укажите, следует ли разрешать работу в режиме моста. Нажмите **Enter** (по умолчанию выбран ответ «нет»).

Конфигурирование интерфейсов маршрутизатора

После того как выполнены все предыдущие операции, нужно настроить интерфейсы маршрутизатора, установив для начала, какие интерфейсы будут использоваться. Затем, поскольку применяется протокол IP, интерфейсам придется назначить IP-адреса. (О том, как работать с IP-адресами, рассказывается в главе 10.) Конфигурирование интерфейсов производится следующим образом:

1. Первым интерфейсом маршрутизатора 2505 является Ethernet 0. Разрешите его использование, нажав **Enter**.
2. На вопрос, конфигурировать ли IP на этом интерфейсе (E0), ответьте «да» (по умолчанию) и нажмите **Enter**.
3. Далее программа запросит IP-адрес интерфейса (напомним, что интерфейсы маршрутизатора, как и сетевые узлы, имеют IP-адреса). Введите `10.16.1.1` (рис. 8.7) и нажмите **Enter**.

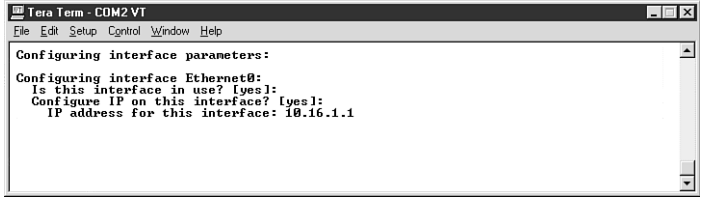


Рис. 8.7. Порту Ethernet 0 присваивается IP-адрес

4. Следующий вопрос касается количества битов в поле подсети. Это число показывает, сколько подсетей IP создано в вашей интерсети (см. главу 10). На данном этапе примите, что доступные IP-адреса (адреса класса A) разделены на 14 подсетей, что требует четырех битов в поле подсети. Введите `4` и нажмите **Enter**.
5. Так как интерфейс E0 в действительности является восьмипортовым концентратором, следует указать, все ли порты концентратора нужно включить. По умолчанию принимается ответ «да», поэтому просто нажмите **Enter**.

6. Далее те же вопросы будут задаваться касательно следующего интерфейса, которым в данном случае является порт Serial 0. По умолчанию предлагается ответ «да». Нажмите **Enter**.
7. Теперь определите, конфигурировать ли IP на интерфейсе S0. Лучше ответить «да», нажав **Enter**.
8. Далее программа предложит вариант безадресного конфигурирования интерфейса S0 (то есть интерфейс будет маршрутизировать протокол IP, не имея своего IP-адреса), чтобы сохранить свободные IP-адреса. Конфигурирование последовательных интерфейсов с IP-адресами детально рассматривается в главе 11. В данном случае ответьте «нет» (нажмите **Enter**).
9. В ответ на запрос о IP-адресе интерфейса S0 введите `10.32.1.1` и нажмите **Enter**.
10. Укажите количество битов в поле подсети: по умолчанию принимается «4» (ответ на аналогичный вопрос для интерфейса E0). Нажмите **Enter** (поскольку расчет битов тот же).
11. Теперь программа спросит, конфигурировать ли интерфейс Serial 1. Скажите «да» (нажмите **Enter**).
12. Определите, должен ли IP быть безадресным. Лучше ответить «нет» (по умолчанию), нажав **Enter**.
13. Задайте IP-адрес интерфейса S1: введите `10.48.1.1` (рис. 8.8) и нажмите **Enter**.
14. Укажите количество битов в поле подсети: по умолчанию по-прежнему принимается ответ «4». Нажмите **Enter**.

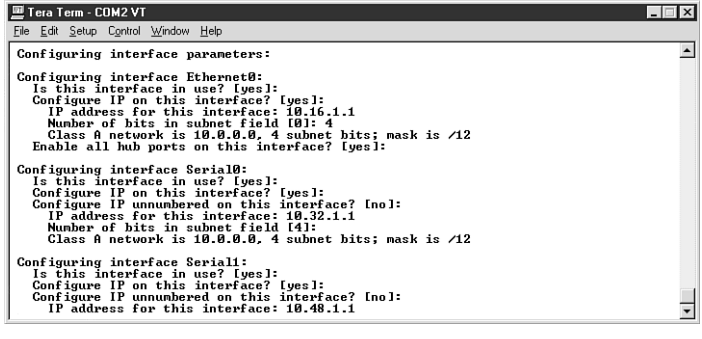


Рис. 8.8. IP-адреса назначаются каждому последовательному интерфейсу

После выполнения всех указанных действий будет произведено тестирование связи со сконфигурированными интерфейсами (на экране промелькнут строки тестирования). На вопрос, сохранить ли текущую конфигурацию, введите `yes` («да») и нажмите **Enter**. Конфигурация будет записана в NVRAM маршрутизатора.

Снова нажав клавишу **Enter**, вы войдете в пользовательский режим, где можно просматривать параметры конфигурации.

Режимы маршрутизатора

Теперь, когда на маршрутизаторе создана основная настройка, можно детально рассмотреть различные режимы его работы. Существует три базовых режима: пользовательский, привилегированный и режим конфигурации, различающиеся уровнем доступа к настройкам маршрутизатора и возможностями ее редактирования.

Пользовательский режим предоставляет ограниченный доступ к маршрутизатору. В этом режиме разрешается просматривать (но не изменять) некоторые параметры конфигурации.

Привилегированный режим, называемый также режимом настроек, позволяет детально анализировать состояние маршрутизатора и предоставляет в распоряжение пользователя большее количество команд. После входа в этот режим с помощью секретного пароля (или простого, если секретный не был установлен) вы можете работать с командами конфигурирования и, таким образом, изменять настройки маршрутизатора.

Режим конфигурации, или режим глобальной конфигурации, включаемый только из привилегированного режима, предоставляет полный набор команд для настройки маршрутизатора. Имеются соответствующие подрежимы работы для конфигурации протоколов, настройки интерфейсов и т.д.

> *Существуют и другие режимы, позволяющие конфигурировать маршрутизатор в тех случаях, когда во флэш-памяти не удается отыскать корректной операционной системы или IOS требуется загрузить из другого источника. Если маршрутизатор не находит работоспособной IOS, включается режим контроля ПЗУ, разрешающий конфигурирование. Режим RXBoot применяется для загрузки маршрутизатора, если подходящей IOS не обнаружено. Режим контроля ПЗУ также используется для смены забытых паролей (см. также раздел «Замена потерянного пароля»).*

Пользовательский режим

Как было отмечено, в пользовательском режиме возможен лишь просмотр конфигурации. По умолчанию после перезагрузки маршрутизатора включается именно этот режим, однако доступ к нему может быть защищен паролем консоли (в разделе «Режим конфигурации» рассматриваются различные команды, связанные с паролями).

На рис. 8.9 показано приглашение, сконфигурированное в диалоговом режиме установки: имя маршрутизатора и значок > («больше»). Здесь же изображен результат выполнения команды `show interfaces`.

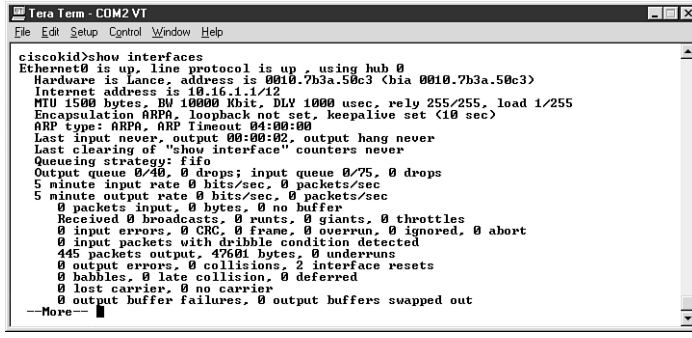


Рис. 8.9. В пользовательском режиме конфигурацию можно просматривать с помощью ограниченного набора команд

Пользовательский режим работает по принципу «смотреть можно, трогать нельзя». Тем не менее он позволяет детально охарактеризовать состояние маршрутизатора.

➢ Подробнее о командах, доступных в пользовательском режиме, рассказывается в главе 9.

Привилегированный режим

В привилегированном режиме доступны те же команды просмотра состояния маршрутизатора, что и в пользовательском, а также некоторые дополнительные (например, команда `show running-config`, позволяющая увидеть текущую конфигурацию). Отсюда с помощью команды `config` можно войти в режим конфигурации.

В привилегированном режиме осуществляется реальный контроль за маршрутизатором, поэтому чрезвычайно важно защитить доступ в этот режим паролем. Нельзя позволять всем желающим изменять конфигурацию (а просматривать ее допустимо и в пользовательском режиме).

Для входа в данный режим нужно воспользоваться командой `enable` в приглашении пользовательского режима и нажать **Enter**, а затем ввести секретный пароль и снова нажать **Enter**. На рис. 8.10 изображен экран терминала после выполнения команды `show running-config`. Приглашение привилегированного режима включает в себя имя маршрутизатора и символ #.

По окончании работы в привилегированном режиме имеет смысл вернуться в пользовательский режим, иначе доступ к конфигурированию маршрутизатора останется открытым для любого, кто окажется за терминалом. Для возврата в пользовательский режим введите команду `disable` и нажмите **Enter**. Если вы хотите отключиться от маршрутизатора, напечатайте `logout` и также нажмите **Enter**. Следующему желающему поработать с консолью придется заново вводить пароль (если таковой установлен) для входа в пользовательский режим.

Рис. 8.10. Привилегированный режим позволяет подробно просматривать конфигурацию и предоставляет доступ в режим конфигурации

Режим конфигурации

В режиме конфигурации разрешается изменять все параметры аппаратного и программного обеспечения маршрутизатора: настраивать интерфейсы, маршрутизируемые протоколы и протоколы маршрутизации, а также устанавливать пароли и конфигурировать протоколы глобального взаимодействия, применяемые интерфейсами последовательного соединения. Некоторые из этих параметров можно определить и в диалоговом режиме настройки системы. Режим конфигурации предоставляет доступ ко всем настройкам маршрутизатора.

Вход в режим конфигурации осуществляется из привилегированного режима посредством команды `config`. Рассмотрим команды глобального конфигурирования, позволяющие изменять имя маршрутизатора и пароли различных уровней доступа:

1. В приглашении привилегированного режима наберите `config` и нажмите **Enter**.
2. На вопрос, откуда будет осуществляться конфигурирование: с терминала, из памяти или из сети – по умолчанию предлагается ответ «с терминала», поэтому просто нажмите **Enter**.
3. Чтобы изменить имя маршрутизатора, введите команду `host-name [name]`, подставив вместо `[name]` новое имя. Завершите ввод нажатием клавиши **Enter**. В приглашении появится новое имя маршрутизатора (рис. 8.11).

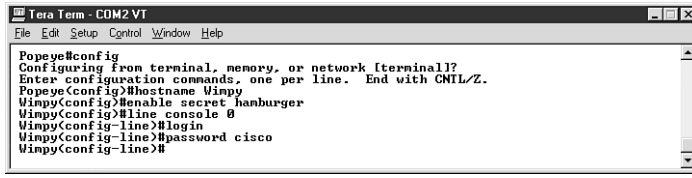


Рис. 8.11. В режиме конфигурации можно изменить имя маршрутизатора и установить пароли

4. Для установки пароля доступа к режиму настроек (то есть к привилегированному режиму) впишите `enable secret [password]`, где `[password]` – это новый пароль. Нажмите **Enter**. В нашем примере паролем является слово `hamburger` (см. рис. 8.11).
5. Теперь можно задать пароль маршрутизатора. Каждый, кто будет подключаться к маршрутизатору, должен будет ввести пароль даже для входа в пользовательский режим. Для установки пароля войдите в режим линии консоли, наберите `line console 0` и нажмите **Enter**.
6. В режиме конфигурации консоли напечатайте `login` и нажмите **Enter**.
7. Введите команду `password [password]`, где вместо `[password]` укажите новый пароль, и нажмите **Enter**. В нашем примере паролем служит слово `cisco` (см. рис. 8.11).
8. Выполнив все эти действия, нажмите **Ctrl**+**Z**. Изменения будут сохранены в текущей конфигурации, и вы вернетесь в привилегированный режим.

Модифицировав текущую конфигурацию (`running-config`), вы, вероятно, захотите сохранить ее как стартовую (`startup-configuration`) в памяти NVRAM, которая загрузится при перезапуске маршрутизатора. Для этого в привилегированном режиме введите `copy running-config startup-config` и нажмите **Enter**. На экране консоли отобразится новая стартовая конфигурация.

Замена потерянного пароля

Случается, что пароль для входа в привилегированный режим и изменения конфигурации не удается вспомнить. В таком случае его можно заменить:

1. Выключите маршрутизатор и, подождав несколько секунд, снова включите. Во время загрузки нажмите **Ctrl**+**Break**.
2. Маршрутизатор войдет в режим контроля ПЗУ. Введите `e/s2000002` и нажмите **Enter**. Запишите появившийся на экране номер виртуальной конфигурации.
3. Наберите `o/r0x2142` (эта команда задает игнорирование конфигурации, записанной в NVRAM) и нажмите **Enter**. В следующем приглашении впи-

шите `i` и снова нажмите **Enter**. Маршрутизатор перезагрузится, после чего запустится программа конфигурации. Выберите ответ **No** и нажмите **Enter**.

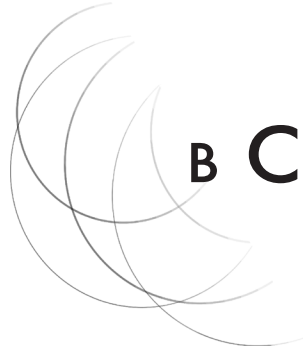
4. В приглашении воспользуйтесь командой `enable` для входа в привилегированный режим. Введите `copy startup-config running-config` и нажмите **Enter**. Исходная конфигурация будет переписана в ОЗУ маршрутизатора.
5. В приглашении привилегированного режима укажите `config`. Войдя в режим конфигурации, наберите `enable secret [new password]`, где `[new password]` – новый секретный пароль.
6. В приглашении режима конфигурации наберите `config-register 0x`, а затем номер виртуальной конфигурации (тот, который вы записали в пункте 2). Нажмите **Enter**.
7. Наберите `end` и нажмите **Enter**, чтобы выйти из режима конфигурации. Перезагрузите маршрутизатор. Вы установили новый секретный пароль, и маршрутизатор снова должен нормально работать[1].

Знание различных режимов и соответствующих команд является чрезвычайно важным аспектом общего управления маршрутизатором. В следующей главе вы познакомитесь с системой Cisco IOS и структурой ее команд. Режимы, описанные выше, будут рассматриваться в контексте системных команд.

Здесь не рассказывалось о пароле виртуального терминала, который используется для соединения с маршрутизатором посредством программы Telnet (см. главу 11, раздел «Применение Telnet»). Чтобы изменить данный пароль, в приглашении режима конфигурации введите ***line vty 0 4*** *и нажмите* ***Enter****. В режиме конфигурации виртуального терминала наберите* ***login*** *и снова нажмите* ***Enter****. Затем воспользуйтесь командой* ***password [password]****, где вместо* ***[password]*** *следует указать новый пароль. Завершите сеанс конфигурации нажатием клавиш* ***Ctrl+Z****.*

[1] Подавляющее большинство приводимых в настоящей книге команд может применяться во всех версиях Cisco IOS. Однако некоторые командные конструкции являются специфическими, поэтому прежде чем применять то или иное выражение следует свериться с документацией по вашему устройству Cisco или обратиться к встроенной в Cisco IOS справке. – *Прим. научн. ред.*

ГЛАВА 9



Работа в Cisco IOS

Операционная система межсетевого взаимодействия Cisco IOS (Internetworking Operating System) позволяет аппаратному обеспечению маршрутизатора управлять пакетами. IOS, как любая операционная система, включает в себя набор команд и функций для контроля и настройки маршрутизатора, а также поддерживает выполнение различных протоколов.

Сконфигурировать маршрутизатор – значит задействовать те или иные протоколы и интерфейсы с помощью системных команд. Нужно также предоставить информацию для маршрутизируемых протоколов, таких как IP или IPX/SPX. Необходимо настроить и протоколы маршрутизации, например RIP или IGRP. После того как маршрутизатор сконфигурирован, требуется управление файлами конфигурации. Рассмотрим некоторые задачи системы IOS:

- настройка интерфейсов локального взаимодействия производится после установления физических соединений. Интерфейсы маршрутизатора должны быть сконфигурированы для применения в локальных и глобальных сетях. Так, если предполагается маршрутизация IP, каждый используемый интерфейс Ethernet должен иметь соответствующий IP-адрес и маску подсети;
- настройка последовательных интерфейсов и протоколов глобального взаимодействия делается в случаях подсоединения к выделенной линии или другому типу межсетевой связи;
- управление конфигурационными файлами осуществляется после того, как маршрутизатор настроен. Текущая конфигурация записывается в NVRAM и становится стартовой. Рекомендуется создать копии файла конфигурации. Конфигурационный файл можно сохранить на сервере TFTP и при необходимости загружать оттуда (см. главу 17);
- контроль и поддержка маршрутизатора производится командами системы IOS, предназначенными для анализа и устранения проблем, а также для обновления системы.

Список может показаться исчерпывающим, но на самом деле это далеко не так. Набор команд системы Cisco IOS огромен и способен стать предметом рассмотрения нескольких книг. Компания Cisco публикует полные списки команд для каждой версии IOS, и объем этих изданий сравним с телефонным справочником Нью-Йорка: например, перечень команд системы IOS 11.3 занимает более тысячи страниц. Однако даже профессионалы, работающие с маршрутизаторами высокого класса в крупных сетях, используют лишь небольшую их часть.

Cisco предоставляет пользователю *интерфейс командной строки* (command-line interface – CLI), в котором можно конфигурировать маршрутизатор и управлять им. Работать в интерфейсе командной строки можно с консоли или через программу Telnet, с виртуального терминала.

Ниже в общих чертах будет рассмотрена система IOS и интерфейс CLI. Команды, относящиеся к конфигурированию протоколов и интерфейсов, описываются в следующих главах.

Если вы пользуетесь операционными системами DOS или UNIX, интерфейс CLI покажется вам знакомым. В противном случае обратите особое внимание на иллюстрации, поясняющие обсуждаемые команды. Вы увидите, что структура команд достаточно проста.

➢ Протоколы маршрутизации (RIP, IGRP) рассматривались в главе 8 (раздел «Конфигурирование маршрутизируемых протоколов»). Перечень основных команд приводится в приложении 1.

Структура команд

В главе 8 уже рассказывалось о некоторых системных командах применительно к различным режимам маршрутизатора: пользовательскому, привилегированному и конфигурационному. В каждом из этих режимов имеется свой набор команд:

- в пользовательском режиме предоставляются только основные команды просмотра системной информации и выполнения базовых проверок;
- привилегированный режим обладает большим набором команд, с помощью которых можно получать информацию о маршрутизаторе и входить в режим конфигурации;
- в режиме конфигурации разрешается пользоваться командами для конфигурирования интерфейсов и протоколов, применяемых маршрутизатором.

➢ Режимы маршрутизатора детально описываются в главе 8 (раздел «Режимы маршрутизатора»).

Команды интерпретатора Exec

В системе Cisco IOS для обработки и выполнения команд задействован командный интерпретатор *Exec*. Пользовательский и привилегированный режимы считаются

различными уровнями интерпретатора; команды здесь построены по следующему принципу: команда и параметр маршрутизатора, обозначающий, к чему эта команда применяется.

Например, по команде `show interface Ethernet 0` будут показаны параметры первого интерфейса Ethernet. Для запуска команды необходимо нажимать клавишу **Enter**; результат появится на экране консоли или виртуального терминала. На рис. 9.1 изображен вывод данной команды для маршрутизатора 2505 с системой IOS 11.2.

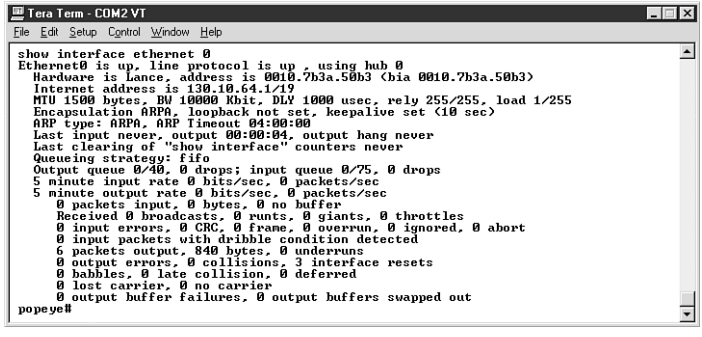


Рис. 9.1. Результат выполнения команды ***show interface Ethernet 0***

> *Хотя режим конфигурации является в определенной степени продолжением привилегированного режима, его команды имеют несколько иную структуру, чем команды интерпретатора Exec. Команды конфигурирования различных протоколов будут рассмотрены в главах 11–13 и 15.*

Команды режима конфигурации

Если команды интерпретатора Exec представляют собой запросы, состоящие из двух частей, то конфигурационные команды устроены иначе: они включают в себя несколько отдельных команд, совокупность которых изменяет какой-либо параметр интерфейса или протокола. Допустим, требуется выбрать протокол глобального взаимодействия, который будет применяться на конкретном интерфейсе (скажем, Serial 1). Не забывайте, что вход в режим конфигурации производится через привилегированный режим. Конфигурирование протокола глобального взаимодействия для последовательного интерфейса выполняется таким образом:

1. В приглашении привилегированного режима введите `config` и нажмите **Enter**.
2. Задайте источник, откуда будет производиться конфигурирование. Ответ по умолчанию – «с консоли». Нажмите **Enter**.

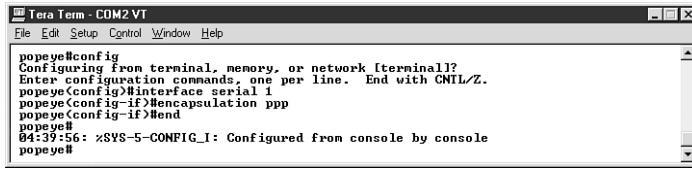


Рис. 9.2. Команды конфигурации обычно выполняются поэтапно

3. Войдя в режим конфигурации, укажите устройство. Для конфигурации интерфейса Serial 1 задайте `interface serial 1` (рис. 9.2).
4. После нажатия клавиши **Enter** приглашение примет вид `<config-if>#`. Это значит, что дальнейшие действия будут касаться конкретного интерфейса, в данном случае Serial 1.
5. Теперь можно воспользоваться командой, которая фактически изменит конфигурацию указанного интерфейса. Чтобы включить, например, протокол PPP, введите `encapsulation ppp`.
6. Разрешается задействовать также дополнительные команды, относящиеся к интерфейсу Serial 1. Завершив изменения, напишите `end` или нажмите клавиши **Ctrl**+**Z**, чтобы выйти из режима конфигурации.

Итак, сначала дается общая команда, потом более конкретная. На первом этапе вы сообщаете системе о своем желании что-то сконфигурировать, а затем говорите, что именно вы хотите сделать. В большинстве случаев конфигурация осуществляется именно так; тем не менее существует несколько специальных команд, выполняемых одной строкой (например, команда `hostname`, позволяющая изменить имя маршрутизатора). Команды конфигурации можно разделить на три категории:

- *глобальные команды*, которые представляют собой самодостаточные, однострочные команды, влияющие на общую (глобальную) конфигурацию маршрутизатора. В качестве примера можно назвать `hostname` и `enable secret`;
- *команды для портов*, позволяющие выбрать интерфейс или контроллер. После таких команд следует подкоманда, которая несет дополнительную информацию, относящуюся к заданному порту или контроллеру. Например, командой, применяемой к порту Serial 0, будет `interface serial 0`;
- *подкоманда*, которая содержит конкретное указание для выбранного порта или контроллера. Например, чтобы назначить последовательному интерфейсу IP-адрес, нужно ввести команду `IP Address`, а затем задать конкретный IP-адрес и маску подсети.

Ниже в этой и последующих главах проанализированы примеры работы в конфигурационном режиме для настройки таких протоколов, как IP, IPX и AppleTalk.

При конфигурации протоколов глобального взаимодействия для последовательных интерфейсов применяется команда инкапсуляции протокола. Инкапсуляция – это упаковка данных в пакет определенного формата. Например, пакеты Ethernet вкладываются в кадры с заголовками Ethernet и в таком виде передаются по сети. Если кадр Ethernet требуется передать по межсетевому соединению, то он помещается в кадр другого формата, соответствующего протоколу глобального взаимодействия, такому как PPP или HDLC. Инкапсуляция рассматривается в главах 10 и 15.

Помощь в IOS

В любом режиме система IOS может предоставить помощь. Допустим, вы находитесь в пользовательском режиме и хотите просмотреть список доступных команд. Введите `?` и нажмите **Enter**. На рис. 9.3 показан перечень команд, который вы увидите на экране консоли.

Далее вы решаете использовать определенную команду, но не знаете, каким образом ее следует запускать. Например, вам нужна команда `show`. Наберите `show` (или любую другую команду, информацию о которой вы хотите получить) и затем `?`, не забыв поставить между ними пробел (иначе команда будет воспринята как неверная), и нажмите **Enter**. На экране появится подсказка по применению данной команды (рис. 9.4).

После вывода запрошенных сведений нужная команда автоматически помещается в приглашение (см. рис. 9.4). Вам остается указать дополнительные параметры и на-

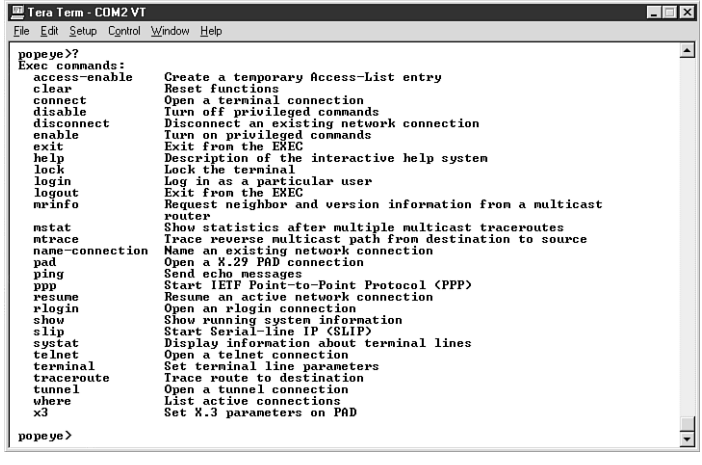


Рис. 9.3. Для получения сведений о командах введите ?

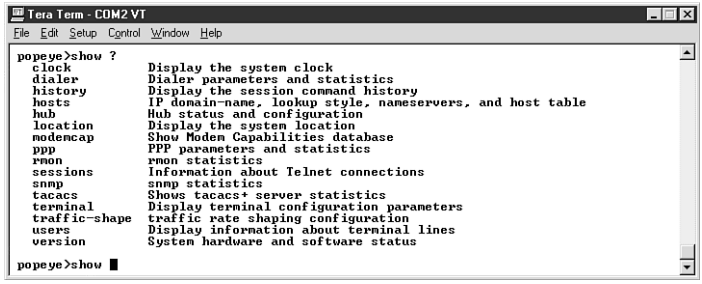


Рис. 9.4. Подсказка по работе с командой

жать **Enter** для запуска команды. Например, можно задать параметр `version` для просмотра версии установленной операционной системы (рис. 9.5).

Как отмечалось ранее, система подсказок доступна также в привилегированном и конфигурационном режимах. Помощь в привилегированном режиме похожа на помощь в пользовательском: общая информация выводится командой `?`, а подсказки по командам – именем команды и `?` (через пробел).

На рис. 9.6 изображен результат запроса необходимых сведений в привилегированном режиме. Обратите внимание: здесь предоставляется больше команд, чем в пользовательском режиме (поскольку этот режим характеризуется расширенным уровнем доступа).

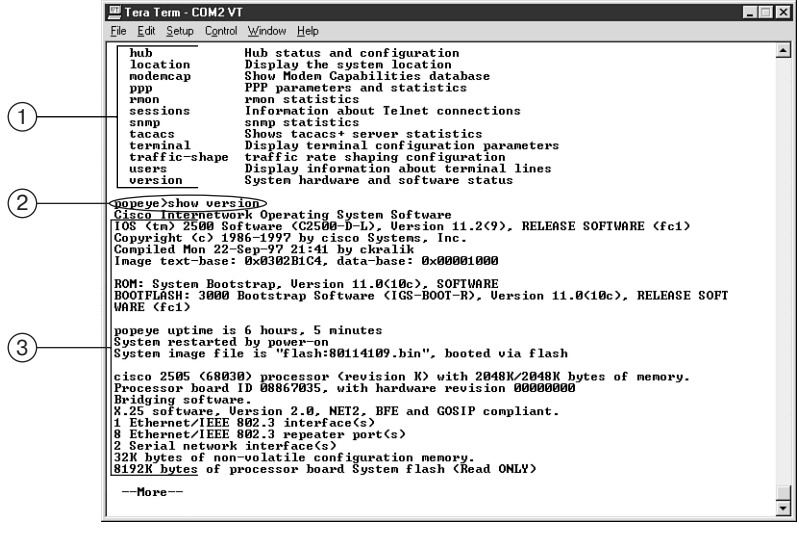


Рис. 9.5. Система помощи позволяет правильно ввести команду:
1 – помощь; 2 – полная команда; 3 – результат выполнения

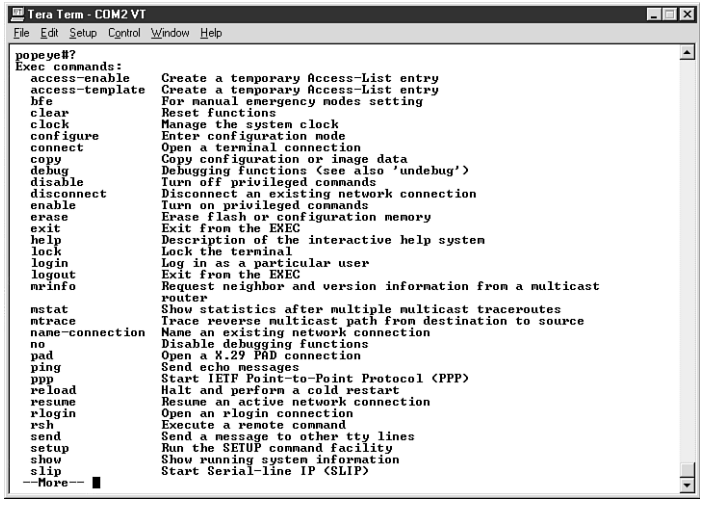


Рис. 9.6. В привилегированном режиме предоставляется больше команд, чем в пользовательском

В конфигурационном режиме также предоставляется помощь. Справку можно получить даже посреди процедуры конфигурирования интерфейса. Введите ?, и вам будет предоставлен список возможных подкоманд (рис. 9.7) для заданной команды порта.

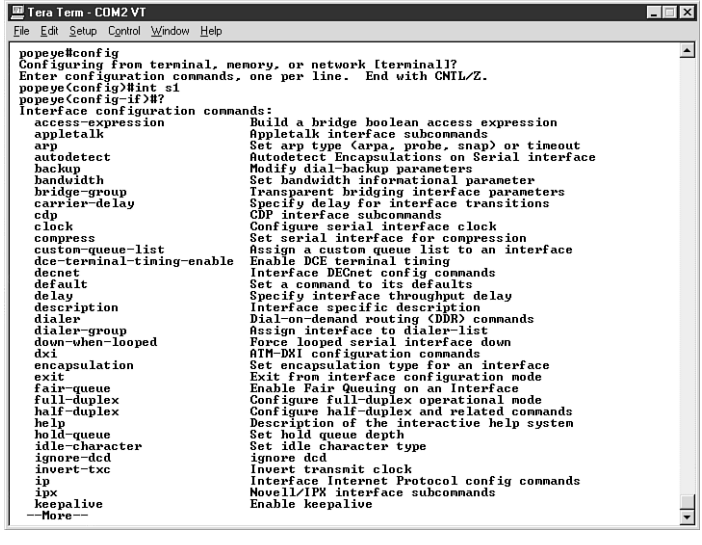


Рис. 9.7. Подсказки в режиме конфигурации

*Если перечень команд не умещается на экране, то внизу появится надпись **More** (Дальше). Чтобы увидеть следующую строчку, нажмите **Enter**, целый экран – клавишу пробела. Если же продолжение списка вас не интересует, нажмите **Esc**.*

Команды просмотра настроек маршрутизатора

В пользовательском и привилегированном режимах ряд команд позволяет просматривать различные установки и параметры маршрутизатора. Одной из наиболее полезных является команда `show`. С ее помощью можно увидеть статус всех интерфейсов маршрутизатора, а также статистику использования памяти и маршрутизируемых в данный момент протоколов.

Итак, команды пользовательского режима являются поднабором команд привилегированного режима. И хотя в первом случае не все доступно для просмотра, о конфигурации маршрутизатора даже в этом режиме можно узнать очень многое.

Допустим, у вас нет пароля доступа к привилегированному режиму. Посмотрим, какие сведения можно получить в пользовательском режиме. В первую очередь следует выяснить, какие имеются интерфейсы.

Команда show interfaces

Введите команду `show interfaces` и нажмите **Enter**. На экране консоли появится результат выполнения этой команды (на рис. 9.8 показан результат для маршрутизатора 2505 с одним портом Ethernet и двумя портами Serial). Так как сводка данных об интерфейсах полностью не помещается на экране, ее можно пролистать при помощи клавиши пробела.

Эта команда позволяет узнать аппаратный адрес (MAC-адрес) и IP-адрес порта Ethernet 0, статус интерфейса (активизирован или нет) и статус протоколов, сконфигурированных для данного интерфейса, количество принятых и отправленных через интерфейс кадров. Кроме того, для порта Ethernet (в Ethernet, напомним, применяется доступ CSMA/CD) приведено число конфликтов и неправильных кадров (с большей или меньшей длиной).

*Если вы допустите ошибку при вводе команды, ее всегда можно исправить. Стереть символ слева от курсора можно с помощью клавиши **Backspace**, для перемещения курсора в начало строки нажмите **Ctrl+A**, в конец – **Ctrl+E**.*

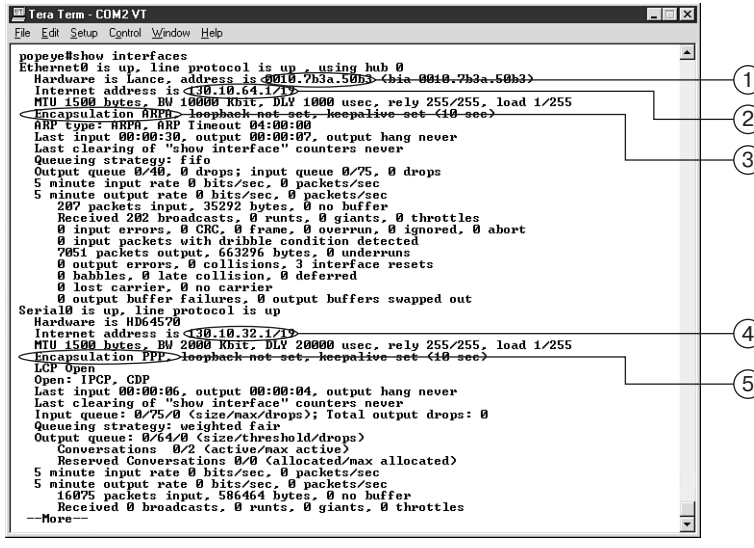


Рис. 9.8. Команда ***show interfaces*** предоставляет информацию об интерфейсах маршрутизатора: 1 – аппаратный адрес порта Ethernet (0010.7b3a.50b3); 2 – IP-адрес порта Ethernet (130.10.64.1/19); 3 – вид инкапсуляции Ethernet (ARPA); 4 – IP-адрес порта Serial (130.10.32.1/19); 5 – вид инкапсуляции Serial (PPP).

Команда `show interfaces` выдает информацию и о других интерфейсах. Так, для порта Serial 0 указывается IP-адрес и тип инкапсуляции (PPP, поскольку именно этот протокол применяется в данном интерфейсе).

Не вся информация об интерфейсах уместилась на экране. При работе с маршрутизатором 2505 следует нажать клавишу пробела, чтобы получить данные об интерфейсе Serial 1 (в маршрутизаторе высокого класса для продолжения можно также использовать клавишу **Enter**).

Если окажется, что команда `show interfaces` предлагает больше информации, чем нужно, а вы хотите получить данные о каком-то определенном интерфейсе, эту команду разрешается использовать иначе.

Получение сведений о конкретном интерфейсе

Введите `show interface Ethernet 0` и нажмите **Enter**. Теперь на экране появится информация, касающаяся только порта Ethernet 0.

Команда `show` может применяться и для сбора других данных о маршрутизаторе. В табл. 9.1 приведены некоторые команды просмотра, доступные в пользовательском режиме (и тем более в привилегированном).

Таблица 9.1. Команда ***show*** *в пользовательском режиме*

Команда	Сведения
`show clock`	Установка даты и времени
`show version`	Версия операционной системы IOS
`show protocols`	Сконфигурированные протоколы
`show processes`	Информация об использовании процессора
`show history`	Список последних десяти команд
`show hub`	Статус портов концентратора в маршрутизаторе 2505

Существуют и другие команды просмотра, некоторые из них будут описаны в следующих главах.

➢ Подробнее о применении команды `show` для просмотра параметров протокола IP рассказывается в главе 11 и 13, протокола IPX – в главе 12.

Во многих случаях разрешается пользоваться сокращенными командами. Например, вместо ***show*** *можно вводить* ***sh****, а вместо* ***interface Ethernet 0*** *–* ***int E0****. Таким образом, команду* ***show interface Ethernet 0*** *допустимо записывать в виде* ***sh int E0****. Пробуйте применять свои сокращения команд. Если ваш вариант не предусмотрен, интерпретатор просто не примет такую запись, сообщив, что команда неверна или неполна.*

Работа в привилегированном режиме

В привилегированном режиме доступны те же команды просмотра, что и в пользовательском, а также некоторые другие (см. следующий раздел). Привилегированный режим позволяет получить более полную информацию о конфигурации маршрутизатора и установить параметры операционной системы (помните, что для входа в режим конфигурации нужно находиться в привилегированном режиме).

Здесь, например, можно задать дату и время:

1. Введите команду `enable` и нажмите **Enter**.
2. Укажите пароль для входа в привилегированный режим.
3. Наберите команду `clock set`, а затем время, день, месяц и год. Пример: `clock set 21:43:05 13 June 1999` (рис. 9.9).
4. Нажмите **Enter**.
5. Для просмотра новых установок воспользуйтесь командой `show clock` и снова нажмите **Enter**.

Некоторые команды привилегированного режима используются достаточно часто. К их числу относится, например, команда `show cdp neighbors`, предна-

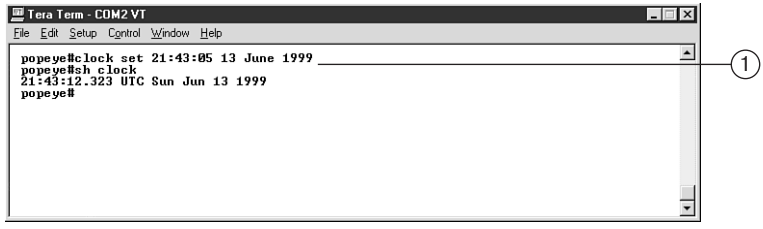


Рис. 9.9. Установка времени и даты: 1 – команда ***clock set***

значенная для исследования сетевого окружения (см. раздел «Просмотр сетевого окружения»).

Проверка памяти маршрутизатора

Во время конфигурирования различных протоколов и интерфейсов конфигурационные данные записываются в ОЗУ маршрутизатора. Эту информацию необходимо где-то сохранить на случай, если маршрутизатор выключится. В привилегированном режиме текущую конфигурацию можно поместить в NVRAM, где она станет стартовой.

Привилегированный режим также позволяет просматривать содержимое ОЗУ и NVRAM с помощью команды `show` с соответствующими подкомандами. Эти команды недоступны в пользовательском режиме.

Чтобы увидеть текущую конфигурацию, выполните следующие действия:

1. Введите команду `enable` и нажмите **Enter**.
2. Укажите пароль для входа в привилегированный режим.
3. Наберите `show running-config` и снова нажмите **Enter** (на рис. 9.10 показан результат выполнения команды).
4. Просмотреть всю информацию можно с помощью клавиши **Enter** (построчное пролистывание) или пробела.

Текущая конфигурация представляет собой информацию о том, как в данный момент настроены различные интерфейсы и какие протоколы задействованы. Она также содержит данные о паролях, установленных на маршрутизаторе (следует помнить, однако, что секретный пароль привилегированного режима зашифрован). Команда `running-config` применяется для получения полного перечня параметров маршрутизатора, поэтому она работает только в привилегированном режиме: эти сведения важны при администрировании маршрутизатора и должны быть защищены.

После настройки текущую конфигурацию надо сохранить в NVRAM, чтобы использовать как стартовую. С помощью команды `copy` ее можно переписать из ОЗУ в NVRAM (то есть сделать стартовой) или из NVRAM в ОЗУ.

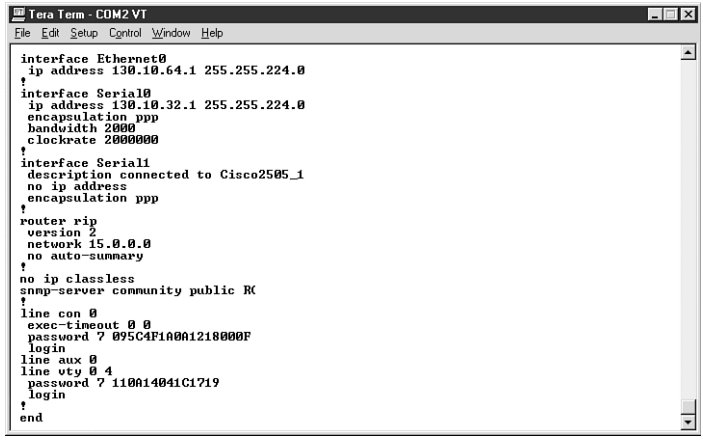


Рис. 9.10. Команда ***show running-config*** позволяет увидеть текущую конфигурацию

Копирование текущей конфигурации

Находясь в привилегированном режиме, наберите `copy running-config startup-config` и нажмите **Enter**. Для копирования потребуется определенное время, в течение которого на экране будет отображаться сообщение **Building configuration** (Создание конфигурации). Когда запись завершится, на экране появится сообщение **[OK]**. Проверить стартовую конфигурацию можно с помощью команды `show startup-config`, результат выполнения которой похож на результат выполнения команды `show running-config` (см. рис. 9.10). Кроме того, вы узнаете объем памяти NVRAM, отведенной под хранение конфигурации.

Другим видом памяти маршрутизатора является флэш-память, в которой находится операционная система IOS. Содержимое флэш-памяти можно просматривать как в привилегированном, так и в пользовательском режиме.

Просмотр флэш-памяти

Находясь в привилегированном или пользовательском режиме, наберите `show flash` и нажмите **Enter** (рис. 9.11). На экране появится имя файла IOS и объем свободной и занятой памяти.

> *С помощью клавиш управления курсором ↑ и ↓ можно вернуться к любой из десяти последних команд. Чтобы повторить ее выполнение, достаточно нажать* ***Enter****.*

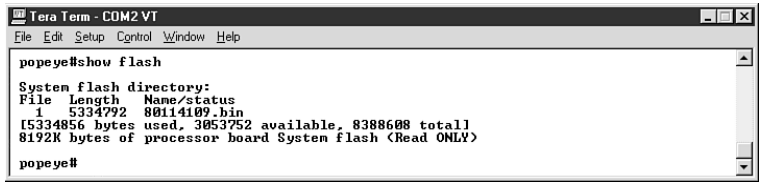


Рис. 9.11. По команде ***show flash*** выводятся сведения о файле IOS и о свободном и занятом пространстве флэш-памяти

Закончив работу в привилегированном режиме, не забудьте выйти из него при помощи команды ***disable****: так вы защитите маршрутизатор от посторонних.*

Прежде чем сохранить новую текущую конфигурацию в виде стартовой, ее можно проверить посредством команд ***show*** *и* ***debug****. Разрешается также создать резервную копию стартовой конфигурации на сервере TFTP, после чего записать новую конфигурацию в NVRAM (см. главу 17).*

Просмотр сетевого окружения

При работе с интерсетями важно иметь сведения о маршрутизаторах, напрямую связанных с вашим, – их обычно называют *соседями*. Маршрутизаторы Cisco применяют собственный *протокол обнаружения* (cisco discovery protocol – CDP), предоставляющий доступ к информации о соседях. В протоколе CDP для обнаружения соседних маршрутизаторов Cisco, также использующих CDP, задействуются широковещательные запросы канального уровня. (В IOS 10.3 и более новых версиях CDP включается автоматически.)

Работа с CDP

Прежде чем начать сбор данных о соседних маршрутизаторах с помощью CDP, необходимо посредством команды `show cdp interface` убедиться, что этот протокол включен на интерфейсах маршрутизатора.

Просмотр интерфейсов CDP

Находясь в привилегированном или пользовательском режиме, наберите `show cdp interface` и нажмите **Enter**. На рис. 9.12 показан результат выполнения этой

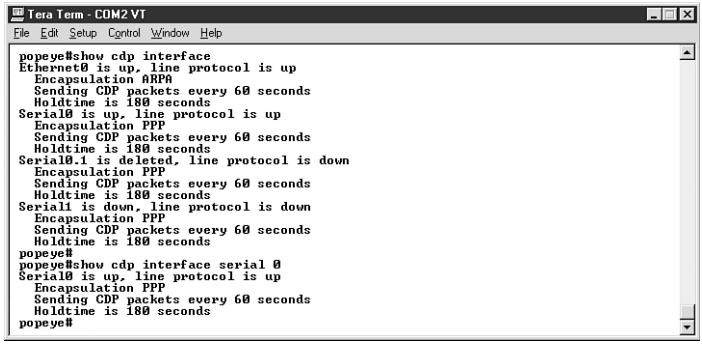


Рис. 9.12. Команда ***show cdp interface*** показывает, на каких интерфейсах включен протокол CDP

команды: на экран выводится информация о протоколе CDP для всех интерфейсов маршрутизатора.

Можно также получить сведения о протоколе CDP для отдельно взятого интерфейса. Например, как показано на рис. 9.12, ввести команду `show cdp interface s0`, предоставляющую данные только о порте Serial 0. Также здесь имеется информация, касающаяся интервала посылки пакетов CDP и времени удержания CDP. Широковещательные запросы CDP посылаются каждые 60 с.

Время удержания – это интервал, в течение которого маршрутизатор должен хранить информацию, полученную от соседа. Если эти сведения не обновляются в течение 180 с, маршрутизатор удаляет устаревшие данные.

CDP применяется для того, чтобы маршрутизатор был в курсе состояния соседних устройств. Когда происходит обрыв линии или возникает какая-то другая проблема, не имеет смысла полагаться на прежнюю информацию при маршрутизации данных.

> *Удалить содержимое флэш-памяти можно с помощью команды **erase** в привилегированном режиме. Разрешается также загрузить новую версию IOS с сервера TFTP командой **copy** (см. главу 17).*

Если на каком-нибудь интерфейсе протокол CDP не включен, это можно сделать в режиме конфигурации следующим образом:

1. Находясь в привилегированном режиме, введите команду `config terminal` (Конфигурация с консоли).
2. В приглашении режима конфигурации укажите тип интерфейса, для которого будет задействован CDP (например, `interface serial 0`). После нажатия клавиши **Enter** приглашение примет вид `<config-if>#`, то есть далее будут запрашиваться команды конфигурации указанного интерфейса.
3. Наберите команду `cdp enable`.

4. Чтобы завершить конфигурацию интерфейса и вернуться в привилегированный режим, нажмите клавиши **Ctrl+Z** (рис. 9.13).

Протокол CDP является платформонезависимым: он собирает информацию о соседних маршрутизаторах вне зависимости от того, какие протоколы они маршрутизируют.

Время удержания допустимо установить вручную в режиме конфигурации, воспользовавшись командой ***cdp holdtime [seconds]****, где вместо* ***[seconds]*** *указано время в секундах.*

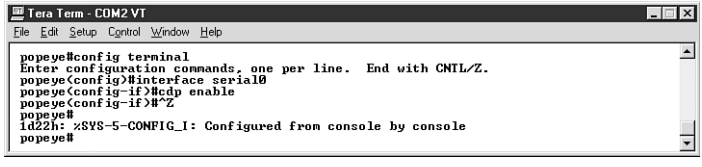


Рис. 9.13. Разрешить применение CDP на интерфейсе довольно легко

Просмотр состояния соседних маршрутизаторов

Проверив состояние протокола CDP на различных интерфейсах вашего маршрутизатора, можно приступить к сбору информации о платформах и протоколах соседних устройств.

Сбор информации о соседних маршрутизаторах

Находясь в привилегированном или пользовательском режиме, наберите `show cdp neighbors` и нажмите **Enter**. На рис. 9.14 показан результат выполнения этой команды для маршрутизатора 2505, у которого есть только один сосед, подключенный через последовательный порт. В табл. 9.2 приводятся пояснения к рисунку.

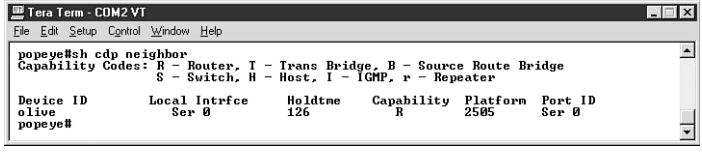


Рис. 9.14. Команда ***show cdp neighbors*** позволяет просматривать сетевое окружение и состояние соседних маршрутизаторов

Таблица 9.2. Команда `show` в пользовательском режиме

Параметр	Обозначение	В данном примере
Device ID	Имя соседнего устройства	Olive
Local Interface	Интерфейс вашего маршрутизатора, к которому подключен соседний маршрутизатор	Serial 0
Capability	Сконфигурирован ли маршрутизатор на выполнение нескольких функций: маршрутизация (R), мост (B), коммутация (S)	R (маршрутизатор выполняет только маршрутизацию)
Platform	Тип маршрутизатора Cisco	2505 (имеется в виду соседнее устройство)
Port ID	Интерфейс соседнего маршрутизатора, через который он подключен к вашему	Serial 0

Разумеется, если вы работаете с маршрутизатором высокого класса, к которому подсоединено множество различных соседей, то и информация, предоставляемая командой `show cdp neighbors`, будет гораздо более полной.

Можно также воспользоваться командой `show cdp neighbors details`, которая доступна в пользовательском и привилегированном режимах. Она позволяет узнать IP-адрес соседнего интерфейса и версию системы IOS, установленной на соседнем маршрутизаторе.

Команда ping

При работе с маршрутизаторами очень полезной бывает команда `ping` (Packet InterNet Groper), которая используется для проверки связи между узлами в сети – компьютерами, серверами или маршрутизаторами.

Эта команда применяется с такими протоколами сетевого уровня, как IP, IPX и AppleTalk, и задействует логическую адресацию узлов (см. также главу 18). На маршрутизаторе можно тестировать различные интерфейсы, поскольку в большинстве случаев каждому интерфейсу предоставляется свой логический адрес.

Допустим, вы хотите проверить, установлена ли связь с соседним маршрутизатором. Для этого нужно только проанализировать его интерфейс.

Тестирование соседей

Находясь в пользовательском или привилегированном режиме, наберите `ping [ip address]`, где вместо `[ip address]` следует указать IP-адрес интерфейса маршрутизатора Olive, подсоединенного к вашему маршрутизатору. В данном случае команда будет выглядеть так: `ping 130.10.32.2`. Результат выполнения представлен на рис. 9.15: успешно доставлено 100% пробных пакетов. Если сообщения не дошли до узла, этот показатель составит 0%.

➢ Для связи с другими маршрутизаторами можно также воспользоваться программой Telnet. Подробнее об этом рассказывается в разделе «Использование протокола Telnet» (глава 11).

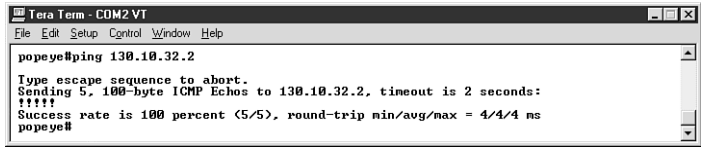


Рис. 9.15. Команда ***ping*** позволяет проверить наличие связи с тем или иным маршрутизатором

Работу протокола CDP можно прекратить с помощью команды ***no cdp run****, которая отключит его на всех интерфейсах. Чтобы запретить CDP на отдельном интерфейсе, нужно войти в режим конфигурации, выбрать интерфейс и ввести команду* ***no cdp enable****. Для общего включения CDP применяется команда* ***cdp run*** *(в привилегированном режиме).*

Создание приветствия маршрутизатора

Выше рассказывалось о пользовательском и привилегированном режимах работы системы Cisco IOS и некоторых полезных командах. Прежде чем приступить к рассмотрению режима конфигурации на примере конфигурирования различных протоколов, обратимся к одному из его применений – созданию приветственного обращения, которое будет появляться на консоли при загрузке или перезагрузке маршрутизатора, а также на экранах подключенных терминалов.

Приветствие создается в режиме конфигурации с помощью команды `banner motd [end character]`, где вместо `[end character]` указывается символ окончания сообщения, который вы можете выбрать сами. Допустимы такие символы, как `#`, `$` или любые другие, не встречающиеся в основном тексте.

Приветствие формируется следующим образом:

1. Находясь в привилегированном режиме, введите команду `config terminal` (Конфигурация с консоли).
2. В данном примере символом окончания приветствия выбран знак `$`. Наберите команду `banner motd $` и нажмите **Enter**.
3. Впишите текст приветствия. С помощью клавиши **Enter** можно создавать пустые строки, а смещать текст в строке удобно посредством пробелов (рис. 9.16).
4. Завершив набор текста, введите символ окончания (в данном случае `$`) и нажмите **Enter**. Вы вернетесь в режим конфигурации.
5. Нажмите клавиши **Ctrl**+**Z** для выхода из режима конфигурации.

После выхода из режима конфигурации снова нажмите **Enter**, чтобы вернуться в привилегированный режим. Если вы хотите просмотреть приветствие, введите

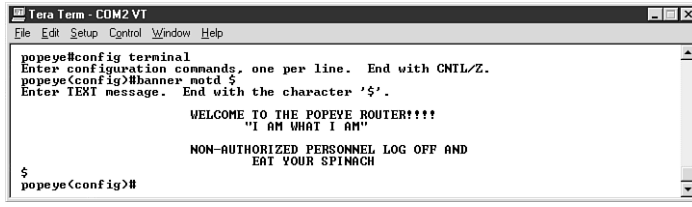


Рис. 9.16. Приветствие создается в режиме конфигурации

команду `quit` и отключитесь от маршрутизатора. После того как вы нажмете **Enter**, чтобы опять подсоединиться к маршрутизатору, на экране появится текст приветствия (рис. 9.17). Если вход на маршрутизатор запаролен, надо будет указать пароль.

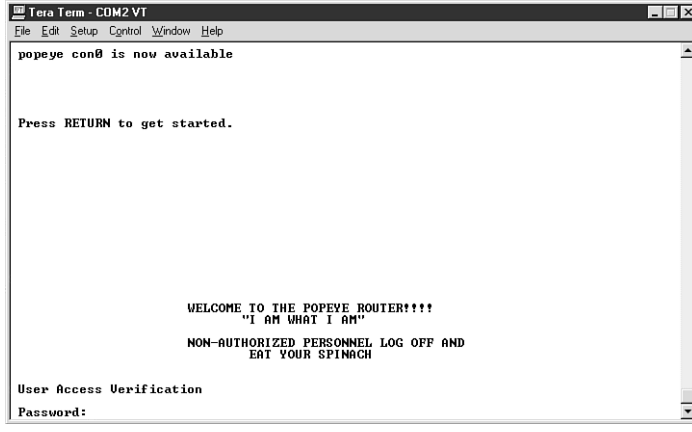


Рис. 9.17. Приветствие появится на экране при подключении к маршрутизатору

Итак, Cisco IOS обладает огромным набором команд (основные команды описаны в приложении 1). Команды, которые часто используются, запоминаются легко, и вам лишь время от времени придется справляться о других, применяемых реже.

➢ Подробнее об установке паролей в режиме конфигурации говорилось в главе 8 (раздел «Режим конфигурации»).

ЧАСТЬ III

Маршрутизация протоколов локальных сетей

ГЛАВА 10

Работа со стеком протоколов TCP/IP

Протокол TCP/IP – это общепринятый сетевой стандарт и наиболее распространенный протокол в сетях компаний. Кроме того, он является базовым для глобальной сети Internet. Многие *сетевые операционные системы* (network operating systems – NOS), такие как Windows NT 4.0 Server, Windows 2000 Server и Novell NetWare 5.0, применяют TCP/IP в качестве протокола по умолчанию.

В главе 2 уже приводилось краткое описание этого протокола. Изначально TCP/IP разрабатывался как набор протоколов WAN, способный поддерживать связь между различными вычислительными центрами даже в том случае, если бы некоторые из них вышли из строя в ходе ядерной войны. В наше время, когда протокол TCP/IP облегчает пользователям работу в Internet, утверждение о том, что этот пакет был создан Министерством обороны в качестве аварийной системы на случай войны, звучит иронично и немного грустно.

Важно отметить, что данный протокол стал незаменимым для работы и поддержки маршрутизаторов в сети Internet. Администраторы маршрутизаторов Cisco используют протокол Telnet (часть пакета TCP/IP) для связи с другими маршрутизаторами, а еще один протокол того же пакета – TFTP – для копирования и записи файлов конфигурации Cisco и загрузки на маршрутизатор нового программного обеспечения IOS. TCP/IP применяется в большинстве крупных сетей, поэтому знание данного пакета необходимо всем, имеющим дело с маршрутизаторами и сетями.

➢ Более детально протокол TFTP описывается в главе 17. Дополнительная информация о пакете протоколов TCP/IP приведена в главе 2, раздел «Протокол TCP/IP».

Протокол TCP/IP и модель OSI

Стек протоколов TCP/IP появился в 70-е годы XX века – приблизительно на десять лет раньше, чем модель OSI. По этой причине различные протоколы стека TCP/IP не полностью соответствуют определенным уровням модели OSI, хотя протоколы низших уровней (сетевого и канального), такие как IP и ARP, почти

целиком отвечают своим аналогам в модели OSI. Когда был разработан пакет протоколов TCP/IP, Министерство обороны (Department of Defense – DOD) предложило свою модель – *модель DOD*, или *модель DARPA*, которая устанавливала способ функционирования различных протоколов в пакете TCP/IP. Эта модель логически разделяет процесс пересылки данных от узла-отправителя к узлу получателю на четыре уровня (а не на семь, как в модели OSI). На рис. 10.1 демонстрируется соответствие моделей DOD и OSI.

Рис. 10.1. Четыре уровня модели DOD в сравнении с семью уровнями модели OSI

В модели DOD определяется, какую именно функцию выполняют протоколы стека TCP/IP на заданном уровне (аналогично модели OSI). В следующих четырех разделах мы рассмотрим, что происходит на каждом уровне модели, а также протоколы, которые здесь используются. На рис. 10.2 представлен пакет протоколов TCP/IP применительно к модели DOD.

➢ Информация о модели OSI содержится в главе 2.

Уровень приложения

Протоколы этого уровня предоставляют пользовательский интерфейс для различных протоколов и приложений, которые имеют доступ в сеть.

В пакете TCP/IP протоколы уровня приложения (application layer)[1] обеспе-

чивают передачу файлов, вход на другие узлы связи, работу электронной почты, а также мониторинг сети. На данном уровне находятся следующие протоколы:

- *протокол передачи файлов* (file transfer protocol – FTP) обеспечивает передачу файлов от одного компьютера к другому. FTP совмещает в себе полнофункциональное приложение (вы можете загрузить клиентскую часть протокола FTP из сети Internet и с ее помощью пересылать файлы между компьютерами) и протокол, который поддерживается другими приложениями, такими как Web-браузеры;
- *упрощенный протокол передачи данных* (trivial file transfer protocol – TFTP), сокращенная версия протокола FTP, позволяет перемещать файлы без аутентификации (нет необходимости вводить имя пользователя и пароль для установления сеанса с сервером TFTP). TFTP служит для сохранения файлов конфигурации маршрутизаторов Cisco или для обновления IOS маршрутизатора (подробно данный протокол рассматривается в главе 17);
- *простой протокол передачи почты* (simple mail transport protocol – SMTP) осуществляет пересылку почты между двумя компьютерами. Он применяется для отправления и получения электронной почты в Internet;
- *простой протокол управления сетью* (simple network management protocol – SNMP) позволяет собирать общую информацию по сети. Он работает с *программами-агентами* (специальными программами, контролирующими работу сети), чтобы получать данные об узлах, которые подключены к сети. Затем эти данные сравниваются с базовыми. В пакетах программного обеспечения маршрутизаторов Cisco, в частности CiscoWorks, SNMP помогает администраторам обнаруживать неисправности в сети или заблаговременно предотвращать их;
- *протокол для эмуляции терминала* (Telnet) предоставляет возможность подключить локальный компьютер к другому компьютеру или устройству, например маршрутизатору. Локальный компьютер при этом играет роль виртуального терминала и получает доступ к сетевым ресурсам подсоединенного устройства. В главе 11 описано, как использовать протокол Telnet для доступа к удаленному маршрутизатору.

Межузловой уровень

Протоколы *межузлового уровня* (host-to-host layer)[2] обеспечивают управление потоком информации и надежность связи при пересылке данных с компьютера-отправителя на компьютер-получатель. Протоколы этого уровня берут данные

[1] В различных источниках этот уровень называется также прикладным – и для модели OSI, и для модели DOD. – *Прим. научн. ред.*

[2] Межузловой уровень модели DOD соответствует транспортному уровню (transport layer) модели OSI. – *Прим. научн. ред.*

у протоколов уровня приложения и начинают их подготовку к перемещению по сети. На межузловом уровне работают два протокола – TCP и UDP:

- *протокол управления потоком данных* (transport control protocol – TCP) – ориентированный на соединение протокол, который предоставляет *виртуальный канал связи* (virtual circuit) между пользовательскими приложениями компьютера-отправителя и компьютера-получателя. TCP берет данные у протоколов уровня приложения, разбивает их на сегменты и проверяет, правильно ли восстановлена информация после ее получения. Для функционирования этого протокола необходимо, чтобы между двумя компьютерами было установлено синхронизированное соединение, то есть происходил обмен пакетами с определенными номерами последовательности и значениями контрольных битов;
- *протокол пользовательских датаграмм* (user datagram protocol – UDP) – транспортный протокол, реализующий соединение между протоколами уровня приложения, которые не требуют подтверждений и синхронизации (в отличие от протокола TCP). Обращение с этим протоколом максимально упрощено. Пакет данных адресуется на узел-получатель и немедленно туда отправляется. UDP более пассивен, чем протокол TCP, и используется протоколами TFTP и SNMP уровня приложения.

Межсетевой уровень

Межсетевой уровень (internet layer), соответствующий сетевому уровню (network) модели OSI, отвечает за маршрутизацию данных по сети, а также поставляет более высоким уровням модели информацию об адресах. Этот уровень также определяет формат пакета данных, который будет использоваться при перемещении информации по сети Internet. Полностью включает в себя только один протокол – IP; другие протоколы поддерживают систему адресации IP, а также формат пакета данных. Важной задачей данного уровня является привязка логических адресов (таких, как адреса IP) к аппаратным адресам (MAC-адресам) узлов в сети.

На межсетевом уровне работают следующие протоколы:

- *протокол Internet* (Internet Protocol – IP) получает данные с межузлового уровня и преобразует их в пакеты (датаграммы), помечая каждый пакет при помощи IP-адреса отправителя и IP-адреса получателя. IP также трансформирует датаграммы на компьютере-получателе в сегменты для протоколов более высокого уровня. Он не работает с содержимым датаграмм. Единственная задача данного протокола – адресовать датаграммы и отправить их по адресу;
- *протокол разрешения адреса* (Address Resolution Protocol – ARP). Когда протокол IP готовит датаграмму к отправке, он владеет информацией об IP-адресах компьютера-отправителя и компьютера-получателя (эти сведения поступают от протоколов более высокого уровня, таких как Telnet или SMTP).

Кроме того, протоколу IP необходим аппаратный адрес (MAC-адрес) компьютера-получателя, чтобы переправить данные протоколу уровня *доступа к сети* (например, Ethernet). ARP устанавливает соответствие адреса IP аппаратному MAC-адресу. Для этого он посылает запросы с адресом IP компьютера-получателя и узнает от этого компьютера его аппаратный адрес;

- *протокол управления сообщениями в Internet* (Internet Control Message Protocol – ICMP). Это служебный протокол обработки сообщений, рассылаемых маршрутизаторами на компьютеры, которые отправляют данные для маршрутизации. Маршрутизаторы уведомляют компьютер о том, что направление, необходимое для дальнейшей передачи, недоступно или буфер памяти переполнен. Кроме того, ICMP, как и ARP, используется в качестве базовой поддержки для протокола IP.

Датаграмма IP состоит из заголовка IP, который содержит IP-адрес источника датаграммы, IP-адреса пункта назначения (и другой информации протокола IP), а также из данных, предоставленных протоколами более высоких уровней. Эта датаграмма помещается между заголовком уровня MAC (в который входит информация о типе носителя, например Ethernet или Token Ring) и последним полем уровня MAC, включающим в себя проверку CRC. В модели DOD протоколы MAC работают на уровне доступа к сети (network access layer), который описывается в следующем разделе, и на канальном уровне (data link layer) модели OSI. Структура IP-датаграммы показывает, как уровни совместно функционируют, чтобы доставлять данные по назначению.

Пакет протоколов TCP/IP, и в частности протокол IP (RFC 791), полностью описаны в документации RFC (Request For Comments). Эту документацию вы можете найти на некоторых сайтах в сети Internet. Удобнее всего обратиться к архиву RFC штата Огайо (http://www.cis.ohio-state.edu/hyper-text/information/rfc.html) или главному сайту RFC (http://www.csl.sony.co.jp/rfc/). Также полезно произвести поиск в сети Internet при помощи ключевого слова RFC.

Команды маршрутизатора `ping` *и* `traceroute` *работают с сообщениями протокола ICMP. Команда* `ping` *рассматривается в главе 9 (раздел «Работа с системой IOS маршрутизатора»), а* `traceroute` *– в главе 18 (раздел «Устранение неисправностей»).*

➢ Более подробно система логической адресации протокола IP обсуждается ниже в разделе «Работа с подсетями».

Уровень доступа к сети

Уровень доступа к сети (network access layer) состоит из протоколов, которые в качестве входящих данных используют датаграммы протоколов межсетевого уровня и добавляют к ним заголовки, состоящие из нескольких полей, и контрольную сумму. Затем полученные таким образом кадры, представляющие собой набор нулей и единиц, подвергаются модуляции (однозначному переводу в аналоговый сигнал) и поступают через соответствующий интерфейс узла (например, через сетевой адаптер) в среду передачи данных. Об этих протоколах уже говорилось ранее как о протоколах канального уровня в модели OSI. Они определены для таких сетевых архитектур, как Ethernet, Token Ring и FDDI. В главе 2 приведены спецификации по IEEE, в которых описываются различные типы кадров, применяемые названными сетевыми архитектурами.

Поскольку эти протоколы находятся на подуровне MAC (части уровня доступа к сети модели DOD и канального уровня модели OSI), они полностью включены в процесс физической адресации пакетов данных. Физический адрес компьютера указан на его сетевой карте. Интерфейсы Ethernet, Token Ring и FDDI маршрутизатора обладают и адресом MAC, жестко заданным в чипе ROM контроллера интерфейса (интерфейсы серийных портов маршрутизаторов не имеют адресов MAC).

На рис. 10.2 показано, как сопоставить модели OSI и DOD, и представлены уровни модели DOD, на которых работают различные протоколы стека TCP/IP. Далее мы расскажем о роли этих протоколов в маршрутизации.

Каким же образом сопоставляются логическая система адресации протокола IP и аппаратные адреса MAC, которые располагаются на различных узлах связи в сети? Ответ на этот вопрос дается в следующем разделе, содержащем описание адресации протокола IP.

➢ Описание сетевых архитектур вы найдете в главе 1 (раздел «Виды сетевых архитектур»). Подробнее о спецификациях IEEE рассказывалось в главе 2 (раздел «Протокол TCP/IP»).

Работа с адресами протокола IP

Адреса протокола IP имеют длину 32 бита и состоят из четырех восьмибитных *октетов* (каждый октет – это один байт). Пример типичного адреса протокола IP – 200.1.25.7 (в десятичном представлении). Сам адрес IP существует в двоичном виде, что важно учитывать при подсчете количества возможных подсетей.

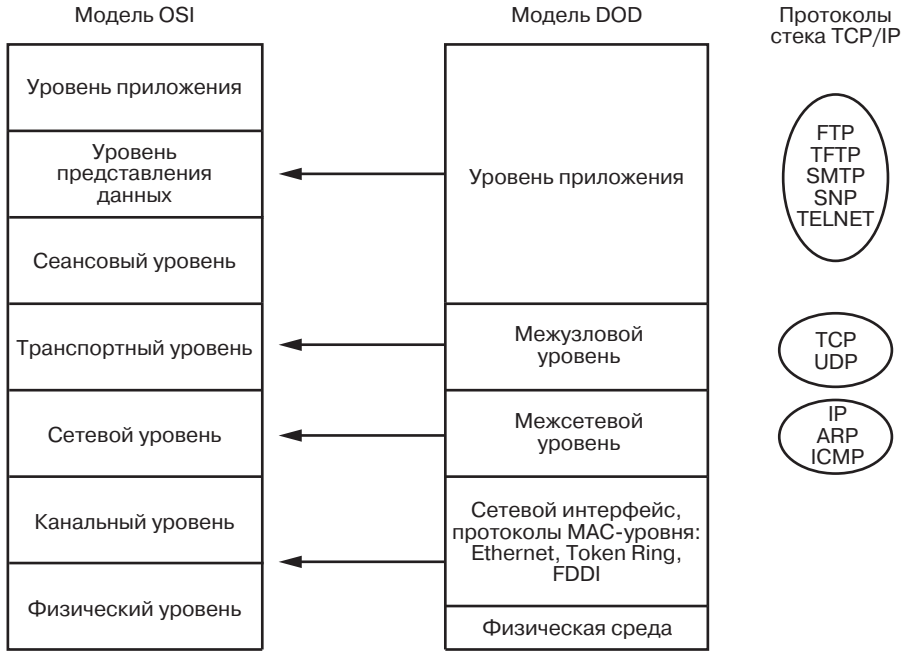


Рис. 10.2. Модель DOD и протоколы пакета TCP/IP применительно к модели OSI

Адрес протокола IP записывается в трех различных формах:

- десятичной: 200.1.25.7;
- двоичной: 11001000 00000001 00011001 00000111;
- шестнадцатеричной: C8 1 19 7.

Адреса протокола IP – это *иерархические адреса*, поскольку они предоставляют различные уровни информации: сообщают, в какой сети и подсети находится узел связи, а также передают сам адрес узла связи. Система адресации протокола IP подобна работе почтовой службы. В письме, адресованном вам, указан номер вашего дома, название улицы, города и страны. В вашем городе и в вашей стране много людей, но по данному почтовому адресу проживаете только вы.

Протокол IP действует аналогично, поэтому в одной части адреса IP указано, в какой сети находится узел связи, в другой – подсеть, а в третьей – адрес самого узла. Такая система адресации упрощает маршрутизацию, поскольку, располагая информацией о сети и подсети, любые маршрутизаторы могут отправлять сообщения на тот маршрутизатор, который обслуживает определенную подсеть (при этом нет необходимости уточнять физический MAC-адрес узла-получателя).

Маршрутизатор, отвечающий за подсеть, получив пакеты для узла, который находится в данной подсети, обеспечивает доставку пакетов по правильному адресу. Он делает это путем установки соответствия адреса IP и аппаратного MAC-адреса

компьютера-получателя. Такая операция подобна работе почты: если вы живете, например, в Калифорнии, письмо с Восточного побережья США будет отправлено на промежуточный почтамт, расположенный на Среднем Западе, и в конце концов придет в нужное почтовое отделение. Там адрес на письме будет сопоставлен с вашим домашним адресом, а затем письмо доставят вам домой.

Адрес IP включает в себя адрес сети, следовательно, маршрутизатору необходимо лишь знать, как доставить пакеты по адресу этой сети, причем в процессе перемещения пакетов данных по сети Internet маршрутизатор-отправитель получает информацию о местонахождении пункта назначения.

> ***Альтернативой иерархической системе адресации IP могла бы стать простая система адресации (все компьютеры с сетевыми картами имеют уникальные MAC-адреса). Однако в таком случае компьютерам пришлось бы запоминать[1] все уникальные MAC-адреса в мире, что технически невозможно. Применение подобной методики было бы так же абсурдно, как присвоение индивидуального номера каждому человеку при адресации письма. Доставка такого письма по назначению потребовала бы колоссальных усилий от почтовой службы.***

При работе с адресами IP должно быть известно, какая часть адреса указывает на подсеть, а какая – на адрес узла связи. В следующем разделе описываются различные классы адресов IP, а также *маски подсети*, которые используются в системе адресации протокола IP.

Классы адресов IP

Адреса IP делятся на три класса в зависимости от размера сети, которую они обслуживают:

- *класс A* предназначен для очень крупных сетей и поддерживает более 16 млн адресов узлов связи. Адреса IP имеют такую структуру, что, хотя сети класса A могут обслуживать огромное количество компьютеров-хостов (узлов связи), допускается существование только 127 сетей класса A. Сеть ARPAnet (созданная в самом начале формирования Internet) – типичный пример сети класса A;
- *класс B* используется для средних сетей, например для сетей крупных компаний или учебных заведений. Имеется 16384 адресов сетей класса B, каждая из которых поддерживает свыше 65000 адресов хостов;
- *класс C* подходит для небольших сетей; всего доступно свыше 2 млн сетей этого класса. Такие сети поддерживают не более 254 адресов узлов связи.

[1] И регулярно обновлять. – *Прим. научн. ред.*

Каждому из этих классов требуется определенное количество октетов в адресе IP для обозначения адреса сети и узла. Так, IP-адрес класса A, например 10.5.25.8, отображает адрес сети при помощи первого октета. Это значит, что сеть имеет номер 10. Остальная часть IP-адреса – 5.25.8 – принадлежит адресу хоста[1]. Поэтому в случае, когда в адресе сети имеется только первый октет, количество адресов сетей класса A оказывается сильно ограниченным (так как при одном октете существенно уменьшается число вариантов). В адресе же хоста присутствует три октета, так что комбинаций очень много. Этим и объясняется тот факт, что доступно ограниченное количество сетей класса A, но каждая из таких сетей поддерживает свыше 16 млн адресов хостов.

Поясним сказанное путем сравнения адреса класса C (200.44.26.3) с адресом класса A. Первые три октета адреса класса C обозначают номер сети IP (200.44.26) и только последний октет доступен для назначения адресов узлов. Таким образом, число комбинаций адресов сетей возрастает (при трех свободных октетах для этих адресов), а число комбинаций адресов узлов, напротив, уменьшается (для них остается лишь один октет).

Существует несколько способов обеспечить определенный диапазон адресов IP для вашей компании. Вы можете получить такой адрес у своего Internet-провайдера или же напрямую у Службы регистрации номеров в сети Internet. Более подробная информация доступна по адресу: http://www.arin.net. Кроме того, вам необходимо зарегистрировать доменное имя. На сайте www.internic.net вы найдете дополнительные сведения о регистрации доменного имени (такого, как Microsoft.com или Habraken.net).

В табл. 10.1 показано, что диапазон первого октета для номеров сетей класса A заканчивается числом 126, а диапазон первого октета для номеров сетей класса B начинается со 128. Почему в таблице не указан номер 127? Дело в том, что он зарезервирован для внутреннего тестирования, в процессе которого компьютеры посылают пакеты данных сами себе, не создавая дополнительной нагрузки на сеть.

На рис. 10.3 представлены классы адресов IP и октеты, которые предназначены в каждом из классов для адресов сетей и адресов хостов.

В табл. 10.1 показан диапазон первого октета каждого из классов IP-адресов в десятичном виде; для каждого класса также приводится число доступных сетей и узлов и пример адреса IP.

[1] В книге встречаются два термина: «узел» и «хост», разница между которыми, как правило, несущественна. – *Прим. научн. ред.*

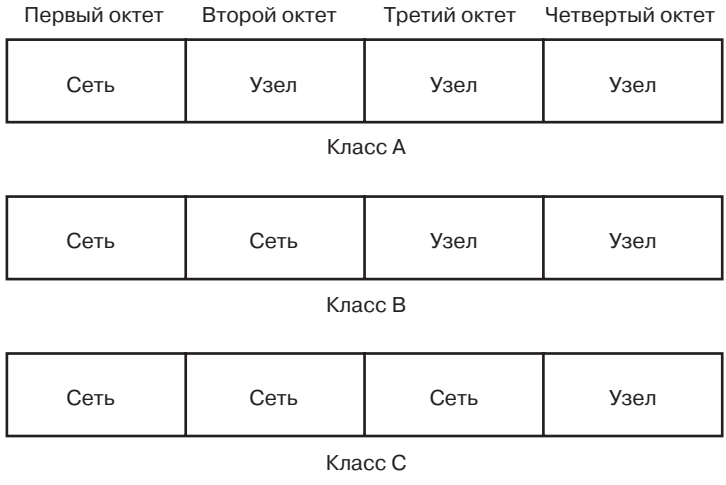


Рис. 10.3. Каждый класс IP-адресов использует определенное число октетов для сетевого адреса и для адресов узлов связи

Таблица 10.1. Классы сетей IP

Класс	Диапазон	Количество сетей первого октета	Количество хостов	Пример адреса
A	1–126	127	16777214	10.15.121.5
B	128–191	16384	65534	130.13.44.52
C	192–223	2097152	254	200.15.23.8

Существуют еще два класса адресов IP: класс D и класс E. Адреса класса D предназначены для сетей, в которые данные поступают от определенного приложения или сервисной службы в Internet. Примером сети с адресами класса D является служба Microsoft NetShow, способная одновременно посылать одну и ту же информацию большому числу пользователей. Адреса класса E относятся к экспериментальному типу, недоступному для обычных пользователей сети Internet.

Двоичные эквиваленты и первые октеты

IP-адрес, такой как 200.1.25.7 (или адрес, который указан в качестве примера в табл. 10.1), представляет собой воспроизведенную в десятичном выражении последовательность из 32 бит, разделенную на четыре октета по 8 бит (что состав-

ляет один байт) в каждом. Поэтому IP-адрес 200.1.25.7 содержит 32 цифры: 11001000 00000001 00011001 00000111.

Ниже, в разделе «Работа с подсетями», мы рассмотрим, каким образом десятичные числа переводятся в двоичные. Пока достаточно знать, что адреса IP записываются в десятичной форме только для удобства, а на самом деле существуют в двоичном представлении как комбинации цифр 1 и 0.

Имеются правила, определяющие, какими должны быть *первые биты* первого октета адресов трех описанных классов (A, B и C). Маршрутизатор может по первому октету адреса IP определить, с каким именно адресом IP он работает (аналогичным образом вы сумеете отличить адреса разных классов друг от друга):

- в классе A первый бит первого октета 0;
- в классе B первый бит первого октета 1, а второй бит 0;
- в классе C первые два бита первого октета 1, а третий бит 0.

На рис. 10.4 показаны первые октеты для адресов классов A, B и C соответственно. Прежде чем описывать процесс перевода адреса из десятичного представления в двоичный и наоборот, рассмотрим маски подсети IP.

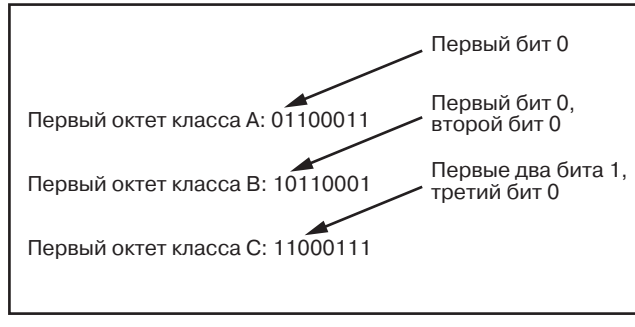


Рис. 10.4. Правило для первого октета позволяет различить классы IP-адресов

*При помощи программы **Калькулятор** Windows вы можете переводить числа из десятичного представления в двоичное и наоборот. Запустите программу Калькулятор (**Пуск** ⇒ **Программы** ⇒ **Стандартные**). Войдите в меню **Вид** и отметьте пункт **Инженерный**. По умолчанию для любого октета адреса IP устанавливается десятичный формат. Затем установите флажок Bin (двоичный формат) в меню форматирования калькулятора: номер будет отображен в двоичной форме – 1111110. Заметьте, что программа в начале номера не ставит цифру 0, поэтому, чтобы получить восьмизначное число, вам необходимо добавить эту цифру: 01111110. Для перевода числа из двоичного кода в десятичный поставьте флажок Bin, введите восьмибитный номер октета, а затем в меню форматирования выберите Dec.*

Базовые маски подсети

Чтобы понять принцип действия системы адресации IP, необходимо освоить применение *маски подсети*, без которой IP-адрес просто не может существовать. Она используется маршрутизатором для определения того, какая часть IP-адреса относится к адресу сети, а какая – к адресу хоста.

В табл. 10.2 указаны базовые маски подсети для всех классов. Они также состоят из четырех октетов. Маршрутизатор сравнивает информацию в маске подсети с адресом IP и задает адрес сети и адрес узла.

Таблица 10.2. Базовые маски подсети

Класс сети	Маска подсети
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Если первый бит октета представлен цифрой 1 в двоичной форме, то в десятичном виде октет имеет значение 128 и выше. Поскольку в адресах класса A первый бит всегда представлен цифрой 0, при переводе в десятичный вид он также будет равен нулю. Поэтому для сетей класса A первый октет обязательно меньше 128 (обратите внимание на диапазон первого октета в десятичном коде для адресов класса A в табл. 10.1).

В базовых масках подсети все биты любого октета равны либо 1, либо 0. Если все восемь бит октета равны единице, то эквивалентом октета в десятичной форме будет число 255, а если нулю – число 0. На рис. 10.5 показан эквивалент базовой маски подсети класса B в двоичном коде.

Маршрутизатор использует маску подсети для нахождения адреса сети по адресу IP при помощи особого метода, который называется *логическим умножением*. Логическое умножение производится так: маршрутизатор просматривает адрес IP и маску подсети в двоичном коде. Затем биты в маске подсети умножаются на соответствующие биты в адресе IP, после чего определяется адрес сети. В табл. 10.3 показаны результаты умножения битов в двоичном коде.

Таблица 10.3. Логическое умножение

Комбинация битов	Результат
1 и 1	1
1 и 0	0
0 и 0	0

Приведем пример логического умножения. На рис. 10.6 IP-адрес и базовая маска подсети записаны в двоичном представлении. Выполнено логическое умножение

Маска подсети класса B
Десятичное представление 255.255.0.0
Двоичный эквивалент 11111111 11111111 00000000 00000000

Рис. 10.5. Маски подсети могут быть выражены как в двоичной, так и в десятичной форме

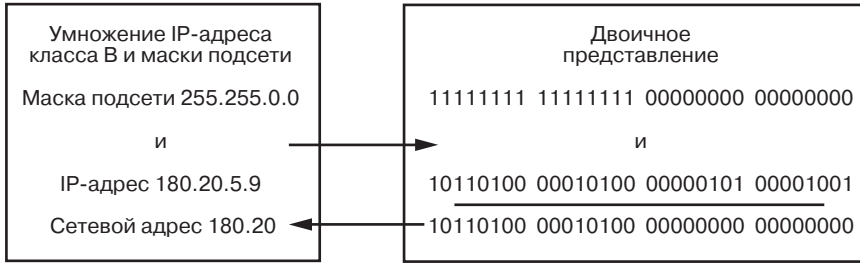


Рис. 10.6. Адрес сети определяется путем логического умножения IP-адреса и маски подсети

IP-адреса и маски подсети. Результатом такого умножения стал адрес сети (в данном случае 180.20.0.0).

Работа с подсетями

После того как мы описали формат IP-адреса и маски подсети, рассмотрим процесс работы с подсетями. Методика создания подсетей позволяет объединить несколько локальных сетей в одну. Кроме того, можно разделить сеть на несколько подсетей, связанных посредством маршрутизаторов. Разделение крупной сети на подсети при помощи маршрутизаторов обеспечивает максимальную эффективность функционирования сети: маршрутизаторы сохраняют основной рабочий трафик в пределах локальной подсети, поскольку в большинстве случаев нет необходимости транслировать информацию, которой обмениваются соседние узлы, по всей сети.

Сети каждого класса, описанного в данной главе (A, B и C), могут быть разделены на подсети. Прежде чем обсуждать способы математического расчета подсетей и новых масок подсетей, познакомимся с тем, как IP-адрес переводится из десятичной формы в двоичную и обратно.

➢ Подробнее о работе маршрутизаторов рассказывается в главе 5.

Изменение формата IP-адреса

Один октет в IP-адресе состоит из восьми бит. Каждая из позиций бита имеет эквивалент в десятичной форме. Однако этот эквивалент распознается только в том

случае, если бит представлен цифрой 1 (биты 0 не имеют значения в десятичной форме). В табл. 10.4 приведены значения для всех позиций бита в октете в десятичном коде, а также общие значения октета при условии, что определенные биты равны 1 в двоичном виде.

Таблица 10.4. Эквиваленты комбинаций битов в октете в десятичном представлении

128	64	32	16	8	4	2	1	Десятичное значение
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

В десятичном представлении первый бит любого октета в адресе IP имеет значение 128, а второй бит – значение 64. Два первых бита октета называются *битами высших разрядов*, а два завершающих бита (последний в десятичном виде равен 1, а предпоследний – 2) – *битами низших разрядов*.

В табл. 10.4 показаны десятичные значения октета при различных значениях битов. Если все биты равны 1, общее значение в десятичном виде составляет 255.

Очевидно, что вы будете работать только с теми октетами IP-адресов, в которых биты низших разрядов имеют значения в десятичном виде. Например, если и первый, и второй биты низших разрядов равны 1 в двоичном коде, то общее значение октета в десятичной форме будет 3 (то есть 1 + 2).

> *Изучив табл. 10.4, вы, вероятно, подумали: «Почему маршрутизатор, прочитав значение 255 в маске подсети, не использует затем значение октета IP-адреса, который находится в одном октете с адресом сети?» Именно так маршрутизатор и работает, однако не следует забывать, что он выполняет операции над двоичными числами, потому что данные поступают на маршрутизатор в виде потока битов. Если же сеть разделена на подсети и при этом адреса имеют различные маски подсети, то маршрутизатору не так просто различить, какая часть адреса включает информацию об адресе сети, а какая – об адресе подсети или узла связи.*

Имея дело с подсетями IP, приходится учитывать биты как высших, так и низших разрядов. И хотя при выполнении математических расчетов в процессе планировки подсетей для одних операций нужны биты высших разрядов, а для других – биты низших, сам расчет достаточно несложен.

Для примера запишем октет 01110001 в десятичном представлении с использованием информации из рис. 10.7. Вот правильный результат перевода: 64 + 32 + +16 + 1 = 113. Все, что нужно сделать для перевода, – это сложить десятичные эквиваленты тех битов октета, значения которых равны 1.

Создание подсетей в сети класса A

Возьмем в качестве примера сеть класса A и проследим всю процедуру создания подсети. Математические расчеты при построении подсетей любых классов совсем не сложные.

Значение первого октета адреса сети класса A в десятичном представлении лежит в диапазоне от 1 до 126. Допустим, что адрес сети – 10.0.0.0.

В адресе сети класса A первый октет показывает адрес сети. Остальные три октета предоставляют информацию об адресе узла, в них находятся все реальные комбинации битов, задающих адрес узла. Доступно 24 позиции битов, поэтому количество возможных адресов узлов составит $2^{24} - 2 = 16777214$ (два в степени, равной количеству битов, которые доступны для создания адресов узлов связи, – в данном случае 3 октета, или 24 бита, минус 2).

Вы должны вычесть число 2 из общего количества доступных адресов узлов (2^{24}), потому что не все биты в октетах адреса узла могут быть представлены в виде только единиц или только нулей. Адрес узла, все октеты которого представлены цифрой 1, будет зарезервирован для отправки запросов всем узлам сети, поэтому его нельзя использовать как адрес конкретного узла. Если все октеты узла связи состоят из нулей, такой адрес является адресом самой сети. В нашем случае, когда все биты в октетах адреса узла равны нулю, полный IP-адрес имеет вид 10.0.0.0, то есть совпадает с адресом сети. Этот факт очень важен для конфигурации сетей IP на маршрутизаторе.

> ***Сети IP необходимо разбивать на подсети в случае, если несколько отдельных сетей соединяются посредством маршрутизаторов. Такое разделение следует производить при условии, что у вас имеется крупная сеть с множеством узлов и существует опасность ее перегрузки.***

Рис. 10.7 иллюстрирует все, сказанное в данном разделе. Вы уже знаете, что для вычисления количества доступных адресов узлов достаточно возвести 2 в степень, равную общему количеству предназначенных для адресации узла битов, и затем вычесть 2.

Следующим шагом будет определение того, сколько подсетей необходимо построить в вашей сети. Если вы работаете с сетью класса A, то вам, скорее всего, надо будет охватить большую площадь и при этом придется иметь дело как с локальными (LAN), так и с глобальными сетями (WAN). Упростим наш пример. Предположим, вы решили разделить свою крупную сеть на 30 подсетей (вам понадобится отдельный интерфейс маршрутизатора для обслуживания каждой

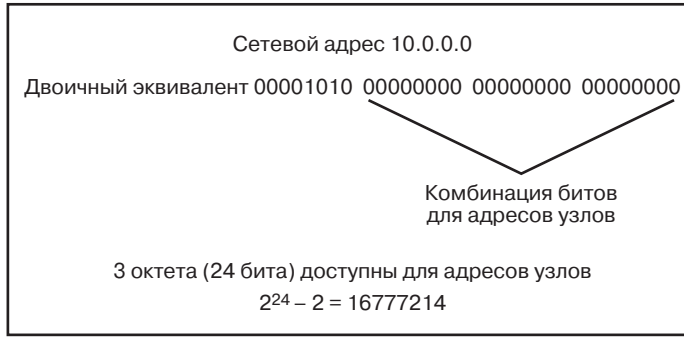


Рис. 10.7. Определение числа доступных узлов по количеству битов, предназначенных для адресов узлов

подсети, поэтому поддержка 30 подсетей потребует нескольких маршрутизаторов, каждый из которых имеет несколько интерфейсов – таких, как интерфейсы Ethernet – для подсоединения к различным подсетям).

На рис. 10.8 изображена часть сети, разделенная на шесть подсетей. Каждая локальная сеть (LAN) представляет собой отдельную подсеть с собственным се-

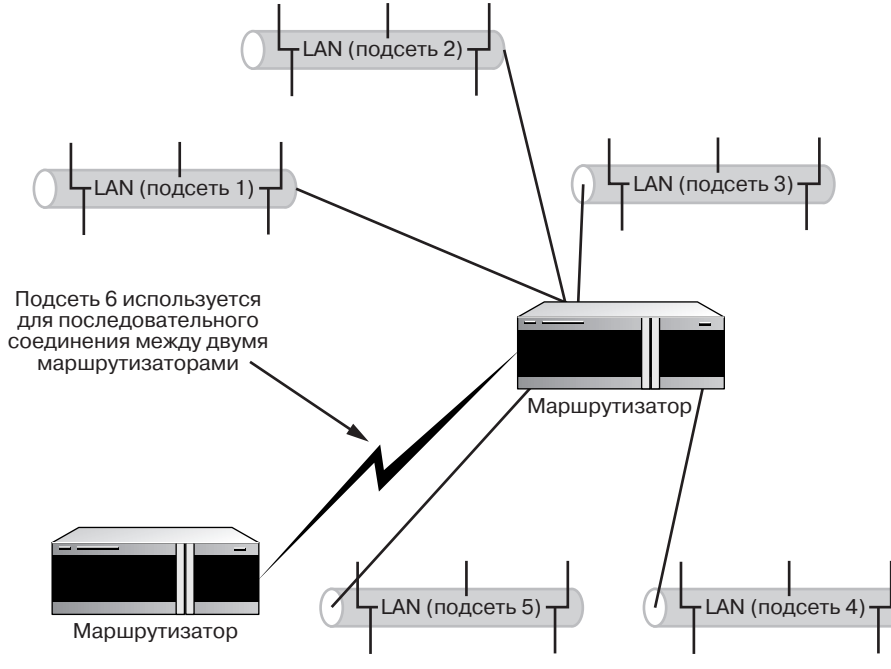


Рис. 10.8. Сеть, разделенная на подсети, состоит из отдельных локальных подсетей LAN и крупных подсетей WAN, которые соединяются маршрутизаторами

тевым адресом. Интерфейс маршрутизатора, подключенный к локальной сети, является частью этой подсети. Для последовательного соединения маршрутизаторов также нужна отдельная подсеть, поэтому одна из создаваемых вами подсетей будет отведена этим интерфейсам (на обоих маршрутизаторах).

Теперь, когда вы определились с необходимым количеством подсетей, можно приступать к выделению битов для них. Первое, что нужно сделать, – это сформировать новую маску подсети, которая будет применяться для всей сети.

Цель разделения сети на подсети состоит в том, чтобы иметь достаточно подсетей для обеспечения взаимодействия со всеми адресами в сети (посредством соединений LAN и WAN), однако нужно избегать неоправданно большого их числа. Кроме того, разделить сеть на подсети следует один раз и не изменять этого разбиения, поскольку различным маршрутизаторам и компьютерам в сети уже будут заданы определенные IP-адреса. Все это необходимо учитывать, иначе потом вы рискуете обнаружить, что создано всего лишь шесть подсетей, а не двадцать, как требовалось.

Создание маски подсети

Требуется 30 подсетей. Текущий адрес сети – 10.0.0.0 – поддерживает только биты адреса сети (первый октет) и биты адресов узлов (три других октета). Как же сформировать подсети? Для этого придется забрать некоторое количество битов из октетов, определяющих адреса узлов, и пустить их на подсети (вы не можете заимствовать биты из октета адреса сети, поскольку изменится номер базовой сети).

Итак, для подсетей вы будете изымать биты из первого октета, который служит для назначения адресов узлов (второй октет в адресе 10.0.0.0, слева направо). Это означает, что общее количество адресов узлов сократится (предоставляя биты подсетям, вы тем самым уменьшаете число доступных адресов узлов).

Забирая биты, вы сможете не только рассчитать диапазон IP-адресов каждой подсети (любая из 30 подсетей будет иметь свой диапазон IP-адресов), но и создать новую маску подсети для всей сети. При помощи этой новой маски маршрутизаторы и другие сетевые устройства получат информацию о том, что вы разделили сеть на подсети, и о том, какое количество логических подсетей у вас появилось.

Прежде всего следует определить, сколько битов потребуется для 30 подсетей. Так как каждый бит в октете можно выразить в десятичной форме (например, первый бит низшего разряда в октете имеет десятичное представление 1, второй после него бит – 2 и т.д.), для 30 подсетей нужно складывать десятичные представления битов низших разрядов до тех пор, пока в сумме не получится 31. Почему 31, а не 30? Дело в том, что нельзя использовать подсеть 0, которая возникает, когда берется первый бит низшего разряда. Следовательно, формула для вычисления

необходимого количества битов такова: сумма десятичных представлений изъятых битов низших разрядов минус 1. Из рис. 10.9 видно, каким образом можно забрать пять бит низших разрядов и получить 30 подсетей.

Определив, что для 30 подсетей требуется пять бит, вы можете сделать новую маску подсети для всей сети класса A. Пока на время «забудем» о том, что мы израсходовали биты низших разрядов на подсети.

Возьмем первые пять бит высших разрядов (128, 64, 32, 16 и 8) по порядку слева направо. Сложим их: 128 + 64 + 32 + 16 + 8 = 248. Обычная маска подсети для сети класса A выглядит так: 255.0.0.0. Однако данная сеть была разделена на подсети (при помощи битов второго октета). Поэтому новая маска подсети представима следующим образом: 255.248.0.0.

Эта маска сообщает маршрутизаторам и другим сетевым устройствам, что сеть класса A разделена на 30 подсетей. Теперь, когда у вас есть маска подсети для всей сети (она будет служить маской подсети для интерфейсов маршрутизаторов и компьютеров сети независимо от того, в какой из подсетей расположен узел), нетрудно определить диапазон IP-адресов, доступный для каждой из 30 подсетей.

Когда вы рассчитаете количество подсетей, то можете обнаружить, что при переводе битов низших разрядов в десятичное представление и последующем суммировании этих представлений получается больше подсетей, чем нужно. Например, если требуется 26 подсетей, то придется сделать 30, потому что именно такова сумма десятичных представлений битов. Это, конечно, не значит, что вам обязательно пользоваться всеми созданными подсетями, вы можете работать только с 26 из них.

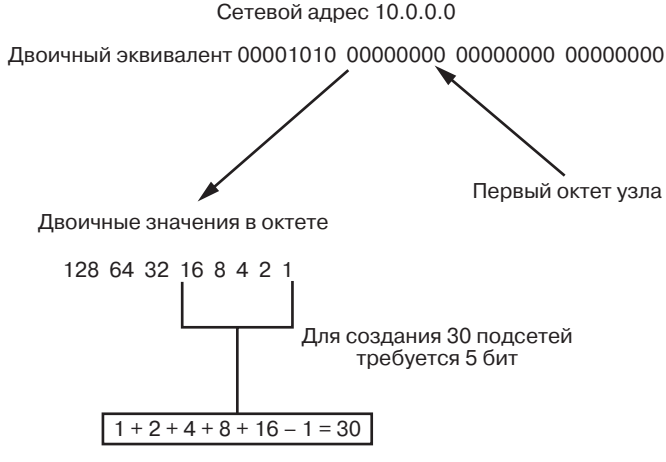


Рис. 10.9. Расчет требуемого количества подсетей

Расчет диапазона IP-адресов в подсети

Расчет диапазона адресов в подсети несложен. Мы использовали пять первых бит высших разрядов и определили номер, который будет находиться во втором октете новой маски подсети рассматриваемой сети. При помощи этих же битов высших разрядов рассчитывается диапазон IP-адресов каждой подсети. Десятичные представления битов высших разрядов таковы: 128, 64, 32, 16 и 8.

Сначала берется наименьший из битов высших разрядов, посредством которых создавалась новая маска подсети, – в данном случае 8. Этот номер становится *величиной прироста*[1], которая входит в расчет диапазонов IP-адресов применительно к каждой из 30 подсетей.

Например, первая из 30 подсетей будет начинаться с IP-адреса 10.8.0.1. Номер 8 – начальная величина прироста второго октета в адресе IP. Вспомним, что при построении подсетей брались биты из второго октета. Поэтому те адреса IP, десятичное представление второго октета которых меньше 8, не используются. Чтобы рассчитать первый номер для следующей подсети, прибавьте 8 к значению второго октета: получится 16. Следовательно, начальный адрес для второй подсети будет 10.16.0.1. Продолжая прибавлять 8 к значению второго октета, определите начальные адреса для всех 30 подсетей.

Но каким образом при расчете начального адреса узла в третьем октете получился 0, а в четвертом октете – 1? Диапазон возможных десятичных представлений любого октета располагается между 0 (все биты октета равны 0) и 255 (все биты октета равны 1), поэтому третий октет первого адреса IP подсети может выражаться нулем. Почему же четвертый октет начинается с единицы? Выше уже говорилось о том, что адрес узла связи не может состоять из октетов, включающих в себя только 1 или только 0. Если бы в четвертый октет входили лишь биты, равные 0, то все октеты, определяющие адрес узла (третий и четвертый), содержали бы исключительно нулевые биты, а такой адрес зарезервирован для подсети, а не узла.

Чтобы рассчитать диапазон IP-адресов одной подсети, нужно определить все адреса, которые находятся между начальными адресами этой и следующей подсети. Например, первой подсети будут принадлежать все адреса от 10.8.0.1 до 10.16.0.1 (за исключением последнего).

В табл. 10.5 представлены начальные и конечные адреса первых 10 подсетей из тех 30, которые мы построили. При расчете диапазонов оставшихся 20 подсетей просто добавляют величину прироста (8) ко второму октету (октету подсети).

---

[1] Термин «величина прироста» не является устоявшимся или распространенным в официальной документации. Автор книги пользуется им лишь для наглядного объяснения принципа расчетов. – *Прим. научн. ред.*

Таблица 10.5. Диапазоны IP-адресов для первых 10 подсетей из 30

Номер подсети	Начальный адрес	Конечный адрес
1	10.8.0.1	10.15.255.254
2	10.16.0.1	10.23.255.254
3	10.24.0.1	10.31.255.254
4	10.32.0.1	10.39.255.254
5	10.40.0.1	10.47.255.254
6	10.48.0.1	10.55.255.254
7	10.56.0.1	10.63.255.254
8	10.64.0.1	10.71.255.254
9	10.72.0.1	10.79.255.254
10	10.80.0.1	10.87.255.254

Расчет доступных адресов узлов

Мы уже отмечали, как важно правильно определить число создаваемых подсетей IP. Но, помимо того, необходимо удостовериться, что доступных адресов узлов в каждой из подсетей хватит для назначения их всем компьютерам и другим сетевым устройствам, которые вы планируете разместить. Каждая подсеть представляет собой самостоятельную IP-сеть, и потом нельзя будет передать несколько адресов IP из одной подсети в другую, если обнаружится, что имеющегося количества недостаточно.

Число возможных в подсети адресов узлов легко рассчитать. В сети класса A изначально для адресов узлов связи доступно 24 бита. На 30 подсетей из второго октета взято пять бит. Это означает, что теперь для IP-адресов осталось 19 бит. Чтобы узнать, сколькими адресами узлов связи располагает подсеть, возведите число 2 в 19 степень, а затем вычтите 2. В результате для подсети получится 524286 адресов IP. Очевидно, что сеть класса A поддерживает огромное количество адресов узлов связи, поэтому ситуация, когда их окажется недостаточно для всех сетевых устройств, практически нереальна. Однако при работе с сетями класса B и C число доступных адресов в каждой подсети придется тщательно просчитывать.

Почему конечный адрес каждой подсети завершается цифрами 254? Вспомните, что часть адреса IP, соответствующая адресу узла (в данном случае третий и четвертый октеты), не должна состоять только из единиц (то есть иметь десятичное представление 255). Поэтому в третьем октете допустимы только единицы (255), но четвертый октет в десятичной форме может иметь максимальное значение 254.

При делении сети на подсети количество адресов IP, доступных в качестве адресов узлов, уменьшается. Например, сеть класса A (без разбиения на подсети) поддерживает 16777214 узлов связи. Но при создании в ней 30 подсетей, в каждой из которых окажется 524286 доступных адресов IP, получится 524286 × 30 = 15728580 адресов. Следовательно, при делении на подсети потерялось 1048634 адресов узлов.

Создание подсетей для сетей класса B и C

Процессы создания подсетей в сетях класса B и C и в сети класса A аналогичны. Расчеты выполняются так же, однако вы располагаете меньшим количеством адресов узлов. Рассмотрим создание подсетей в сетях класса B и C более подробно.

Подсети для сетей класса B

Сети класса B, которые не были разделены на подсети, предоставляют два октета (16 бит) для адресов узлов. Таким образом, в сети класса B доступно 65534 адреса. Базовая маска подсети для сети класса B – 255.255.0.0.

Предположим, что на подсети требуется разделить сеть класса B с адресом 180.10.0.0. Для этого необходимо взять биты из третьего октета. Допустим, нужно шесть подсетей. На рис. 10.10 показано, как изымаются биты и создается новая маска подсети – 255.255.224.0.

При расчете диапазона IP-адресов для каждой из шести подсетей возьмите те биты высших разрядов из третьего октета, которые были использованы при создании новой маски подсети. Их сумма составит 32. Поэтому начальный адрес для первой подсети имеет вид 180.10.32.1 (адрес 180.10.32.0 зарезервирован для подсети и не может быть адресом узла связи). Чтобы определить начальный адрес второй подсети, добавьте 32 к третьему октету (64). Получите начальный адрес второй подсети – 180.10.64.1. В табл. 10.6 представлены диапазоны адресов для шести подсетей, на которые была разделена сеть класса B.

Таблица 10.6. Диапазоны IP-адресов для сети класса B

Номер подсети	Начальный адрес	Конечный адрес
1	180.10.32.1	180.10.63.254
2	180.10.64.1	180.10.95.254
3	180.10.96.1	180.10.127.254
4	180.10.128.1	180.10.159.254
5	180.10.160.1	180.10.191.254
6	180.10.192.1	180.10.223.254

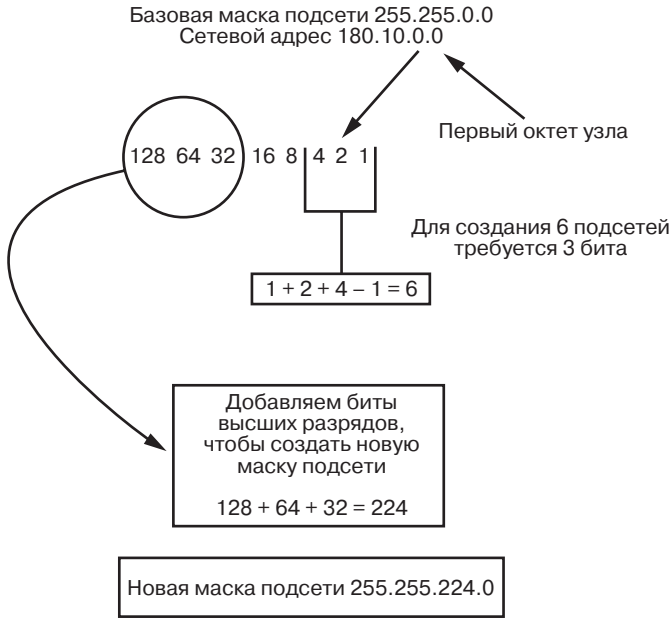


Рис. 10.10. Расчет маски подсети для сети класса B

Так как мы изъяли три бита при создании подсетей, для адресов узлов осталось 13 бит, поэтому для каждой из подсетей доступно $2^{13} - 2 = 8190$ адресов IP.

Подсети в сетях класса C

Разделить сеть класса C на подсети немного сложнее, чем сети класса A и B, поскольку в этом случае разрешается забирать биты только из одного октета. Сети класса C невелики (254 IP-адреса), так что если построить много подсетей, то в каждой из них останется весьма небольшое количество адресов узлов.

Рассмотрим пример формирования подсетей в сети класса C. Адрес сети – 200.10.44.0. Для адресов узлов доступен только один октет (четвертый), и именно оттуда мы должны брать биты.

Разделим сеть класса C на две подсети. Для этого воспользуемся двумя первыми битами низших разрядов, которые в десятичной форме составляют 1 и 2 (1 + 2 – 1 = = 2 подсети). Затем возьмем два первых бита высших разрядов (поскольку два бита низших разрядов потребовались для подсетей) и сделаем новую маску подсети. Суммируя два первых бита высших разрядов, 128 и 64, получим 192, поэтому новая маска подсети будет выглядеть в десятичном представлении как 255.255.255.192.

На рис. 10.11 показано, какие действия следует выполнить, чтобы получить новую маску подсети с помощью соответствующего количества битов высших разрядов четвертого октета.

Рис. 10.11. Расчет маски подсети для сети класса C

Теперь следует рассчитать диапазон IP-адресов, доступных для двух подсетей. Наименьший из битов высших разрядов, которые использовались при создании новой маски подсети, составляет 64. Число 64 будет величиной прироста для диапазонов подсетей. Знания, полученные при изучении подсетей класса B и C, позволят вам определить начальный адрес первой подсети – 200.10.44.64. Не забудьте, что один из адресов диапазона необходимо зарезервировать как адрес подсети. Поскольку мы работаем только с одним октетом, в качестве адреса подсети назначается первый из доступных IP-адресов – 200.10.44.64.

Диапазон IP-адресов, которые могут быть взяты для адресов узлов в первой подсети, начинается с 200.10.44.65. Во второй подсети начальный адрес 200.10.44.128 (величина прироста + начальный адрес первой подсети) также будет зарезервирован в качестве адреса подсети: данный адрес служит для идентификации подсети как самостоятельной единицы. Поэтому диапазон адресов второй подсети, предоставленных для адресов узлов связи, начинается с 200.10.44.129.

В табл. 10.7 перечислены диапазоны адресов для двух подсетей сети класса C, а также приведены те адреса, которые не могут быть адресами узлов.

Таблица 10.7. Диапазоны IP-адресов для двух подсетей сети класса C

Номер подсети	Адрес подсети	Начальный адрес	Конечный адрес	Широковещательный адрес
1	200.10.44.64	200.10.44.65	200.10.44.126	200.10.44.127
2	200.10.44.128	200.10.44.129	200.10.44.190	200.10.44.191

Идентификатор сети (Net ID) выделяется вашим ISP (например, 200.10.44.0), Иногда об Net ID говорят как об основном адресе сети. Идентификатор, зарезервированный для подсети, именуется адресом подсети. Если идентификатор сети называют основным адресом сети, то идентификатор подсети можно называть просто адресом сети. Нужно только помнить, что идентификатор, предоставляемый InterNIC или ISP, – это адрес сети или основной адрес сети, а идентификаторы подсетей, которые вы создаете, – это адреса подсетей или адреса сети в зависимости от текущего контекста.

Существует формула быстрого расчета числа доступных IP-адресов подсети: 2 в степени, равной количеству битов, которые доступны для адресов узлов, минус 2. В нашем примере расчет будет следующим: $2^6 - 2 = 62$. У нас есть две подсети, так что в сумме имеем $62 \times 2 = 124$ возможных IP-адреса.

При разделении сети класса C на подсети много доступных адресов IP теряется: пропадает два адреса в каждой подсети, один из которых резервируется для подсети, а другой – для обращения ко всем узлам этой подсети[1]. Вы, кроме того, теряете все адреса до 200.10.44.64[2], то есть пропадают адреса от 200.10.44.1 до 200.10.44.63[3]. В сети класса C и без того мало доступных адресов узлов, поэтому такая потеря весьма чувствительна.

Работа с подсетью 0

Известен способ применения потерянных адресов в качестве адресов узлов связи в подсетях (в нашем примере потерянные адреса – это адреса от 200.10.44.2 до 200.10.44.62; 200.10.44.1 зарезервирован как адрес подсети, а 200.10.44.63 – как широковещательный адрес подсети). Эти потерянные адреса составляют *подсеть 0*, и при обычных условиях воспользоваться ими нельзя. Однако вы можете сконфигурировать маршрутизатор таким образом, чтобы работать с адресами IP подобной подсети: напечатайте в режиме конфигурации команду `ip subnet-zero` и затем нажмите на клавишу **Enter** (это команда глобальной конфигурации, поэтому нет необходимости вводить ее для каждого интерфейса маршрутизатора).

Если вам требуется подсеть 0, то для создания двух подсетей – подсети 0 и подсети 1 – нужно забрать из четвертого октета только один бит. Новая маска подсети примет вид 255.255.255.128 (лишь один бит высшего разряда расходуется при формировании новой маски подсети). Диапазоны адресов IP для двух подсетей составят: 200.10.44.1–

[1] Он называется также широковещательным адресом подсети. – *Прим. научн. ред.*
[2] И после 200.10.44.191. – *Прим. научн. ред.*
[3] И адреса от 200.10.44.192 до 200.10.44.254. – *Прим. научн. ред.*

200.10.44.126 (200.10.44.127 зарезервирован как широковещательный адрес подсети) для подсети 0 и 200.10.44.129–200.10.44.254 (200.10.44.128 зарезервирован в качестве адреса подсети, а 200.10.44.255 – в качестве широковещательного адреса подсети) для подсети 1.

Поскольку при наличии подсети 0 расчет несколько усложняется (по сравнению с расчетом подсетей класса A или B), мы представили в табл. 10.8 список IP-адресов, доступных для каждой подсети при условии, что сеть класса C разделена на подсети с использованием подсети 0. IP-адреса приведены для двух, четырех и восьми подсетей в сети класса C.

Помните: если у вас есть подсеть 0, то при вычислении количества битов, которые придется забрать для формирования требуемого числа подсетей, не нужно вычитать единицу из суммы десятичного представления битов низших разрядов.

Таблица 10.8. Диапазоны IP-адресов при разбиении сети класса C на подсети с использованием подсети 0

Количество подсетей в сети	Маска подсети	Начальный адрес	Конечный адрес	Широковещательный адрес
2	255.255.255.128	x.x.x.1 x.x.x.129	x.x.x.126 x.x.x.254	x.x.x.127 x.x.x.255
4	255.255.255.192	x.x.x.1	x.x.x.62	x.x.x.63
		x.x.x.65	x.x.x.126	x.x.x.127
		x.x.x.129	x.x.x.190	x.x.x.191
		x.x.x.193	x.x.x.254	x.x.x.255
8	255.255.255.224	x.x.x.1 x.x.x.33 x.x.x.65 x.x.x.97 x.x.x.129 x.x.x.161 x.x.x.193 x.x.x.225	x.x.x.30 x.x.x.62 x.x.x.94 x.x.x.126 x.x.x.158 x.x.x.190 x.x.x.222 x.x.x.254	x.x.x.31 x.x.x.63 x.x.x.95 x.x.x.127 x.x.x.159 x.x.x.191 x.x.x.223 x.x.x.255

Заключительное слово по работе с подсетями

Работая с любой сетью, которая ориентирована на выход в Internet, вы непременно столкнетесь с необходимостью ее разделения на несколько подсетей. Если вы освоите несложные вычисления, приведенные в данной главе, разбить сеть любого класса на подсети будет совсем не сложно. В некоторых случаях удобнее просмотреть информационные таблицы.

В табл. 10.9 представлена сводная информация о маске подсети и числе хостов, доступных при разделении сети класса A на определенное количество подсетей (без подсети 0). В табл. 10.10 содержатся аналогичные сведения о сетях класса B (также без подсети 0).

Таблица 10.9. Подсети для сетей класса A

Количество подсетей	Количество используемых битов	Маска подсети	Количество хостов в подсети
2	2	255.192.0.0	4194302
6	3	255.224.0.0	2097150
14	4	255.240.0.0	1048574
30	5	255.248.0.0	524286
62	6	255.252.0.0	262142
126	7	255.254.0.0	131070
254	8	255.255.0.0	65534

Таблица 10.10. Подсети для сетей класса B

Количество подсетей	Количество используемых битов	Маска подсети	Количество хостов в подсети
2	2	255.255.192.0	16382
6	3	255.255.224.0	8190
14	4	255.255.240.0	4094
30	5	255.255.248.0	2046
62	6	255.255.252.0	1022
126	7	255.255.254.0	510
254	8	255.255.255.0	254

ГЛАВА 11

Конфигурирование маршрутизации протокола IP

Как уже неоднократно отмечалось, TCP/IP – сетевой протокол, стандартный для всех сетей (благодаря тому, что почти все такие сети стали частью глобальной сети Internet). Это надежный стек протоколов, который поддерживает маршрутизацию. В главе 10 рассказывалось о IP-адресации и разделении сетей IP на подсети. Теперь речь пойдет о конфигурировании маршрутизаторов.

Конфигурирование интерфейсов маршрутизатора

IP-маршрутизация в сети требует решения двух основных задач: конфигурирования интерфейсов LAN и WAN при помощи правильных IP-адресов и масок подсетей, а затем назначения маршрутизирующего протокола на маршрутизаторах (они автоматически поддерживают IP-маршрутизацию в отличие от IPX или AppleTalk). При IP-маршрутизации у вас есть выбор между несколькими маршрутизирующими протоколами (в частности, между RIP и IGRP).

Рассмотрим сначала процесс конфигурирования интерфейса LAN на маршрутизаторе. Например, присвоим сети класса B адрес 130.10.0.0, а затем разделим ее на шесть подсетей. Новая маска подсети будет иметь вид 255.255.224.0.

В табл. 11.1 показан диапазон IP-адресов для шести подсетей.

Таблица 11.1. Диапазон IP-адресов для шести подсетей, на которые разделена сеть с адресом 130.10.0.0

Номер подсети	Начальный адрес	Конечный адрес
1	130.10.32.1	130.10.63.254
2	130.10.64.1	130.10.95.254
3	130.10.96.1	130.10.127.254
4	130.10.128.1	130.10.159.254
5	130.10.160.1	130.10.191.254
6	130.10.192.1	130.10.223.254

На рис. 11.1 изображена диаграмма с частью локальной сети компании. IP-адреса (см. табл. 11.1) были присвоены интерфейсам всех маршрутизаторов. Этот рисунок поможет изучить те команды системы IOS, с которыми мы будем работать в данной главе.

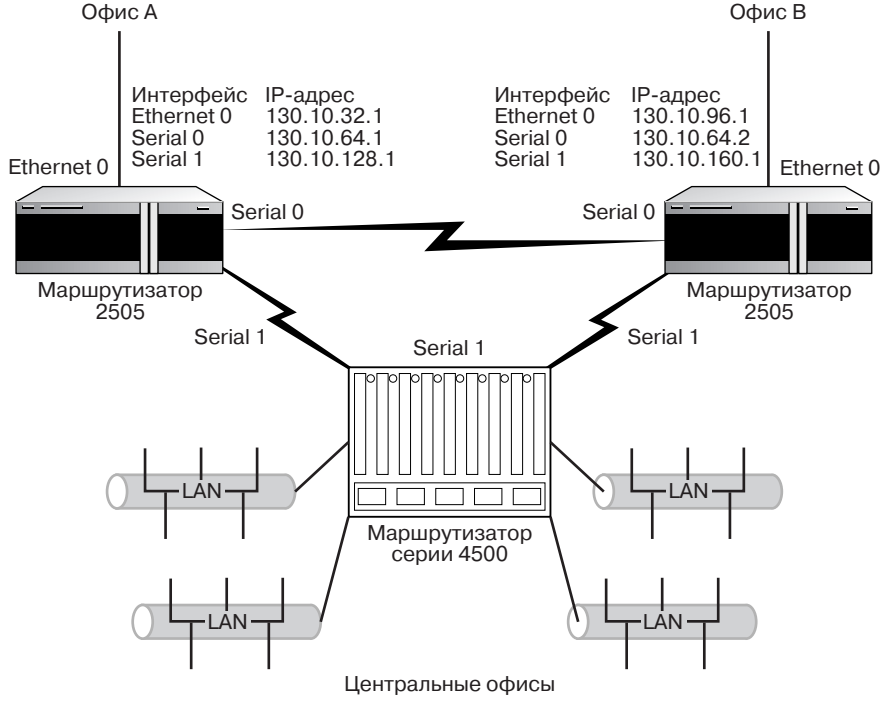


Рис. 11.1. Две удаленные сети, подключенные к объединенной сети центрального офиса (маршрутизация протокола IP)

Сконфигурируем маршрутизатор 2505 для сети офиса A. Каждый интерфейс данного маршрутизатора (всего их три: один Ethernet и два Serial) следует конфигурировать под отдельный IP-адрес. Все IP-адреса должны принадлежать диапазонам отдельных подсетей. В табл. 11.2 собраны IP-адреса (они также отображены на рис. 11.1), которые будут использоваться для конфигурации данного маршрутизатора.

Таблица 11.2. IP-адреса для интерфейсов маршрутизатора 2505

Интерфейс	IP-адрес
Ethernet 0	130.10.32.1
Serial 0	130.10.64.1
Serial 1	130.10.128.1

➢ Информация о конфигурировании интерфейсов LAN (таких, как порты Ethernet) представлена ниже, в разделе «Интерфейсы LAN», а сведения о конфигурировании интерфейсов WAN – в разделе «Интерфейсы WAN». Подробнее о маршрутизирующих протоколах, в частности о RIP и IGRP, рассказывается в главе 5, раздел «Типы протоколов маршрутизации».

Интерфейсы LAN

Интерфейсы LAN, например порты Ethernet или Token Ring, соединяют маршрутизатор с локальной сетью. Число интерфейсов LAN для маршрутизатора зависит от количества подсетей (при наличии только одного маршрутизатора).

Каждый из интерфейсов LAN находится в отдельной подсети. Самый простой способ назначить такому интерфейсу IP-адрес – взять первый IP-адрес, доступный в диапазоне адресов подсети, к которой подсоединен интерфейс.

Конфигурация IP-адресов для интерфейса LAN выполняется следующим образом:

1. В строке привилегированного режима напечатайте `config t`, затем нажмите клавишу **Enter**. Вы войдете в режим общей конфигурации.
2. Чтобы сконфигурировать определенный интерфейс LAN, введите название этого интерфейса, например `interface ethernet 0`. Затем нажмите **Enter**. Вы окажетесь в режиме конфигурации интерфейса.
3. Теперь наберите команду `ip address` вместе с IP-адресом и маской подсети для интерфейса. В нашем случае это команда `ip address 130.10.32.1 255.255.224.0` (рис. 11.2). Чтобы команда была выполнена, нажмите **Enter**.

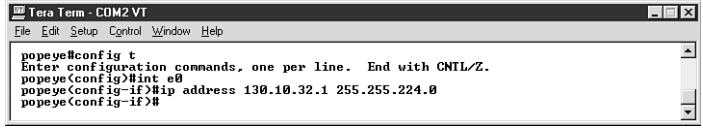


Рис. 11.2. Для отдельных интерфейсов LAN должны быть сконфигурированы IP-адреса и маски подсети

4. Нажатием клавиш **Ctrl+Z** завершите конфигурирование интерфейса.
5. Чтобы вернуться в командную строку привилегированного режима, еще раз нажмите **Enter**.

При помощи команды `show ip interface` можно быстро проверить параметры конфигурации порта LAN. Например, для контроля IP-адресации порта Ethernet 0 наберите в командной строке `show ip interface e0` и нажмите клавишу **Enter**. Рис. 11.3 иллюстрирует результат исполнения такой команды на маршрутизаторе 2505.

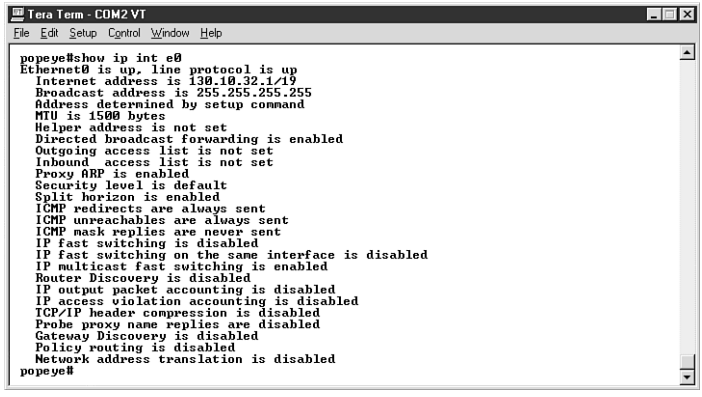


Рис. 11.3. Проверка IP-адресации интерфейса при помощи команды ***show ip interface***

Если вы внимательно просмотрите информацию о конфигурации протокола IP на рис. 11.3, то заметите, что там указан IP-адрес 130.10.32.1/19 и нет данных о маске подсети. Число 130.10.32.1 вы вводили в качестве адреса для интерфейса, а последние цифры – /19 – это сведения о маске подсети: количество битов, выделенных для адреса сети и израсходованных при разделении сети на подсети. Как правило, в сети класса B два октета (16 бит) применяются для обозначения сетевого адреса: 19 – 16 = 3 (3 – это количество битов, которые были взяты при создании подсетей). Если вы просуммируете три первых бита высших разрядов (128 + 64 + 32), то получите 224. Следовательно, маска подсети – 255.255.224.0.

> ***Если вы наберете команду `show ip interface`, не указав интерфейс маршрутизатора, то получите информацию о IP-адресации для всех интерфейсов маршрутизатора.***

Увидев сообщение, оканчивающееся числом /19, вычтите из этого числа количество битов, необходимое для сети того класса, с которым вы работаете. Таким образом вы определите количество битов, используемых для создания подсетей, и сможете рассчитать маску подсети.

Интерфейсы WAN

Интерфейсы WAN конфигурируются для IP-маршрутизации аналогично интерфейсам LAN. Конфигурация интерфейса Serial 0 маршрутизатора для IP-адресации производится следующим образом:

1. В строке привилегированного режима напечатайте `config t`, затем нажмите клавишу **Enter**. Вы войдете в режим общей конфигурации.

2. Чтобы сконфигурировать определенный интерфейс WAN, наберите в строке название этого интерфейса, например `interface serial 0`. Затем нажмите **Enter**, чтобы перейти в режим конфигурации интерфейса.
3. Теперь впишите команду `ip address` вместе с IP-адресом и маской подсети для текущего интерфейса. В данном примере это `ip address 130.10.64.1 255.255.224.0` (рис. 11.4). Для выполнения команды нажмите **Enter**.

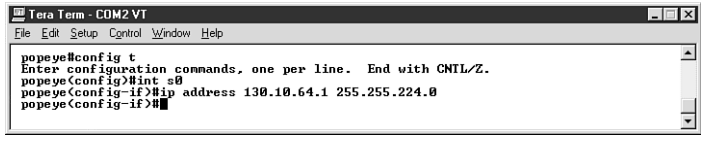


Рис. 11.4. Для каждого интерфейса WAN должны быть сконфигурированы IP-адрес и маска подсети

4. Нажмите клавиши **Ctrl+Z** и завершите конфигурирование интерфейса.
5. Еще раз нажмите **Enter**, чтобы вернуться в командную строку привилегированного режима.

Изменяя конфигурацию своего маршрутизатора, переносите изменения из памяти RAM в NVRAM. При этом текущий файл конфигурации станет файлом стартовой конфигурации маршрутизатора, то есть будет использоваться после перезагрузки маршрутизатора или после сбоя в питании. Введите в строке привилегированного режима команду `copy running-config startup-config`, затем нажмите Enter. Файл конфигурации будет сформирован и сохранен в памяти NVRAM маршрутизатора.

Проверить конфигурацию интерфейса Serial 0 можно посредством команды `show ip interface s0`.

При конфигурировании интерфейсов WAN проявляется специфическая особенность количества допустимых IP-адресов, о которой говорилось в предыдущей главе. При конфигурировании двух маршрутизаторов, соединенных через интерфейс WAN, теряется целая подсеть[1].

Например, два маршрутизатора 2505 на рис. 11.1 взаимодействуют через интерфейсы Serial 0 (при помощи соединения WAN и одного из протоколов WAN). Такое соединение должно быть сконфигурировано как отдельная подсеть. Следовательно, интерфейс Serial 0 маршрутизатора офиса A будет применять один адрес в диапазоне адресов выбранной подсети, а интерфейс Serial 0 маршрутизатора офиса B – другой адрес в том же диапазоне адресов той же подсети. Все другие адреса в данном диапазоне подсети пропадают.

[1] Диапазон IP-адресов из всей подсети, за вычетом двух, используемых для конфигурации последовательных интерфейсов маршрутизаторов. – *Прим. научн. ред.*

Во избежание подобных потерь интерфейсы Serial разрешается сконфигурировать без назначения им IP-адресов (при этом интерфейсы по-прежнему смогут маршрутизировать пакеты IP, хотя и будут созданы как *интерфейсы без назначенного IP-адреса*). Для этого в режиме конфигурации интерфейса нужно ввести команду `ip unnumbered [interface]`. Параметр `[interface]` служит для назначения реального интерфейса, например Ethernet 0, или виртуального интерфейса, такого как Loopback 0, который был сконфигурирован с IP-адресом (рис. 11.5).

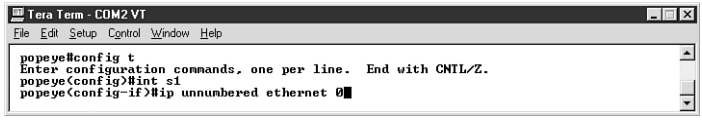


Рис. 11.5. Можно конфигурировать интерфейсы Serial без IP-адресов, при этом IP-адреса сохраняются для других маршрутизаторов и узлов сети

Если вы применяете команду `ip unnumbered` для интерфейса Serial, другой интерфейс Serial, с которым он связан через соединение WAN, также должен быть сконфигурирован как интерфейс без IP-адреса. Недостаток подобного конфигурирования в том, что протоколу Telnet невозможно задать адрес этого интерфейса, не удастся и работать с данным интерфейсом при помощи команды `ping` (поскольку он не имеет собственного IP-адреса). Кроме того, как показано на рис. 11.5, если интерфейс, к которому вы «прикрепили» порт Serial 1, например Ethernet 0, отключится, вы не сумеете пользоваться сетью WAN, подсоединенной к порту Serial 1.

Конфигурирование маршрутизирующего протокола

Завершив конфигурирование IP-адресов и маски подсети для интерфейсов маршрутизатора, приступайте к конфигурированию маршрутизирующего протокола[1]. Есть несколько протоколов, предназначенных для маршрутизации во внутренней сети[2]. Выбор протокола маршрутизации зависит от размера сети. Например, протокол RIP отлично работает с небольшими сетями, но в состоянии поддерживать максимум 15 переходов (от одного маршрутизатора к другому), поэтому вряд ли подходит для крупных сетей. В последнем случае предпочтительными являются протоколы IGRP или OSPF. Ниже мы рассмотрим конфигурирование протоколов RIP и IGRP.

➢ Подробнее о маршрутизирующих протоколах IP, таких как RIP и IGRP, рассказывается в главе 5, раздел «Типы протоколов маршрутизации».

[1] Также называемого протоколом маршрутизации. – *Прим. научн. ред.*

[2] Их относят к протоколам IGP (interior gateway protocol). – *Прим. научн. ред.*

Если IP-маршрутизация на маршрутизаторе запрещена (по умолчанию она разрешена), вам нужно включить ее, прежде чем приступить к конфигурированию протокола маршрутизации. В режиме глобальной конфигурации введите команду `ip routing`, затем нажмите клавишу Enter. Чтобы выйти из режима конфигурации, воспользуйтесь клавишами Ctrl+Z. Отключить IP-маршрутизацию можно при помощи команды `no ip routing`.

Конфигурирование протокола RIP

Протокол RIP – это маршрутизирующий протокол, который использует в качестве метрики число переходов. RIP хранит информацию в таблице маршрутизации в виде адресов сетей, или основных сетевых адресов.

Конфигурирование протокола RIP несложно. Сначала нужно выбрать его в качестве протокола маршрутизации, а затем проинформировать об основных сетевых адресах для каждого интерфейса, который вы применяете при IP-маршрутизации. В сети, взятой здесь в качестве примера (см. рис. 11.1), используется один основной сетевой адрес – 130.10.0.0, поэтому при конфигурировании протокола RIP на маршрутизаторе необходимо указать только этот адрес.

Конфигурирование протокола RIP производится следующим образом:

1. В строке приглашения привилегированного режима введите команду `configt` и нажмите клавишу **Enter**. Вы войдете в режим глобальной конфигурации.
2. В строке приглашения поместите команду `router rip`, затем нажмите **Enter**. Так вы назначите протокол RIP в качестве маршрутизирующего.
3. Наберите команду `network [major network number]`. Параметр `[major network number]` (основной сетевой адрес) – это сетевой адрес для сети класса A, B или C, которая напрямую подсоединена к маршрутизатору. В нашем примере к маршрутизатору подключена только одна основная сеть с адресом 130.10.0.0. Поэтому введите команду `network 130.10.0.0` (рис. 11.6) и нажмите **Enter**.
4. Воспользуйтесь командой `network [major network number]` для каждой сети IP, к которой подсоединен маршрутизатор. Например, если к нескольким интерфейсам Ethernet подключены различные сети класса C, то для каждого сетевого адреса этих сетей нужно повторить команду `network`[1].
5. По завершении ввода информации о сетях нажмите клавиши **Ctrl**+**Z**, чтобы закончить сеанс конфигурирования.
6. Нажав клавишу **Enter**, вы вернетесь в привилегированный режим.

[1] Вышеописанная процедура конфигурирования RIP относится к версии RIP classfull. Также существует версия RIP-2 classless. Для конфигурирования протокола RIP-2 classless при вводе команды `network` необходимо указывать адреса всех присоединенных к маршрутизатору подсетей, а не основной сетевой адрес. – *Прим. научн. ред.*

Рис. 11.6. Команда ***router rip*** назначает RIP протоколом маршрутизации, а команда ***network*** определяет основные сетевые адреса IP-сетей, присоединенных к маршрутизатору

Закончив эту процедуру, вы сможете с помощью команд системы IOS получить информацию о маршрутизации протокола RIP, в частности содержимое таблицы маршрутизации или настройки широковещательных пакетов RIP.

Чтобы просмотреть таблицу маршрутизации протокола RIP, введите команду `show ip route` в пользовательском или привилегированном режиме, затем нажмите клавишу **Enter**. На рис. 11.7 показан результат исполнения этой команды для маршрутизатора 2505, который соединен с другим маршрутизатором через последовательный интерфейс. Подсети, напрямую подключенные к маршрутизатору, обозначаются буквой «C» (это интерфейсы, сконфигурированные для данного маршрутизатора). Подсети, доступ к которым осуществляется не с локального маршрутизатора, а через другие подсети и маршрутизаторы, отмечены буквой «R» (протокол RIP определяет местонахождение таких подсетей).

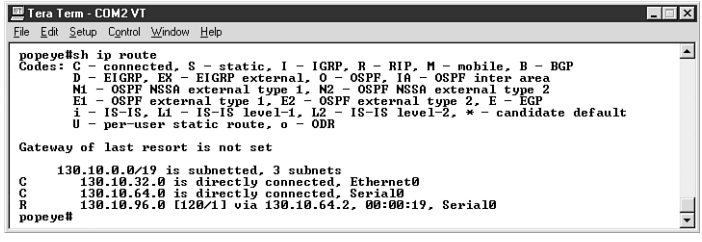


Рис. 11.7. По команде ***show ip route*** выводится таблица маршрутизации протокола RIP

Просмотреть настройки, заданные для протокола RIP, можно с помощью команды `show ip protocol`. Например, обновления протокола RIP рассылаются каждые 30 с. *Время ожидания* для протокола RIP составляет 180 с. Это означает, что маршрутизатор, не получивший обновления протокола RIP от соседнего маршрутизатора, будет ждать 180 с после последнего поступившего обновления, а затем пометит путь к соответствующей подсети или подсетям данного маршрутизатора как неподтвержденный. Через 240 с маршрутизатор удалит информацию об этом пути из своей таблицы маршрутизации, поскольку сочтет, что он более недоступен.

Введите в приглашении пользовательского или привилегированного режима команду `show ip protocol`, затем нажмите **Enter**. Отобразятся настройки протокола RIP, а также список сетей, для которых RIP служит протоколом маршрутизации (рис. 11.8).

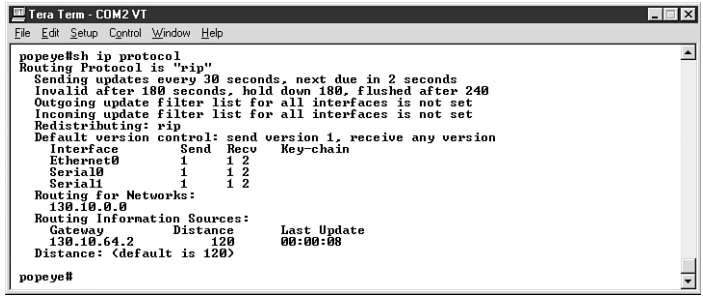


Рис. 11.8. Результат выполнения команды ***show ip protocol***

Посредством команды `debug ip rip` просмотрите пакеты обновлений протокола RIP, которые отправляются и принимаются маршрутизатором. Наберите в приглашении привилегированного режима эту команду и нажмите **Enter** (рис. 11.9).

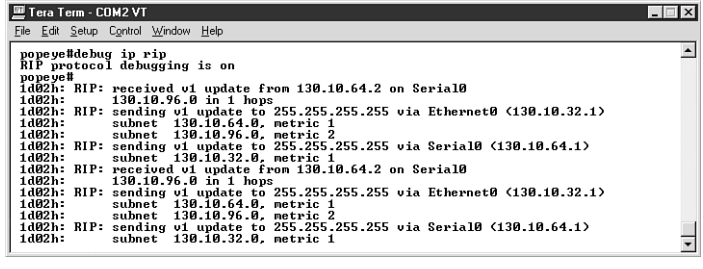


Рис. 11.9. Результат выполнения команды ***debug ip rip***

Чтобы отключить режим отладки протокола RIP, введите команду `no debug ip rip` и нажмите клавишу **Enter** (в противном случае при работе на маршрутизаторе будет очень трудно отслеживать все сообщения по обновлениям данного протокола).

➢ Информация о том, как работают маршрутизаторы и каким образом протоколы маршрутизации используются для построения маршрутных таблиц, приведена в главе 5.

Конфигурирование протокола IGRP

Поскольку RIP могут применять только маршрутизаторы, работающие максимум с 15 переходами, для средних и крупных сетей требуется другой протокол. IGRP – это протокол маршрутизации (аналогичный RIP) с такими метриками, как задержка, пропускная способность и надежность. Он не рассматривает количество переходов в качестве метрики, но при этом поддерживает до 255 переходов, что делает его удобным маршрутизирующим протоколом для крупных сетей.

Протокол IGRP конфигурируется так же, как и RIP: надо задействовать IGRP в качестве протокола маршрутизации и указать основные IP-сети, напрямую подсоединенные к интерфейсам маршрутизатора. Поскольку протокол IGRP предназначен для крупных сетей (например, для сетей, объединяющих корпорации), необходимо задать номер *автономной системы* (autonomous system – AS), к которой принадлежит маршрутизатор. В одну автономную систему могут входить несколько различных сетей любого класса. Автономные системы связаны между собой через базовые маршрутизаторы, на которых функционируют протоколы класса EGP (exterior gateway protocol). Одним из таких протоколов является протокол BGP (border gateway protocol).

> *Если объединяются две фирмы или сеть компании чрезмерно увеличивается, допустимо воспользоваться автономными системами (в случае, когда в качестве протокола маршрутизации применяется IGRP, делать это обязательно). Номера автономных систем могут находиться в пределах от 1 до 65655. Вы сами назначаете их своим сетям, но не хаотично, а по порядку. Затем такие автономные системы связываются посредством базовых маршрутизаторов, на которых работает протокол EGP. Информация о маршрутизаторах Cisco серии 7500, способных исполнять функции базовых маршрутизаторов, содержится в приложении 2.*

Конфигурирование протокола IGRP осуществляется следующим образом:

1. В строке приглашения привилегированного режима введите команду `configt` и, нажав клавишу **Enter**, войдите в режим глобальной конфигурации.
2. В строке приглашения поместите команду `router igrp [autonomous system number]`, где параметр `[autonomous system number]` (номер автономной системы) – номер, заданный для той системы AS, к которой относится маршрутизатор. Например, команда `router igrp 10` задействует IGRP-маршрутизацию и укажет систему AS с номером 10. Затем нажмите **Enter**.
3. Наберите в строке конфигурации команду `network [major network number]`. Параметр `[major network number]` (основной сетевой адрес) – это сетевой адрес для сети любого класса, напрямую подсоединенной к маршрутизатору. В нашем примере к маршрутизатору подключена только одна основная сеть с адресом 130.10.0.0. Поэтому введите команду `network 130.10.0.0` (рис. 11.10) и нажмите **Enter**.

Рис. 11.10. Конфигурирование протокола IGRP

4. Воспользуйтесь командой `network [major network number]` для каждой сети IP, к которой непосредственно подсоединен маршрутизатор. Например, если к нескольким интерфейсам Ethernet подключены различные сети класса C, то для каждого их сетевого адреса нужно повторить команду `network`.
5. Завершив ввод информации по сетям, нажмите клавиши **Ctrl**+**Z**, чтобы закончить сеанс конфигурирования.

Вы можете использовать команды `show` (и различные их варианты, имеющие отношение к протоколу IGRP), описанные выше, в разделе «Конфигурирование протокола RIP». Например, команда `show ip route` выводит таблицу маршрутизации, построенную протоколом IGRP (рис. 11.11). Сетевые адреса, обозначенные буквой «C», – это адреса сетей, напрямую подсоединенных к маршрутизатору, а помеченные буквой «I» – адреса сетей, поиск которых выполняется протоколом IGRP.

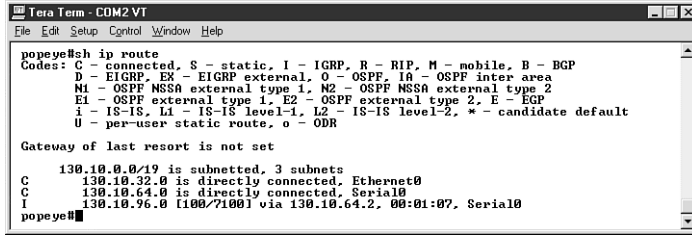


Рис. 11.11. Команда ***show ip route*** позволяет просмотреть таблицу маршрутизации протокола IGRP

Протокол IGRP посылает обновления каждые 90 с (в отличие от протокола RIP с интервалом в 30 с между обновлениями). Если период ожидания для какого-либо пути превысил 630 с, этот путь удаляется из таблицы маршрутизации.

Для просмотра пакетов обновлений протокола IGRP, которые отправляются и принимаются локальным маршрутизатором, можно воспользоваться командой `debug ip igrp events`. Рис. 11.12 иллюстрирует результат выполнения данной команды.

Команда `debug ip igrp transaction` позволяет получить информацию о применяемых метриках (рис. 11.13).

➢ Подробнее о протоколе IGRP и о протоколах связи с внешней сетью рассказывается в главе 5, раздел «Типы протоколов маршрутизации».

Для полного отключения режима отладки на маршрутизаторе введите в строке приглашения привилегированного режима команду `no debug all` и нажмите клавишу Enter.

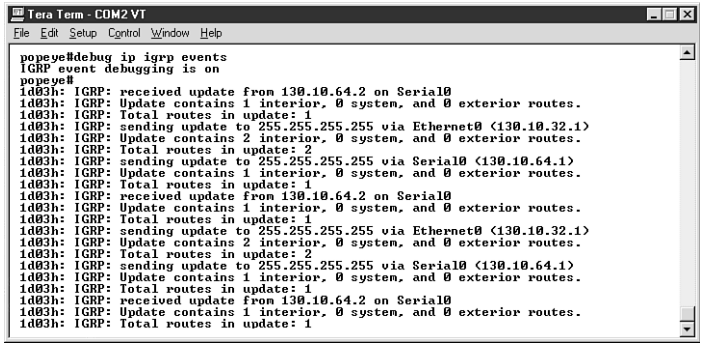


Рис. 11.12. Команда ***debug ip igrp events*** позволяет просматривать все исходящие и входящие обновления протокола IGRP

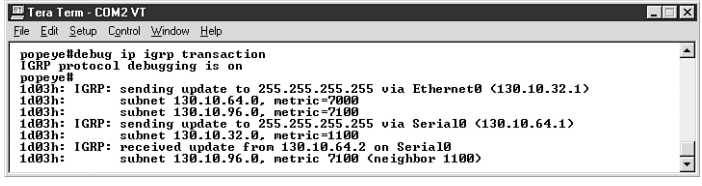


Рис. 11.13. Команда ***debug ip igrp transaction*** выводит информацию, касающуюся исходящих и входящих обновлений, а также используемых метрик

Динамическая и статическая маршрутизация

Выше рассматривалось функционирование маршрутизатора с динамической маршрутизацией. Выбранный протокол – RIP или IGRP – формирует таблицу маршрутизации в соответствии с информацией, полученной от соседних устройств. Можно также сконфигурировать маршрутизаторы для работы со *статической маршрутизацией*, указав пути в статической таблице маршрутизации. Обновление такой таблицы выполняется вручную.

При статической маршрутизации протокол маршрутизации не нужен: вы сами должны контролировать таблицы маршрутизации. Статическую маршрутизацию следует применять в случае, если пути в сети немногочисленны и неизменны, а между сетью или сетями, которые обслуживаются маршрутизатором, и соседними сетями существует только один путь. Статические таблицы маршрутизации не реагируют на изменения путей.

Поясним сказанное на примере. Допустим, имеется два маршрутизатора, которые обслуживают сети класса C, не разделенные на подсети. Эти маршрутизаторы соединены так, как показано на рис. 11.14. Требуется задать статический путь от

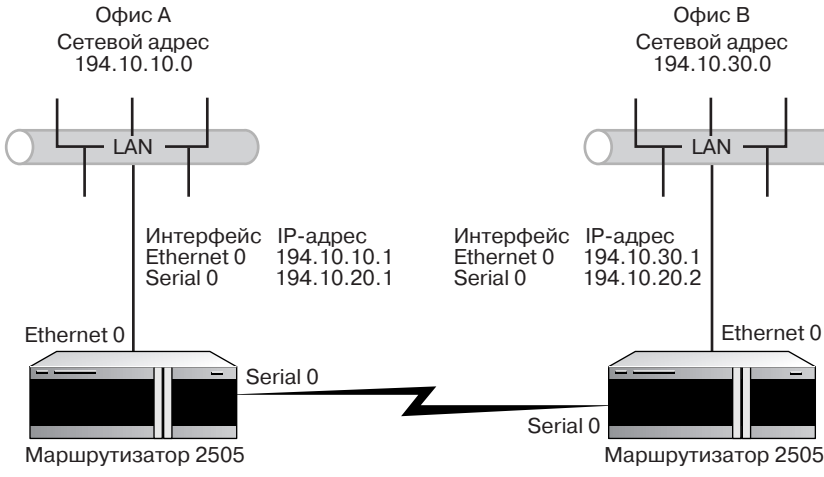


Рис. 11.14. Небольшая сеть может быть сконфигурирована со статической IP-маршрутизацией

маршрутизатора в офисе A к локальной сети LAN в офисе B (адрес сети класса C – 194.10.30.0).

Введите в приглашении режима глобальной конфигурации маршрутизатора в офисе A команду `ip route 194.10.30.0 255.255.255.0 194.10.20.2`. Тем самым вы заставите маршрутизатор в офисе A создать статическую таблицу маршрутизации, где связь с локальной сетью LAN в офисе B (адрес 194.10.30.0) реализуется через последовательное соединение между двумя маршрутизаторами. Кроме того, вы сообщаете, что последовательный интерфейс маршрутизатора в офисе B сконфигурирован с IP-адресом 194.10.20.2. Из рис. 11.15 видно, как данная команда будет выглядеть на консоли маршрутизатора.

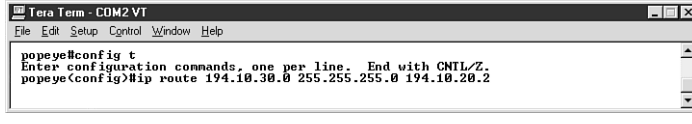


Рис. 11.15. Статические пути конфигурируются при помощи команды ***ip route***

Для маршрутизатора в офисе A необходимо указать пути ко всем сетям, за которые отвечают удаленные маршрутизаторы. И поскольку в офисе B имеется маршрутизатор, с помощью команды `ip route` нужно сформировать на нем статическую таблицу маршрутизации, содержащую пути к сетям, которые обслуживаются другими маршрутизаторами (например, к сети 194.10.10.0, связанной с маршрутизатором в офисе A). В команде указываются сеть-адресат, а также IP-адрес интерфейса того маршрутизатора, который обслуживает данную сеть.

Как видите, ручное составление таблиц маршрутизации требует больших усилий. Кроме того, если маршруты изменятся, придется также вручную корректировать все таблицы на всех маршрутизаторах.

Статическая маршрутизация обеспечивает полный контроль над всеми путями, по которым проходят пакеты данных. Однако при работе с крупными и динамичными сетями значительно удобнее динамическая маршрутизация и соответствующие протоколы IGP для конфигурирования маршрутизаторов.

Использование протокола Telnet

Преимущество конфигурирования IP-адреса на интерфейсе маршрутизатора заключается в том, что подсоединиться к другому маршрутизатору (посредством протокола Telnet) можно, воспользовавшись IP-адресом одного из его интерфейсов. Например, вы работаете с двумя маршрутизаторами 2505, которые связаны последовательным кабелем. Один из маршрутизаторов имеет IP-адрес 130.10.96.1 на порте Ethernet 0 и IP-адрес 130.10.64.2 на порте Serial 0. Чтобы получить доступ к этому маршрутизатору (при помощи протокола Telnet), разрешается применить любой из этих адресов. Обратившись к маршрутизатору по протоколу Telnet, введите пароль виртуального терминала, который был сконфигурирован для данного маршрутизатора.

Для получения доступа к другому маршрутизатору с помощью протокола Telnet выполните следующие действия:

1. В приглашении пользовательского или привилегированного режима наберите команду `telnet [ip address]`, где параметр `[ip address]` – это IP-адрес одного из интерфейсов маршрутизатора. Чтобы получить доступ к маршрутизатору A, который подсоединен к маршрутизатору B последовательным кабелем, воспользуйтесь командой `telnet 130.10.96.1`, содержащей IP-адрес порта Ethernet 0. Затем нажмите клавишу **Enter**.
2. Вы обратитесь к маршрутизатору по протоколу Telnet, после чего поступит запрос о пароле виртуального терминала. Введите требуемый пароль и нажмите **Enter**.

Теперь вы работаете на другом маршрутизаторе (рис. 11.16).

Если вам известен пароль, вы сумеете войти в привилегированный режим маршрутизатора и изменить его конфигурацию. По окончании работы на маршрутизаторе

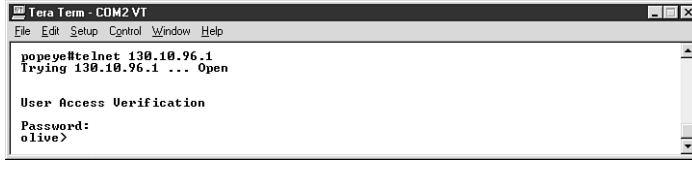


Рис. 11.16. Для подсоединения к другому маршрутизатору служит протокол Telnet

наберите команду `quit`, чтобы завершить сеанс с удаленным маршрутизатором и вернуться к приглашению командной строки своего локального маршрутизатора.

Протокол Telnet – удобное средство удаленного доступа к маршрутизаторам, которое позволяет просматривать и менять их конфигурацию. Работа с этим протоколом аналогична администрированию с компьютера, напрямую подсоединенного к маршрутизатору.

Подробнее об установке пароля виртуального терминала при первом конфигурировании маршрутизатора рассказывается в главе 8, раздел «Работа в режиме системной конфигурации».

ГЛАВА 12

Маршрутизация протокола Novell IPX

Операционная система Novell NetWare – это популярная *сетевая операционная система* (network operating system – NOS), которая предоставляла в локальных сетях LAN файловый сервис и сервис печати с начала 80-х годов. Система NetWare имеет собственный стек протоколов под названием *IPX/SPX*[1]. Протоколы этого стека, как и стека TCP/IP, не полностью соответствуют модели OSI. IPX/SPX получил широкое распространение в локальных сетях благодаря своей высокой производительности и тому, что, в отличие от TCP/IP, он не требует выделения дополнительных ресурсов. ОС NetWare была и остается одной из самых популярных систем, обеспечивающих компьютеры-клиенты доступом к ресурсам LAN и WAN.

Введение в стек протоколов IPX/SPX

Novell NetWare – это пример сетевой операционной системы, полностью соответствующей архитектуре клиент/сервер. Все компьютеры в сети – либо клиенты (получение услуг), либо серверы (предоставление услуг).

IPX/SPX – маршрутизируемый протокол, поэтому он играет немаловажную роль в изучении маршрутизации и, в частности, маршрутизаторов Cisco. На рис. 12.1 представлен стек протоколов IPX/SPX применительно к модели OSI. В следующих двух разделах мы рассмотрим протоколы данного стека, а также обсудим принципы IPX-адресации.

➢ Информация о стеке IPX/SPX применительно к другим сетевым протоколам (таким, как TCP/IP и AppleTalk) приведена в главе 2 (раздел «Протокол IPX/SPX»). О модели OSI рассказывается в той же главе (раздел «OSI – теоретическая модель стека сетевых протоколов»).

---

[1] До недавнего времени IPX/SPX был единственным стеком протоколов в ОС Novell NetWare. Начиная с версий 4x, фирма Novell добавила в свой продукт поддержку TCP/IP. В версиях NetWare 5.0 и 5.1 TCP/IP считается основным стеком протоколов и используется по умолчанию, хотя для совместимости со старыми версиями сохранена возможность работы со стеком IPX/SPX. – *Прим. научн.*

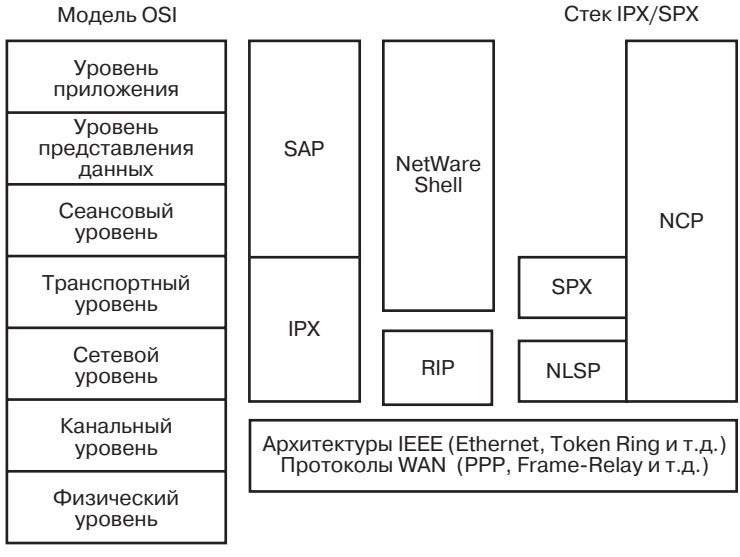


Рис. 12.1. Стек протоколов IPX/SPX

В 60-е годы группа программистов в Исследовательском центре Xerox Palo создала операционную систему Xerox Network Systems – XNS, на которой во многом основана ОС NetWare. Та же группа программистов сконструировала и сетевой компьютер с графическим пользовательским интерфейсом, который использовал в качестве устройств ввода информации мышь и клавиатуру. Технология, разработанная в Исследовательском центре Xerox Palo, опередила по времени как IBM PC, так и Apple Macintosh. Много великих идей родилось в этом центре. Так почему же компания Xerox сейчас не является мировым лидером в компьютерных продуктах и решениях? Хороший вопрос...

Протоколы стека IPX/SPX

Аналогично TCP/IP, стек IPX/SPX состоит из нескольких протоколов. Так, *NetWare Core Protocol* (NCP) предоставляет сетевые функции на уровне приложения, уровне представления данных и сеансовом уровне модели OSI. *Виртуальные загрузочные модули* (Virtual Loadable Modules – VLMs) обеспечивают сеансы связи между клиентом и сервером.

Ниже мы рассмотрим те протоколы стека IPX/SPX, которые участвуют в маршрутизации:

- *протокол SPX (Sequence Packet Exchange)* – ориентированный на соединение протокол транспортного уровня, который обеспечивает протоколы более

высоких уровней прямой виртуальной связью между компьютером-отправителем и компьютером-получателем. SPX посредством виртуальных линий связи реализует взаимодействие между компьютерами и выводит номер ID-соединения в заголовке SPX-датаграммы (SPX – это аналог протокола TCP в стеке TCP/IP);

- *протокол IPX (Internet Package Exchange)* – не ориентированный на соединение протокол транспортного уровня, который предоставляет систему адресации для стека IPX/SPX. Функционируя на сетевом и транспортном уровнях модели OSI, IPX управляет движением пакетов данных в сети с помощью информации, предоставляемой протоколом IPX RIP;
- *протокол RIP (Routing Information Protocol)* – протокол маршрутизации, который посредством двух метрик, *отсчета времени* (1/18 с) и *счетчика переходов* маршрутизирует пакеты в сети IPX. Протокол RIP стека IPX/SPX (аналогично протоколу RIP стека TCP/IP) – это протокол маршрутизации, создающий и поддерживающий таблицы маршрутизации между маршрутизаторами, работающими с протоколом IPX, и серверами NetWare;
- *протокол SAP (Service Advertisement Protocol)* – протокол, который информирует о доступности различных ресурсов в сети NetWare. Серверы NetWare через каждые 60 с рассылают широковещательные пакеты протокола SAP, что позволяет компьютерам-клиентам получать сведения о местонахождении доступных сетевых ресурсов (каждому типу службы в пакетах протокола SAP присваивается уникальный шестнадцатеричный номер);
- *протокол NLSP (NetWare Link Services Protocol)* – разработанный фирмой Novell протокол маршрутизации, который может заменить протокол RIP (и SAP) при IPX-маршрутизации. Взаимодействие протоколов RIP и SAP рассматривается ниже (раздел «Конфигурирование IPX-маршрутизации»).

Стек IPX/SPX во многом похож на стек TCP/IP (его описание имеется в главе 10), хотя и работает по-другому. Он содержит несколько протоколов, которые функционируют на низших уровнях модели OSI (сетевом и канальном) и участвуют в процессе маршрутизации. Прежде чем рассказывать о том, как эти протоколы взаимодействуют и обеспечивают маршрутизацию пакетов данных стека IPX/SPX, рассмотрим систему адресации IPX/SPX.

Система IPX-адресации

IPX-адресация использует 80-битную (10-байтную) систему адресации (стек TCP/IP применяет, как вы помните, 32-битную систему), которая содержит информацию об адресе сети и адресе узла. Система адресации иерархическая, как и для стека TCP/IP. IPX-адреса представлены в шестнадцатеричном виде и состоят из двух частей. Первая часть, занимающая 32 бита, – это *номер сети IPX*, остальные 48 бит представляют собой адрес узла. На рис. 12.2 показан пример типичного IPX-адреса в сети Novell.

Откуда появляется номер сети и где брать информацию об адресе узла? Когда в локальной сети Novell создается сервер NetWare, при установке его программного обеспечения генерируется номер сети. Это число становится номером локальной сети вне зависимости от того, сколько будет добавлено дополнительных серверов NetWare (серверов файлов и принтеров). Поэтому все компьютеры-клиенты (и дополнительные серверы) в сети Novell NetWare получат одинаковый номер сети (например, 763B20F3, как на рис. 12.2).

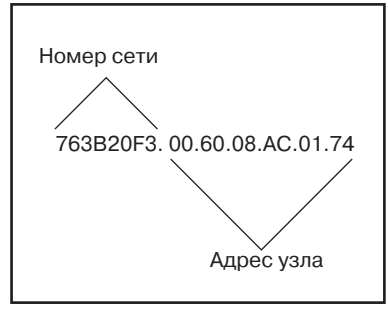


Рис. 12.2. IPX-адрес состоит из номера сети и адреса узла

Для настройки IPX-маршрутизации необходимо знать номер сети IPX (вам его может сообщить администратор сети NetWare). Если же вы сами являетесь администратором, загрузите утилиту Monitor (для версий Novell NetWare 5.0 и 5.1) или Servman (для предыдущих версий Novell). Для этого в системной консоли сервера введите команду `load servman` *или* `monitor` *(в зависимости от версии NetWare) и нажмите клавишу Enter. Затем просмотрите информацию о конфигурации сетевого адаптера в соответствующем окне.*

Если строится новая сеть NetWare (отдельная самостоятельная сеть), номер для нее предоставит первый сервер NetWare, который будет создан в этой сети. Таким образом, сети IPX идентифицируются по своим сетевым номерам (а сети IP – по маскам подсети и битам, выделенным в IP-адресах для формирования подсетей). Любой маршрутизатор, участвующий в передаче пакетов от определенной сети, будет сконфигурирован с таким же номером сети, как и эта сеть NetWare. Следовательно, если интерфейс Ethernet 0 маршрутизатора подсоединен к сети NetWare, то в конфигурации интерфейса будет использоваться ее номер.

При работе с адресами узлов для IPX-клиентов не возникает проблем. Такие адреса динамически задаются всем узлам в сети и представляют собой аппаратные адреса MAC на сетевой карте. Можно сделать вывод о том, что IPX-адрес

получается добавлением сетевого номера к аппаратному MAC-адресу узла. На рис. 12.3 показаны два узла и сервер в одной сети NetWare.

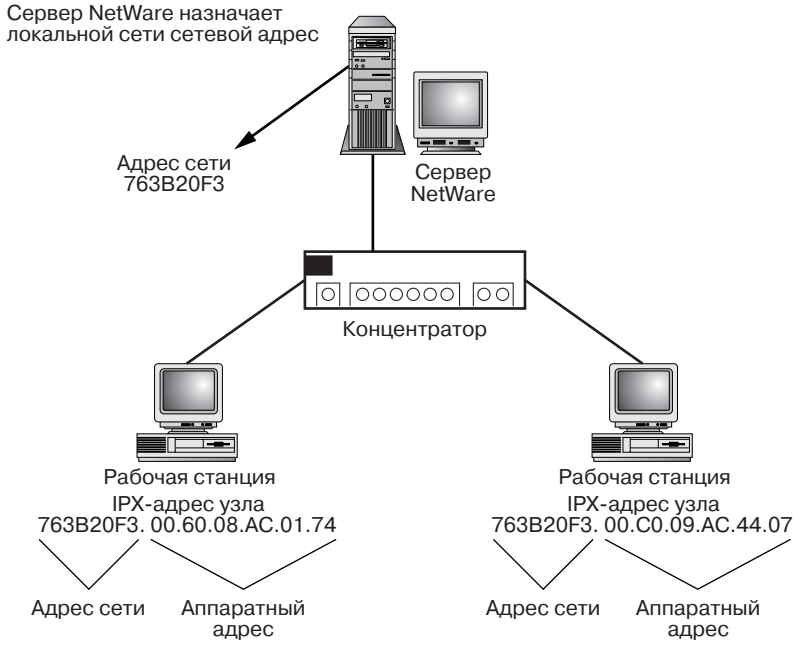


Рис. 12.3. IPX-адреса узлов состоят из номера сети и аппаратных MAC-адресов узлов

➢ Сведения об аппаратных адресах MAC приведены в главе 2 (раздел «Канальный уровень»), а о сетевых картах – в главе 1 (раздел «Сетевые адаптеры»).

Протокол SAP

Прежде чем изучать конфигурирование IPX-маршрутизации, обсудим роль широковещательных пакетов протокола SAP в работе сети IPX[1]. Серверы Novell рассылают пакеты протокола SAP через каждые 60 с. Эти пакеты содержат сведения обо всех ресурсах системы, отправляющей пакеты SAP, а также обо всех ресурсах, данные о которых были получены от других серверов NetWare. Информация, поступившая на сервер от других серверов, а также список этих серверов заносятся в таблицу протокола SAP в системе NetWare.

[1] Излагаемая информация касается операционных систем Novell NetWare до версии NetWare 5.0, начиная с которой сервисы Novell могут объявлять о себе по IP, используя протокол SLP. – *Прим. научн. ред.*

Отправляя пакеты протокола SAP, сервер NetWare, по сути, рассылает целиком свою таблицу протокола SAP и таким способом передает информацию протокола SAP всем серверам в сети.

Маршрутизаторы Cisco с интерфейсами, сконфигурированными для работы с протоколом IPX, строят таблицы протокола SAP и посылают данные этих таблиц всем сетям, к которым подсоединены интерфейсы маршрутизатора. Маршрутизаторы Cisco, однако, не транслируют широковещательные пакеты протокола SAP от одной сети Novell к другой, а только отправляют свою таблицу SAP – список ресурсов, которые предоставляются каждой сетью, подключенной к тому или иному интерфейсу маршрутизатора. Маршрутизатор передает суммарную таблицу SAP всем доступным сетям NetWare. На рис. 12.4 показано, каким образом маршрутизатор Cisco формирует суммарную таблицу протокола SAP.

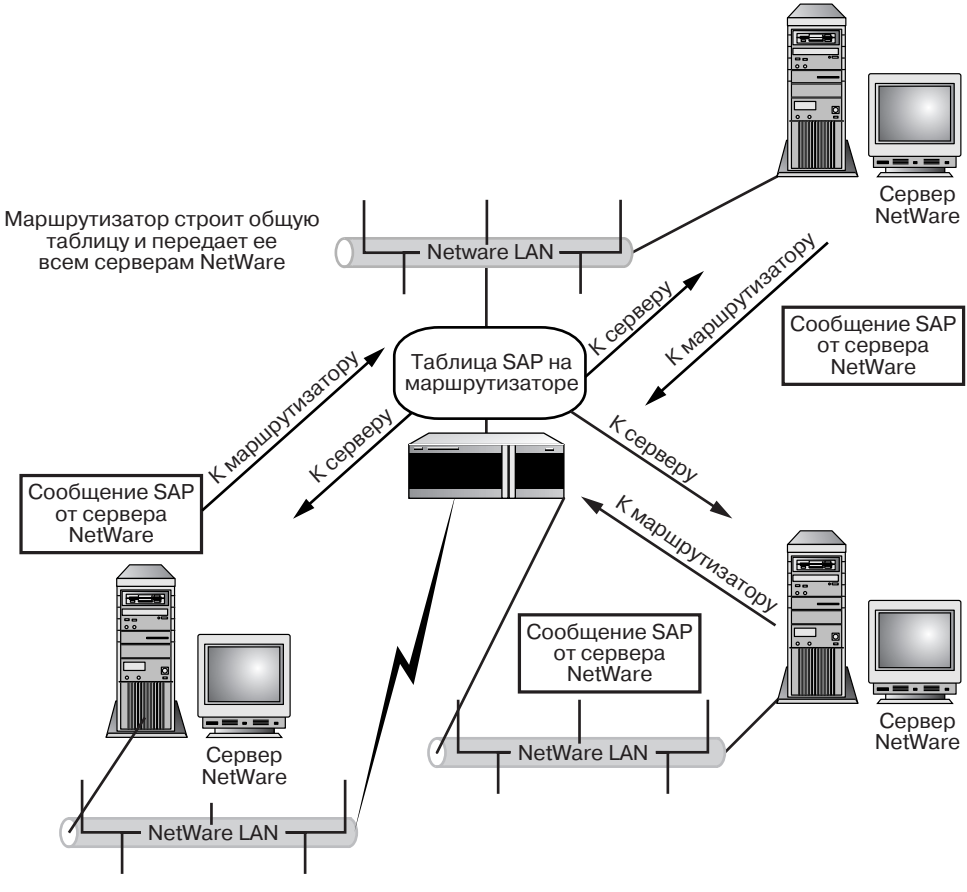


Рис. 12.4. Пакеты протокола SAP передаются с серверов на маршрутизатор, и суммарная таблица SAP посылается от маршрутизатора к серверам

Если клиент сети Novell нуждается в информации об определенном ресурсе, он отправляет широковещательный запрос, или запрос ближайшего сервера (Get Nearest Server request – GNS), где указывается, какой именно ресурс требуется. Сервер, получив запрос GNS, проверяет свою таблицу протокола SAP, чтобы определить местонахождение необходимого ресурса (такого, как файл или принтер), а затем посылает клиенту ответ на запрос, сообщая, на каком сервере можно найти данный ресурс.

Конфигурирование IPX-маршрутизации

Мы рассказали, как работает IPX-адресация и как протоколы стека IPX/SPX обеспечивают маршрутизацию, теперь попробуем сконфигурировать маршрутизатор для IPX-маршрутизации. Сначала необходимо разрешить поддержку IPX-маршрутизации, а потом сконфигурировать отдельные интерфейсы.

Поддержка IPX-маршрутизации включается следующим образом:

1. В приглашении привилегированного режима введите команду `config t`, затем нажмите клавишу **Enter**. Вы окажетесь в режиме общей конфигурации.
2. Поместите в строке приглашения команду `ipx routing` и снова нажмите **Enter**. Результат выполнения этой команды показан на рис. 12.5.

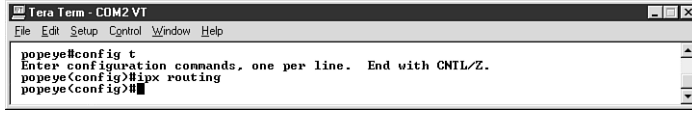


Рис. 12.5. Чтобы включить IPX-маршрутизацию, достаточно выполнить всего одну команду в режиме общей конфигурации

3. Выйти из режима конфигурации можно при помощи клавиш **Ctrl**+**Z**.
4. Для возвращения в привилегированный режим нажмите **Enter**.

Проверить, задействована ли IPX-маршрутизация, очень легко. Введите в строке команду `show protocol` и нажмите клавишу **Enter**. Появится список сетевых протоколов, которые применяются при маршрутизации (рис. 12.6). Для всех интерфейсов маршрутизатора также выводится информация о протоколах.

При включении IPX-маршрутизации посредством команды `ipx routing` происходит автоматическая конфигурация протокола IPX RIP как маршрутизирующего. Как уже отмечалось, IPX RIP работает со счетчиком переходов и отсчетом времени в качестве метрики (протокол RIP, применяемый для IP-маршрутизации, использует только счетчик переходов). Эти метрики взаимодействуют простым способом: если найдены два пути до одного пункта назначения (при помощи таблицы маршрутизации протокола IPX маршрутизатора), то они имеют одинаковое

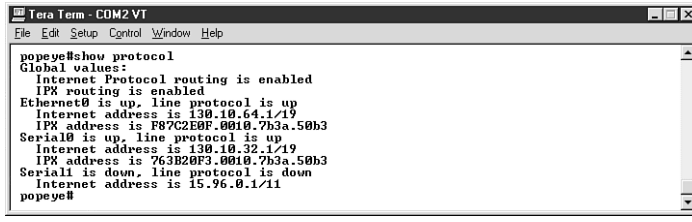


Рис. 12.6. Просмотр списка протоколов, задействованных в сети

количество переходов (допустим, пять). Путь с наименьшей метрикой времени будет назначен маршрутом для пересылки пакетов данных. Возможен и обратный принцип: из двух путей с одинаковой метрикой времени будет выбран путь с меньшим числом переходов.

На рис. 12.7 представлена сеть IPX, в которой между двумя компьютерами (отправителем и получателем) существуют два пути с одинаковым числом переходов (два). Однако маршрут через сеть 2 (последовательное соединение между

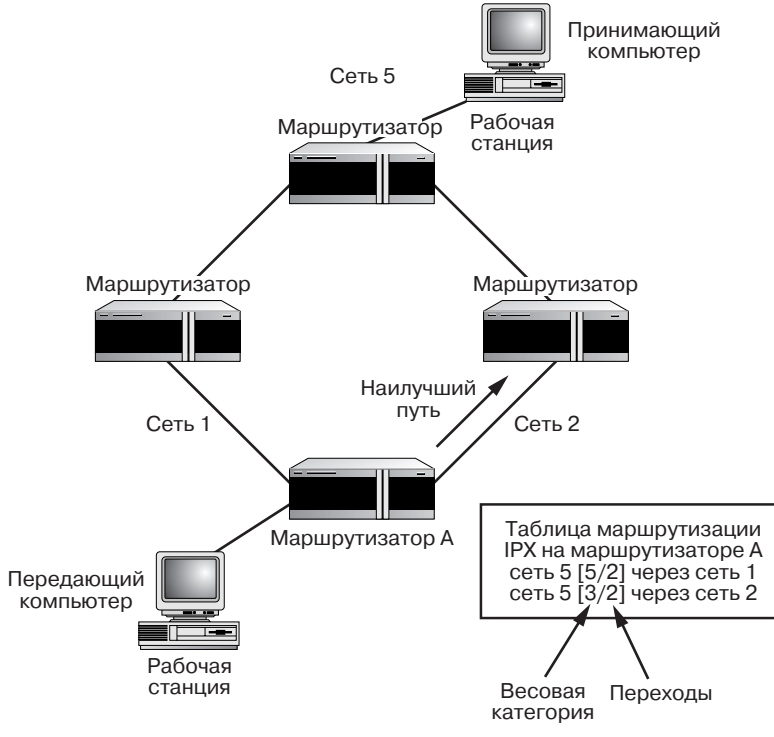


Рис. 12.7. Протокол IPX использует в качестве метрики счетчик времени и счетчик переходов

маршрутизатором A и его соседом) имеет метрику времени 3, поэтому маршрутизатор A предпочтет именно этот путь доставки пакетов данных.

> *Команда, которая задействует IPX-маршрутизацию, записывается в формате* `ipx routing node`*, где* `node` *(узел) – аппаратный MAC-адрес интерфейса. Если вы не введете адрес узла (аппаратный адрес MAC), он будет задан автоматически. Поскольку последовательный интерфейс не имеет аппаратного адреса, он «занимает» такой адрес у одного из интерфейсов Ethernet маршрутизатора. Более подробно эта тема рассматривается в следующем разделе.*

Конфигурирование интерфейсов для IPX-маршрутизации

Включив IPX-маршрутизацию, вы получаете возможность сконфигурировать интерфейсы маршрутизатора для работы с IPX. Их необходимо конфигурировать под определенную сеть IPX – для номера сети, который был сгенерирован первым созданным сервером Novell. Адреса узлов задаются автоматически и соответствуют аппаратным адресам MAC, так что нет нужды беспокоиться о них.

Может показаться, что сконфигурировать протокол IPX проще, чем IP. Однако при конфигурировании протокола IPX приходится решать существенную проблему – определять *тип кадра*, который нужно задать интерфейсам LAN маршрутизатора.

Интерфейсы LAN

Все данные при перемещении по сети в виде потока битов заключаются в особое *обрамление*, тип которого зависит от содержимого некоторых полей кадра канального уровня модели OSI. Для протоколов LAN назначить тип кадра несложно: сети Ethernet используют кадры Ethernet, сети Token Ring – кадры Token Ring, сети FDDI – кадры FDDI.

Однако операционная система NetWare поддерживает несколько типов кадра для популярных архитектур LAN: Ethernet, Token Ring и FDDI. И если вы сконфигурируете интерфейсы маршрутизатора неправильно, они не смогут обмениваться информацией с другими узлами или маршрутизаторами.

Операционная система NetWare поддерживает четыре типа кадров для архитектуры Ethernet. Так как сети Ethernet очень распространены, в табл. 12.1 приводятся описания и способ применения для всех типов обрамлений. Там же представлены команды маршрутизатора Cisco, посредством которых задается нужный тип кадров Ethernet на интерфейсе маршрутизатора.

Если вы не знаете, как правильно сконфигурировать тип кадра, не отчаивайтесь. Кадры WAN, такие как HDLC и PPP, описаны в главе 9. Типы кадров для IEEE-архитектур, например Ethernet и Token Ring, рассматривались в главе 2. Процесс обрамления пакета данных напоминает вложение письма в конверт. Для сети LAN таким «конвертом» (то есть хранилищем данных) будут кадры Ethernet. В случае сети WAN информация помещается в кадры («конверты») HDLC до тех пор, пока не пройдет через соединение WAN.

Таблица 12.1. Типы кадров Ethernet

Тип кадра Ethernet	Применение	Команда операционной системы Cisco IOS
Ethernet 802.3	Применяется в ранних версиях NetWare (2/3.11). Данный тип кадра устанавливается по умолчанию, когда на маршрутизаторе задействуется IPX-маршрутизация	`novell-ether`
Ethernet 802.2	Устанавливается по умолчанию для версий NetWare 3.12/5.x	`sap`
Ethernet II	Используется в сетях, работающих с протоколами TCP/IP и/или DECnet	`arpa`
Ethernet SNAP	Используется в сетях, работающих с протоколами TCP/IP и/или AppleTalk	`snap`

Для одного интерфейса маршрутизатора разрешается указать несколько типов кадров, но при этом каждому кадру требуется отдельный номер сети. При маршрутизации различных типов кадров через один интерфейс приходится пользоваться *виртуальными сетями* (если вы проверите номер сети на сервере NetWare, то заметите, что у каждого типа кадра Ethernet свой номер сети).

Таким образом, при конфигурировании интерфейса LAN для IPX-маршрутизации необходимо сообщить номер сети IPX и назначить тип (или типы) кадра на интерфейсе. Адрес узла задается автоматически как аппаратный MAC-адрес интерфейса.

Операционная система Novell NetWare поддерживает различные типы кадров не только для архитектуры Ethernet, но и для архитектур Token Ring и FDDI. Применительно к архитектуре Token Ring поддерживаются кадры Token Ring (стандартные кадры) и Token Ring SNAP; применительно к архитектуре FDDI – кадры SNAP, FDDI 802.2 и FDDI RAW (кадры архитектуры FDDI, которые не соответствуют спецификациям IEEE).

Конфигурирование IPX-маршрутизации для интерфейса LAN выполняется следующим образом:

1. В приглашении привилегированного режима наберите команду `config t`, затем нажмите клавишу **Enter**. Вы войдете в режим общей конфигурации.
2. Чтобы сконфигурировать порт Ethernet (например, Ethernet 0) для IPX-маршрутизации, поместите в строке конфигурации команду `interface ethernet 0` и нажмите **Enter**. Строка конфигурации примет вид config-if, после чего можно вводить информацию об IPX-маршрутизации для интерфейса.
3. Напечатайте команду `ipx network: [network number] encapsulation [frame type]`, где параметр `[network number]` – это номер сети NetWare, который вам сообщил администратор. Укажите также значение `[frame type]` (тип кадра). Допустим, что интерфейс Ethernet подсоединяется к сети Novell, которая работает под управлением ОС Novell IntraNetWare 4.11. Данная операционная система применяет тип кадра Ethernet 802.2 (такое обрамление задается командой `sap` маршрутизатора Cisco). Команда будет выглядеть следующим образом: `ipx network f87c2e0f encapsulation sap` (рис. 12.8). Нажмите клавишу **Enter** и выполните команду.

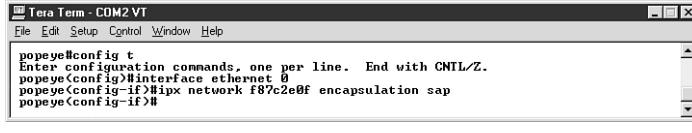


Рис. 12.8. Чтобы сконфигурировать интерфейс LAN для IPX-маршрутизации, необходимо ввести номер сети и тип кадра

4. Для выхода из режима конфигурации воспользуйтесь клавишами **Ctrl**+**Z**.
5. Нажав **Enter**, вернитесь в привилегированный режим.

Рассмотрим конфигурирование одного интерфейса для IPX-маршрутизации. Например, чтобы проверить конфигурацию интерфейса Ethernet 0 (который был настроен для IPX-маршрутизации), введите команду `show ipx interface Ethernet 0` и нажмите клавишу **Enter**. На рис. 12.9 вы видите информацию о конфигурации интерфейса Ethernet 0 для IPX-маршрутизации на маршрутизаторе 2505.

Чтобы просмотреть все интерфейсы, для которых была настроена IPX-маршрутизация, введите команду `show ipx interface` и нажмите клавишу Enter. Появится список всех интерфейсов с номерами сетей и типами кадров.

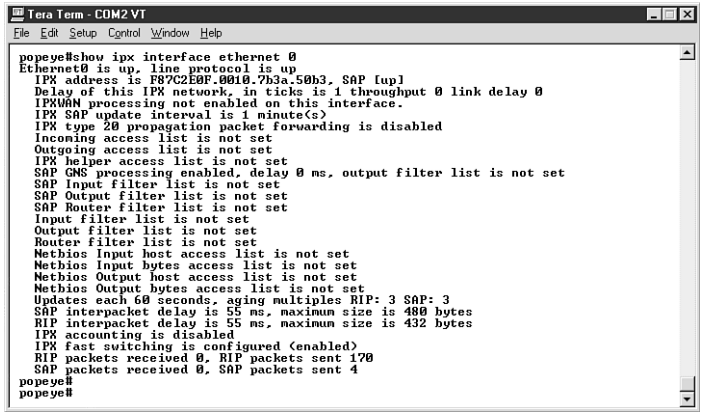


Рис. 12.9. Проверка номера сети и типа кадра на интерфейсе маршрутизатора

➢ Подробнее об операционной системе Cisco IOS и различных режимах этой системы рассказывается в главе 9.

Интерфейсы WAN

Последовательные интерфейсы (применяющие протоколы WAN) конфигурируются для IPX-маршрутизации аналогично интерфейсам LAN. Так как протоколы WAN используют собственные типы кадров (а именно тот тип кадра, который поддерживается соответствующим протоколом WAN), нет необходимости задавать тип кадра вместе с номером сети, как при конфигурировании интерфейсов LAN. Тип кадра для интерфейсов WAN[1] назначается отдельной командой, в которой следует указать тип кадра WAN, например PPP или Frame-Relay. По умолчанию устанавливается тип HDLC (в главе 15 рассказывается, как задавать различные типы кадров, в частности HDLC, Frame-Relay и PPP, для протоколов WAN).

На рис. 12.10 показаны параметры конфигурации для интерфейса Serial 0 маршрутизатора 2505. При конфигурировании последовательных интерфейсов не забывайте, что два связанных между собой последовательных порта (два маршрутизатора, включенных через последовательные интерфейсы соединением

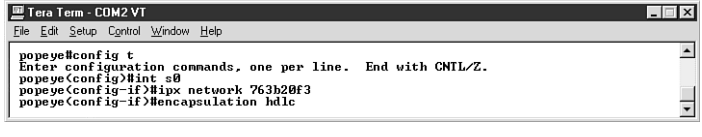


Рис. 12.10. IPX-конфигурация последовательного интерфейса

[1] Иначе называемый *типом инкапсуляции*. – *Прим. научн. ред.*

Frame-Relay) должны находиться в одной сети IPX. Этим IPX-маршрутизация похожа на IP-маршрутизацию, требующую, чтобы два соединенных последовательных порта размещались в одной подсети IP.

➢ Подробнее о таких протоколах WAN, как HDLC и PPP, говорится в главе 3 (раздел «Другие протоколы глобальных сетей»).

Мониторинг IPX-маршрутизации

Завершив конфигурацию одного или нескольких маршрутизаторов для IPX-маршрутизации, вы можете просмотреть таблицы маршрутизации IPX. В них указаны сети, к которым маршрутизатор подсоединен напрямую, а также сети, информацию о которых он получил от других устройств. Введите в приглашении пользовательского или привилегированного режима команду `show ipx route` и нажмите клавишу **Enter**.

На рис. 12.11 представлена таблица маршрутизации IPX маршрутизатора 2505, который подключен к другому маршрутизатору 2505 через последовательное соединение. Заметьте, что две сети (763B20F3 и F87C2E0F, они обозначены буквой «C») напрямую связаны с маршрутизатором, а сеть B86C033F, подсоединенная к интерфейсу Ethernet 0 другого маршрутизатора, фигурирует в информации таблицы маршрутизации. До нее можно дойти за семь временных интервалов и один переход (7/1).

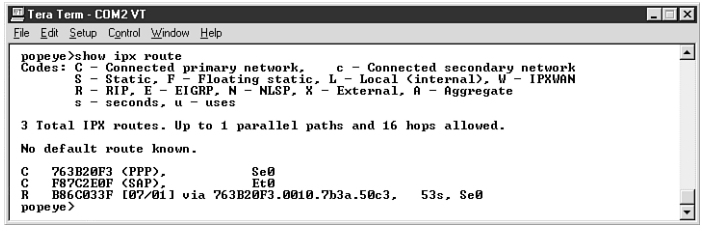


Рис. 12.11. Таблица маршрутизации IPX маршрутизатора

Данная сеть включена в таблицу маршрутизации, поскольку маршрутизатор получил сведения о ней от своего соседа. Это основной принцип, по которому строятся таблицы IPX, независимо от протокола маршрутизации. Соединенные между собой маршрутизаторы обмениваются всей информацией о структуре сети.

Для мониторинга IPX-маршрутизации предназначены команды `show ipx traffic` и `debug ipx routing activity`. Команда `show ipx traffic` позволяет увидеть количество и тип пакетов IPX, которые были посланы и получены маршрутизатором. На рис. 12.12 показаны формат этой команды и результат ее выполнения.

Команда `debug ipx routing activity` отличается от команд `show ipx route` и `show ipx traffic` тем, что не выводит статическую таблицу информации. С

ее помощью удается просматривать пакеты протоколов RIP и SAP, получаемые и отправляемые маршрутизатором. Эту команду следует выполнять в привилегированном режиме (рис. 12.13).

В режиме отладки никакую другую работу на маршрутизаторе проводить невозможно, потому что поступающая информация RIP и SAP будет мешать вашим действиям. Команда `no debug ipx routing activity` устранит эту проблему, запретив режим отладки IPX. Так что, разрешая этот режим, помните, как его отключить.

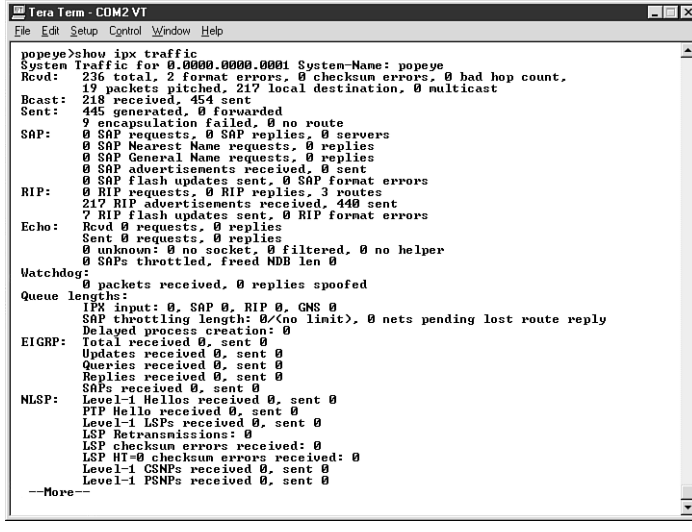


Рис. 12.12. Команда ***show ipx traffic*** позволяет увидеть отправленные и полученные пакеты IPX

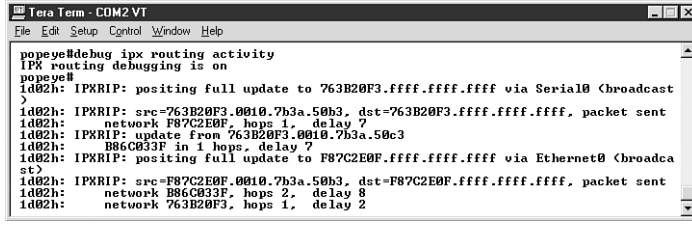


Рис. 12.13. С помощью команды ***debug*** можно просматривать пакеты обновлений протоколов RIP и SAP по мере их появления

ГЛАВА 13

Маршрутизация стека протоколов AppleTalk

Стек AppleTalk – это пакет сетевых протоколов, обеспечивающий связь между компьютерами одного типа (как правило, Apple Macintosh) для совместного доступа к файлам и принтерам. Пакет AppleTalk обладает собственной системой сетевой адресации и объединения компьютеров в логические рабочие группы, которые называются *зонами* (zones).

Поскольку практически в каждой компании или учебном заведении, которые специализируются на мультимедийных и настольных издательских средствах, имеются в наличии компьютеры Apple, возникает необходимость осуществлять маршрутизацию пакета AppleTalk через маршрутизаторы Cisco, чтобы компьютеры Macintosh могли обмениваться информацией с другими сетями.

Компьютеры Macintosh оснащаются встроенным сетевым адаптером, который присоединяется к серверу или другому устройству связи при помощи экранированного кабеля типа «витая пара» спецификации Apple (Macintosh всегда были в состоянии функционировать в сети; новые компьютеры PowerMac и G3 поставляются со встроенными портами Ethernet). Компьютеры Macintosh, работающие в других сетевых архитектурах, иногда снабжаются дополнительной сетевой картой для работы в данной сети (такой, например, как сетевая карта EtherTalk). Пакет AppleTalk поддерживает архитектуры Ethernet (EtherTalk), Token Ring (Token Talk) и FDDI (FDDITalk).

На рис. 13.1 представлены те протоколы из пакета AppleTalk, которые находятся на нижних уровнях модели OSI. Компьютеры и маршрутизаторы в сети используют их для обмена информацией о местонахождении ресурсов (серверов или принтеров). Ниже приводится список указанных протоколов и их описания:

- *протокол доставки датаграмм* (Datagram Delivery Protocol – DDP) – протокол сетевого уровня, отвечающий за функционирование системы доставки датаграмм, аналогично UDP в стеке TCP/IP;
- *протокол преобразования адресов* (AppleTalk Address Resolution Protocol – AARP) – протокол сетевого уровня, используемый для преобразования сетевых адресов AppleTalk в аппаратные адреса. AARP посылает сообщения на все станции сети, чтобы сопоставить аппаратные адреса с сетевыми;

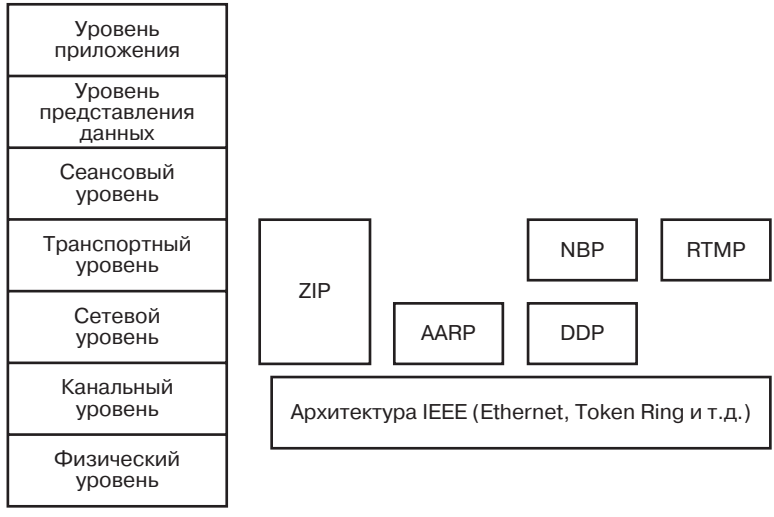


Рис. 13.1. Протоколы стека AppleTalk, относящиеся к маршрутизации, в соответствии с моделью OSI

- *протокол информации о зонах* (Zone Information Protocol – ZIP) – протокол сетевого и транспортного уровня, который служит для присвоения сетевых адресов узлам связи. Более подробно этот протокол описан в следующем разделе;
- *протокол поддержки таблицы маршрутизации* (Routing Table Maintenance Protocol – RTMP) – протокол транспортного уровня, обеспечивающий создание и поддержку таблиц маршрутизации на маршрутизаторах, которые работают с пакетами AppleTalk. Маршрутизаторы периодически проводят широковещательную рассылку информации о таблицах маршрутизации соседним устройствам, предоставляя тем самым сведения о местоположении сетей AppleTalk в общей сети;
- *протокол привязки имен* (Name Binding Protocol – NBP) – протокол транспортного уровня, который позволяет установить соответствие между адресами низших уровней и именами AppleTalk, идентифицирующими конкретные сетевые ресурсы. По этим именам удается определить, какой именно сетевой ресурс доступен в объединенной сети.

➢ Подробнее о стеке AppleTalk в применении к другим сетевым архитектурам рассказывается в главе 2, раздел «Протокол AppleTalk».

Адресация в стеке протоколов AppleTalk

Стек протоколов AppleTalk применяет 24-битную схему адресации, которая определяет, к какому сегменту сети относится данный узел, а также идентифицирует сам адрес узла, что дает возможность распознать рабочую станцию или сервер.

Адрес сети занимает 16 бит, а адрес узла в адресе AppleTalk – 8 бит. Количество битов для адреса сети и адреса узла всегда фиксировано, поэтому, в отличие от сетей IP, в AppleTalk нельзя создать подсеть. Адрес AppleTalk для одного узла в формате десятичных знаков записывается так: сеть.узел.

Администратор присваивает различным сетям AppleTalk адреса. Это может быть один номер для одной сети в одном физическом сегменте или несколько номеров, показывающих количество сетей в таком сегменте. Например, адрес сети 10–10 обозначает, что в физическом сегменте, к которому подключены компьютеры, серверы и принтеры, существует только одна сеть (сеть 10). Диапазон адресов 100–130 указывает на наличие нескольких сетей. Такой диапазон называется *диапазоном кабеля* (cable range).

Сегмент сети AppleTalk с несколькими сетями, имеющими разные адреса, называется *расширенным сегментом*. Если же в нем только одна сеть, он именуется *нерасширенным*. Расширенный сетевой сегмент может содержать до 253 адресов узлов на каждый из адресов сетей, назначенных для данной сети. На рис. 13.2 показана объединенная сеть AppleTalk с крупной локальной сетью (LAN), состоящей из расширенных сегментов, а также с локальной сетью (LAN), включающей в себя один нерасширенный сегмент. Поскольку сегменту разрешается присваивать различные адреса сетей (каждая сеть ограничена 253 узлами), на одном сегменте сети может быть размещено множество узлов. Восьмибитный адрес узла ограничивает число доступных узлов, поэтому чем больше доступных сетей в сегменте, тем больше узлов в нем можно разместить.

Сетевому администратору очень легко работать с адресами узлов связи AppleTalk, поскольку они имеют динамическое присвоение. Когда к сети подключается компьютер Macintosh, он посылает запрос по протоколу ZIP и определяет доступный сетевой номер (или диапазон номеров) в сети. При этом генерируется произвольный номер узла. Узел отправляет *запрос протокола AARP*, чтобы узнать, занят полученный номер или нет.

> *Как уже отмечалось, компьютеры Macintosh применяют динамическое присвоение адресов узлам в сети. Совершенно иная методика используется в пакете Novell NetWare (при работе с протоколами IPX/SPX). Здесь адрес узла связи назначается статически при помощи аппаратного адреса компьютера Macintosh.*

Если выбранный для конкретного адреса сети адрес узла уже выделен, компьютер сгенерирует другой произвольный адрес узла и повторно пошлет запрос протокола AARP. Обнаружив, что все номера узлов в данной сети уже распределены, компьютер назначит новый адрес сети и попытается занять произвольный адрес узла в этой сети (в том случае, если были сконфигурированы расширенные сегменты).

После того как компьютер найдет номер сети и соответствующий доступный номер узла, он будет пользоваться данным адресом (сеть.узел связи) в качестве

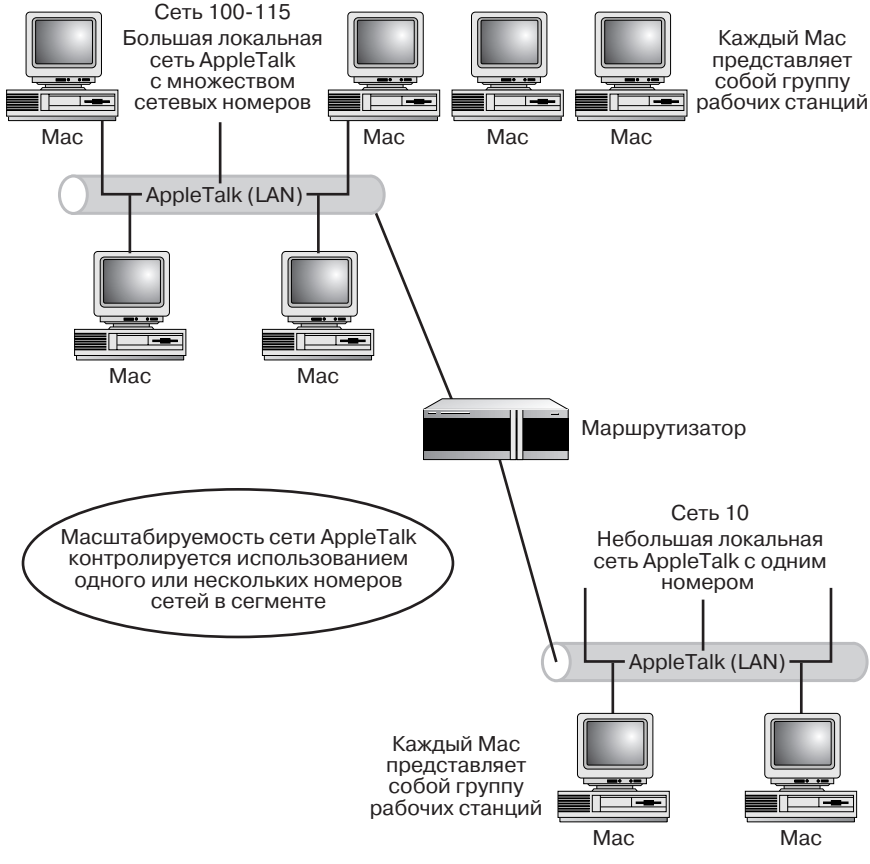


Рис. 13.2. Сегменты сети AppleTalk, соединенные маршрутизатором

Существуют две различные версии пакета AppleTalk. В версии 1 сегменту может быть присвоен только один адрес сети. Количество узлов в сети, как и количество серверов, ограничено числом 127, поэтому к такой сети может быть подсоединено не более 254 компьютеров. В версии 2 сети в одном физическом сегменте можно назначать разные адреса сетей и размещать в нем неограниченное количество узлов связи и серверов. Версия 2 также позволяет создавать в сети различные зоны. При описании пакета AppleTalk в данной главе предполагается, что вы используете версию 2, которая представляет собой схему присвоения адресов для правильной конфигурации маршрутизаторов Cisco с последующей маршрутизацией в сетях AppleTalk.

постоянного сетевого адреса. Например, компьютер в сети 10, который занимает номер узла связи 200, будет иметь постоянный адрес 10.200.

➢ Сведения о разделении сетей IP на подсети были приведены в главе 10 (раздел «Работа с подсетями»).

Зоны в сетях AppleTalk

Стек протоколов AppleTalk предоставляет еще одно средство управления сетью – возможность разделения ее на зоны. *Зоны* – это логические группы пользователей, принцип организации которых аналогичен принципу рабочих групп в сетях Microsoft. Рассмотрим такой пример: сотрудники издательской группы работают на разных этажах здания, при этом несколько пользователей находятся в отделе маркетинга, другие – в отделе публикаций и т.д. Хотя компьютеры всех ваших пользователей принадлежат к разным сегментам сети AppleTalk, вы можете объединить их в логическую сетевую группу – *логическую зону*.

Сгруппировав компьютеры всех сотрудников издательской группы в логическую зону «издатели», вы предоставите им доступ к сетевым ресурсам, расположенным на разных этажах здания. Маршрутизаторы, для которых задействована AppleTalk-маршрутизация, сформируют *таблицы зон*. Такие таблицы будут передаваться от одного сегмента сети к другому при условии, что они являются частью одной логической зоны.

Названия зон фиксированы и содержат цифровые и буквенные обозначения. Для зоны допустимо название Marketing1 или desktopA1. На рис. 13.3 проиллюстрирован принцип объединения сегментов сети LAN AppleTalk в одну зону.

Стек протоколов AppleTalk резервирует некоторые номера узлов из диапазона 0–255, а именно номера 0, 254 и 255. Номер узла 0 предназначен для временного использования узлами, которые пытаются определить, в какой сети они находятся. Номера узлов 254 и 255 служат для широковещательной рассылки в сети, поэтому не могут быть заданы собственно узлам.

Конфигурирование AppleTalk-маршрутизации

После того как вы включите поддержку AppleTalk и соответствующим образом сконфигурируете интерфейсы, маршрутизаторы построят таблицы маршрутизации, которые (во многом аналогично таблицам в сетях IP) будут содержать сведения о маршрутах к различным сетям. Такие таблицы позволяют устройствам

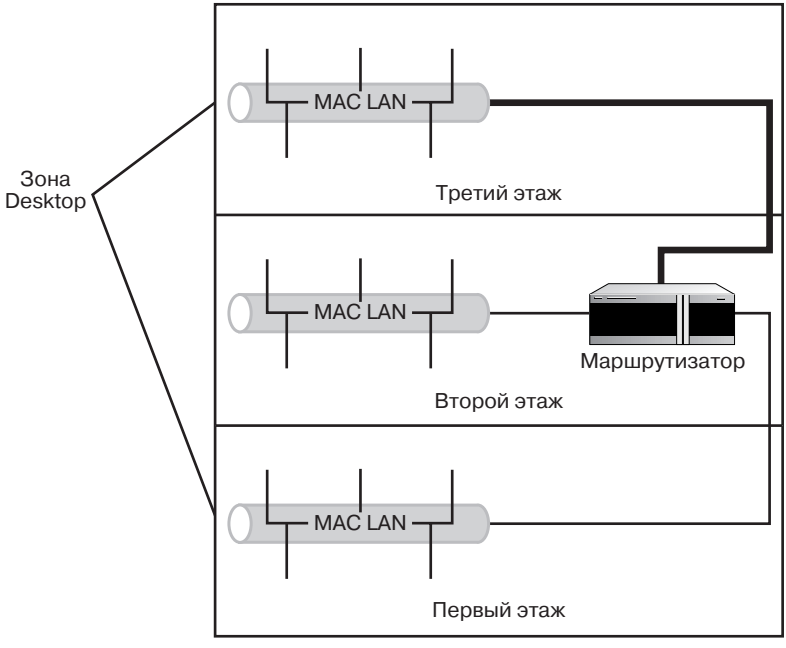


Рис. 13.3. Зоны AppleTalk можно использовать для объединения нескольких сетевых сегментов в одну логическую рабочую группу

Стек протоколов AppleTalk так же сложен и многопрофилен, как стек TCP/IP или IPX/SPX. Вам, наверное, придется иметь дело с AppleTalk реже, чем с другими стеками сетевых протоколов, однако AppleTalk распространен достаточно широко. Причина в том, что компьютеры Apple Macintosh повсеместно применяются в сфере настольных издательских средств и мультимедиа. Поскольку настоящая книга посвящена работе маршрутизаторов, стек протоколов AppleTalk здесь рассматривается лишь в самых общих чертах, в частности схема AppleTalk-адресации показана только применительно к маршрутизации. Более подробную информацию о стеке протоколов AppleTalk можно найти в Web-библиотеке компании Apple Macintosh, расположенной по адресу http://til.info.apple.com, или на сайте www.cisco.com (здесь также представлены сведения о системе Cisco IOS).

в сети доставлять пакет маршрутизатору, непосредственно обслуживающему сеть узла-адресата.

Прежде чем конфигурировать интерфейсы для AppleTalk-маршрутизации, включите ее посредством команды глобальной конфигурации:

1. В приглашении привилегированного режима введите команду `config t`, затем нажмите клавишу **Enter**.
2. Наберите команду `appletalk routing` и снова нажмите **Enter** (рис. 13.4).

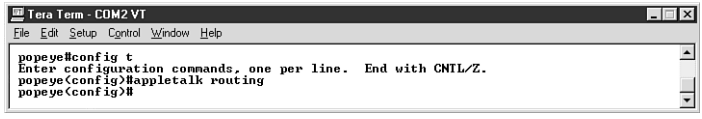


Рис. 13.4. Прежде чем конфигурировать интерфейсы, включите AppleTalk-маршрутизацию

3. Чтобы выйти из режима конфигурации, воспользуйтесь клавишами **Ctrl**+**Z**.
4. Нажмите **Enter** для возвращения в привилегированный режим.

При включении AppleTalk-маршрутизации в качестве протокола маршрутизации автоматически назначается RTMP, поэтому в данном случае, в отличие от протокола RIP и других протоколов маршрутизации IP, нет необходимости конфигурировать его отдельно.

Включив AppleTalk-маршрутизацию, вы можете сконфигурировать те интерфейсы, которые будут участвовать в маршрутизации пакетов AppleTalk. Для каждого интерфейса необходимо задать диапазон кабеля (количество сетей на каждом сегменте) и задействованные зоны AppleTalk. На рис. 13.5 показаны две различные сети, соединенные посредством маршрутизаторов 2505.

Каждая сеть LAN использует диапазон кабеля (который увеличивает количество доступных для адресации узлов), а соединение WAN применяет один адрес сети (он должен быть сконфигурирован для последовательного порта каждого подключенного маршрутизатора). Чтобы упростить работу, соединению WAN присваивается название зоны: Wanconnect.

В табл. 13.1 обобщена информация о конфигурировании сети AppleTalk, представленная на рис. 13.5. В двух следующих разделах рассказывается о конфигурировании интерфейсов WAN и LAN для AppleTalk-маршрутизации, а описанная конфигурация послужит в качестве примера.

Таблица 13.1. Информация о конфигурации сети AppleTalk

Маршрутизатор	Интерфейс	Диапазон кабеля	Зона
1 (Popeye)	Ethernet 0 Serial 0	1–10 11	Desktop Wanconnect
2 (Olive)	Ethernet 0 Serial 0	12–20 11	Multimedia Wanconnect

Конфигурирование интерфейсов LAN

Конфигурирование интерфейсов LAN для AppleTalk во многом похоже на конфигурирование IP или IPX. Необходимо ввести в режиме конфигурации информацию о сети и зоне для конфигурируемого интерфейса.

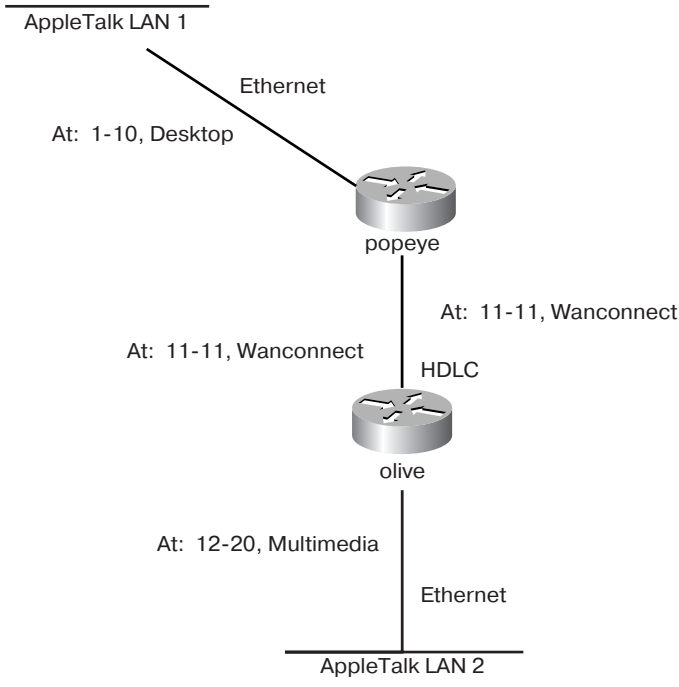


Рис. 13.5. Объединить две сети LAN AppleTalk можно посредством двух маршрутизаторов, которые связаны через последовательные порты по выделенной линии с соответствующим протоколом WAN

Процедура конфигурирования интерфейса LAN для AppleTalk выполняется следующим образом:

1. В приглашении привилегированного режима поместите команду `config t`, затем нажмите клавишу **Enter**. Тем самым вы войдете в режим общей конфигурации.
2. Наберите команду `interface ethernet 0` (помните, что команды можно сокращать) и нажмите **Enter**.
3. В приглашении config-if напечатайте команду `appletalk cable-range 1-10`, потом нажмите **Enter**. Укажите тот диапазон кабеля, который вы задали для сети LAN AppleTalk. Таким образом вы устанавливаете диапазон кабеля для сети LAN, подсоединенной к интерфейсу LAN маршрутизатора.
4. Чтобы назначить зону для интерфейса, воспользуйтесь командой `appletalk zone desktop`. Параметр `desktop` – это имя зоны сети LAN. Впишите имя вашей зоны. Затем нажмите **Enter** (рис. 13.6).
5. Для выхода из режима конфигурации воспользуйтесь клавишами **Ctrl**+**Z**.
6. Нажмите **Enter** и вернитесь в привилегированный режим.

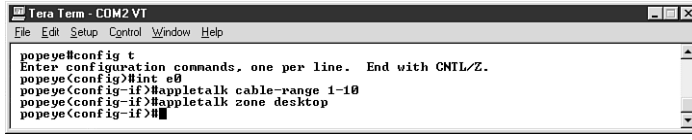


Рис. 13.6. При конфигурировании интерфейсов LAN необходимо ввести информацию о сети и зоне

Вам придется повторить эти действия для всех интерфейсов LAN, которые вы желаете сконфигурировать для AppleTalk-маршрутизации. Нужно правильно указать диапазон кабеля и информацию о зоне для каждого интерфейса: если вы ошибетесь, повторно указав один и тот же диапазон кабеля, результат будет таким же, как при использовании одного IP-адреса для двух интерфейсов маршрутизатора – маршрутизация между сетями не станет работать.

> *В приведенном примере мы рассмотрели конфигурирование AppleTalk для LAN-интерфейса Ethernet. Кроме того, AppleTalk поддерживает Token Ring и DDI. Поэтому, если вы конфигурируете интерфейс Token Ring (первый интерфейс маршрутизатора) для AppleTalk-маршрутизации, вам необходимо предоставить информацию о сети и зоне для интерфейса Token Ring 0.*

Конфигурирование интерфейсов WAN

Конфигурирование интерфейсов WAN достаточно легко: следует сконфигурировать все последовательные порты на всех маршрутизаторах для соответствующего протокола WAN и указать для интерфейсов сведения о сети и зоне. Последовательные интерфейсы двух соединенных маршрутизаторов необходимо сконфигурировать таким образом, чтобы оба маршрутизатора находились в одной сети и зоне (аналогично случаю IP-маршрутизации, когда оба маршрутизатора должны иметь связанные между собой последовательные интерфейсы в одной подсети IP).

Конфигурирование интерфейсов WAN для AppleTalk-маршрутизации осуществляется так:

1. В приглашении привилегированного режима поместите команду `config t`, затем нажмите клавишу **Enter**. Вы окажетесь в режиме общей конфигурации.
2. Введите команду `interface serial 0` (команды можно сокращать) и нажмите **Enter**.
3. В строке config-if наберите команду `appletalk cable-range 11` и снова нажмите клавишу **Enter**. Задайте тот диапазон кабеля, который вы определили для соединения WAN.
4. Чтобы указать зону для последовательного интерфейса, напечатайте команду `appletalk zone wanconnect`, где `wanconnect` – имя, которое применя-

ется в качестве имени зоны для последовательного соединения, а также для напоминания о том, что это соединение WAN. Нажмите **Enter** (рис. 13.7).

5. Для выхода из режима конфигурации воспользуйтесь клавишами **Ctrl**+**Z**.
6. Нажмите **Enter**, чтобы вернуться в привилегированный режим.

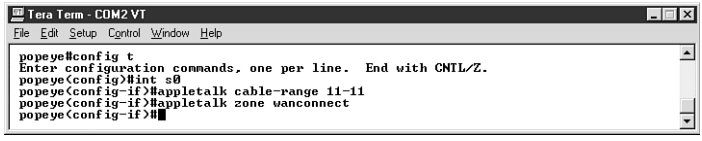


Рис. 13.7. При конфигурировании интерфейсов WAN следует задать информацию о сети и зоне

➢ О конфигурировании наиболее часто используемых на маршрутизаторах Cisco протоколов WAN говорится в главе 15.

Мониторинг AppleTalk-маршрутизации

Включив AppleTalk-маршрутизацию и сконфигурировав интерфейсы, вы получаете возможность пользоваться таблицами маршрутизации AppleTalk и просматривать конфигурацию различных интерфейсов, а также сведения о трафике AppleTalk в сети, в частности список пакетов, которые маршрутизатор получил и отправил.

Чтобы вывести таблицу маршрутизации, наберите команду `show appletalk route` в приглашении пользовательского или привилегированного режима и нажмите клавишу **Enter**. На рис. 13.8 представлена таблица маршрутизации на маршрутизаторе 2505, у которого интерфейс Ethernet 0 связан с сетью LAN AppleTalk, а интерфейс Serial 0 – с другим маршрутизатором 2505 через последовательное соединение. Диапазоны сетей, помеченные буквой «C», подключены напрямую к маршрутизатору. Диапазон сети 12–20, обозначенный буквой «R», – это другая сеть LAN AppleTalk, связь с которой осуществляется через последовательное соединение с другим маршрутизатором (схема соединения маршрутизаторов представлена на рис. 13.5).

Мониторинг AppleTalk-маршрутизации на маршрутизаторе реализуется с помощью еще нескольких команд `show`. Вы можете познакомиться с информацией

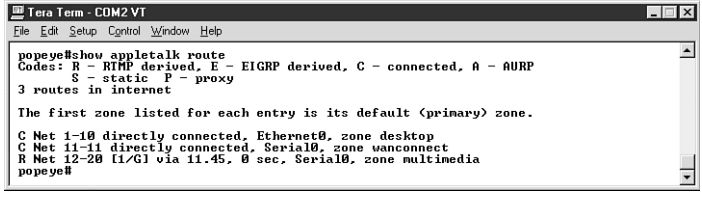


Рис. 13.8. Просмотр таблицы маршрутизации на маршрутизаторе

об одном интерфейсе или просмотреть сведения о конфигурации всех интерфейсов, которые поддерживают AppleTalk-маршрутизацию, а также о зонах AppleTalk и связанных с ними диапазонах сетей. Табл. 13.2 содержит список этих команд (они вводятся в приглашении пользовательского или привилегированного режима).

Таблица 13.2. Команды `show appletalk`

Команда	Функция
`Show appletalk interface brief`	Предоставляет краткие сведения по всем интерфейсам маршрутизатора и их конфигурации для стека протоколов AppleTalk
`Show appletalk interface`	Дает подробную информацию по всем интерфейсам маршрутизатора и их конфигурации для стека протоколов AppleTalk
`Show appletalk interface e0`	Позволяет просмотреть подробные сведения по конфигурации AppleTalk для указанного интерфейса маршрутизатора
`Show appletalk zone`	Предоставляет данные о зоне и сети для зоны, доступной в объединенной сети
`Show appletalk global`	Выводит информацию о количестве сетей и зон, которые доступны в объединенной сети, а также о временных интервалах для запросов протокола ZIP и сообщений протокола RTMP

Если вы читали главы данной книги по порядку, то, вероятно, заметили, что команды `show`, приведенные в табл. 13.2, аналогичны командам `show`, которыми мы пользовались для просмотра конфигурационной информации IP и IPX/SPX. Освоив эти команды, вы сможете познакомиться с конфигурацией любого маршрутизатора для любого сетевого протокола.

На рис. 13.9 показан результат исполнения команды `show appletalk interface brief`, на рис. 13.10 – команды `show appletalk zone`, а на рис. 13.11 – команды `show appletalk global`.

Разрешается также включить режим отладки протокола RTMP AppleTalk и просматривать все пакеты его обновлений, отправленные и полученные маршрутизатором. Напечатайте в приглашении привилегированного режима команду `debug apple routing` и нажмите клавишу **Enter**. На рис. 13.12 демонстрируется результат выполнения этой команды. Чтобы выключить режим отладки, наберите команду `no debug apple routing` и нажмите **Enter**: в противном случае вам будет трудно вводить следующие команды.

Вы видите, что стек протоколов AppleTalk функционирует с маршрутизацией настолько же эффективно, насколько и стеки IP и IPX. Кроме того, AppleTalk предоставляет такие функции, как работа с зонами и расширенными сетями, что позволяет упростить создание крупных сетей. Однако первое место среди стеков сетевых протоколов по-прежнему занимает IP (второе место принадлежит стеку IPX), поэтому вы, скорее всего, будете редко сталкиваться с протоколами стека AppleTalk.

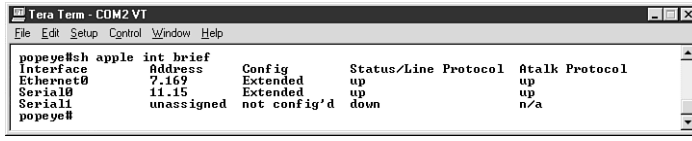


Рис. 13.9. Используйте команду ***show appletalk interface brief*** для просмотра конфигурации интерфейсов маршрутизатора

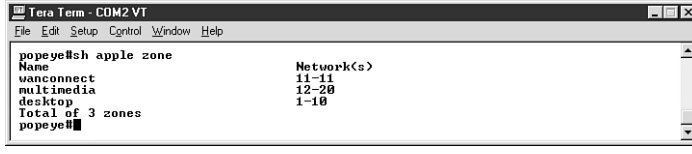


Рис. 13.10. С помощью команды ***show appletalk zone*** можно познакомиться со сведениями о зоне и сети

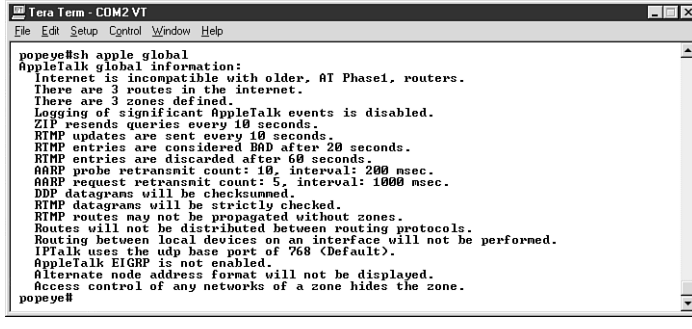


Рис. 13.11. Команда ***show appletalk global*** предназначена для отображения общей конфигурации AppleTalk на маршрутизаторе

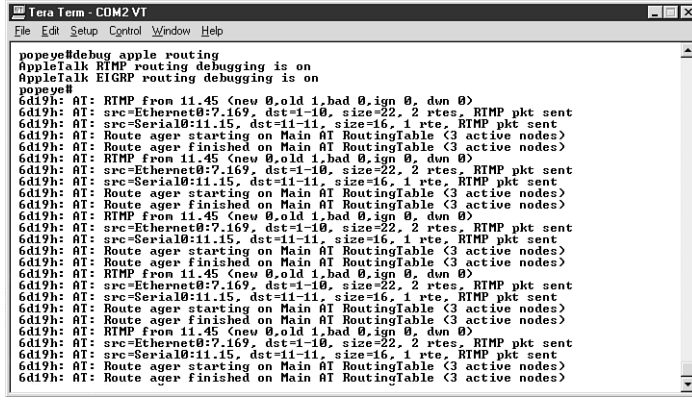


Рис. 13.12. Результат выполнения команды ***debug apple routing***

ЧАСТЬ IV

Дополнительные возможности конфигурирования

ГЛАВА 14

Фильтрация трафика маршрутизатора при помощи списков доступа

Итак, вы уже знаете, как на маршрутизаторе Cisco конфигурируются три различных протокола LAN – TCP/IP, IPX/SPX и AppleTalk. Мы также обсудили, как конфигурировать интерфейсы и создавать сеть, которая поддерживает данные типы протоколов.

После того как вы сконфигурируете маршрутизаторы, ваша сеть станет напоминать проходную комнату с настежь распахнутыми дверями. Пакеты будут свободно отправляться и приниматься на любом порте маршрутизатора; похоже, что вы создали город без мэра. При управлении маршрутизаторами и сетью крайне важно закрывать доступ для некоторых пакетов, а также контролировать, какие интерфейсы на каких маршрутизаторах вашей сети оказались доступными для трафика от определенных узлов или целых сетей.

Справиться с этой задачей вам помогут списки доступа. *Список доступа* представляет собой перечень особых предписаний, называемых *предписаниями «разрешить»* (permit) и *«отклонить»* (deny), которые позволяют регулировать трафик на маршрутизатор и от него (они способны также управлять доступом пользователей по протоколу Telnet[1]). Предписание «разрешить» означает, что пакеты, отвечающие известным требованиям, будут пропущены. Другими словами, им будет разрешено дальнейшее движение. Предписание «отклонить» (в соответствии с каким-либо критерием, например IP-адресом или адресом сети IPX) указывает на то, что пакет необходимо отсортировать или удалить.

Списки доступа могут применяться для запрещения продвижения пакетов на определенный интерфейс маршрутизатора или от него, а также для ограничения доступа некоторых пользователей и устройств к сетевым ресурсам.

[1] Это очень важный момент, и администратор сети при конфигурации защиты практически всегда выполняет настройку доступа к устройству Cisco по протоколу Telnet. – *Прим. научн. ред.*

Списки доступа – интереснейшая тема исследования. Они предоставляют большие возможности по управлению потоками данных в сети. Освоить все принципы работы со списками доступа – нелегкая задача. В настоящей главе дана вводная информация по этой теме, а также представлены стандартные списки доступа (вам, скорее всего, потребуются списки доступа IP, поскольку IP – самый популярный маршрутизируемый протокол в мире). Для сетевых протоколов IP и IPX также могут быть созданы расширенные списки доступа. Если вам нужна дополнительная информация, посетите сайт www.cisco.com или обратитесь к представителю местного учебного центра Cisco (обучение доступно и через Web-сайт Cisco). В учебных центрах проводятся курсы, на которых вы сможете получить дополнительные сведения по маршрутизаторам и операционной системе Cisco IOS.

Списки доступа

Как указывалось ранее, списки доступа – это наборы из условных предписаний, которые могут запретить пакетам доступ из сети на маршрутизатор или с маршрутизатора в какую-либо сеть при выполнении определенных условий. Каждое из предписаний в таком списке читается по порядку, то есть новый входящий пакет будет последовательно сравниваться со всеми критериями в списке доступа с начала списка до конца.

Пакеты, которым отказано в доступе, отбрасываются, а те, доступ для которых разрешен, пропускаются. Если пакет, пришедший на маршрутизатор, не соответствует первому предписанию в списке доступа (а это может быть как директива «отклонить», так и директива «разрешить»), то он сравнивается со следующим предписанием.

Процесс сопоставления пакета и списка доступа продолжается до тех пор, пока одно из предписаний не окажется выполненным, и тогда пакет будет либо пропущен, либо отброшен. На рис. 14.1 продемонстрирован процесс сопоставления пакета и предписаний «отклонить» и «разрешить» в списке доступа.

Пакет, пропущенный на входном интерфейсе (на основании списка доступа, созданного для этого интерфейса), затем может быть проверен списком доступа на выходном интерфейсе того же маршрутизатора. Это означает, что фильтровать пакеты разрешается и при получении, и при отправлении.

Например, если требуется, чтобы определенные пакеты не попали на маршрутизатор, заблокируйте им доступ на соответствующий интерфейс, скажем на Ethernet, подсоединенный к сети LAN. Вы также можете сортировать пакеты в момент, когда они уходят с маршрутизатора. Допустим, нужно запретить отправку некоторых пакетов с последовательного интерфейса, связанного с другим маршрутизатором через медленное соединение WAN. Вы имеете право назначить

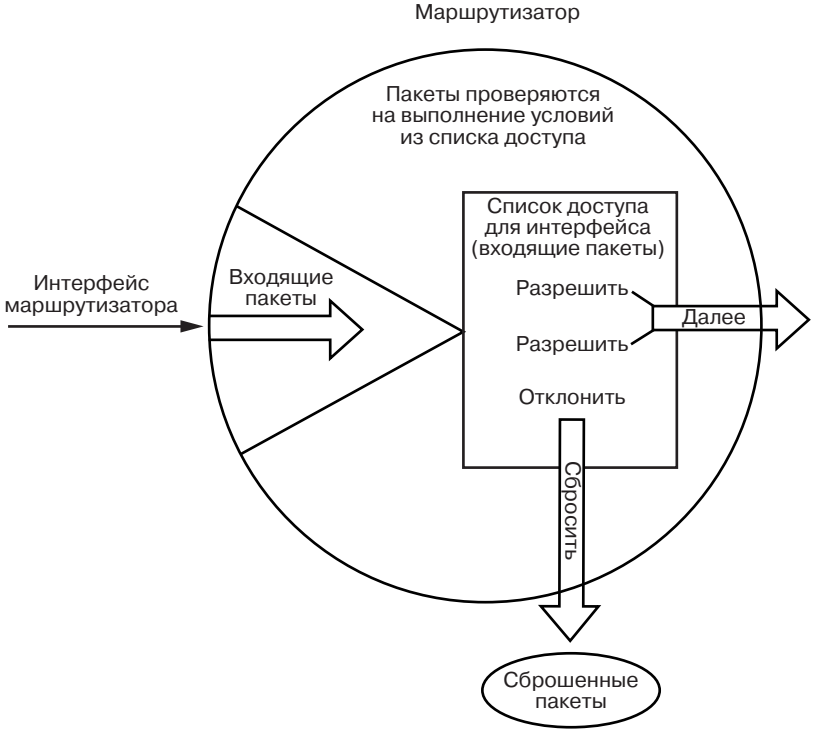


Рис. 14.1. В зависимости от предписаний в списке доступа пакеты либо пропускаются, либо отбрасываются

этому интерфейсу фильтр, который не будет пропускать через последовательный интерфейс пакеты с определенным адресом.

Создание списка доступа

Разрешается составить список доступа для любого интерфейса маршрутизатора. Однако каждый сетевой протокол, поддерживаемый интерфейсом, ассоциируется только с одним списком доступа. Так, для порта Ethernet 0 маршрутизатора (который сконфигурирован под IP- и IPX-маршрутизацию) может существовать список доступа для фильтрации трафика IP и список доступа для фильтрации трафика IPX. Однако недопустимо, чтобы для одного интерфейса одновременно существовало два списка доступа, фильтрующих трафик IP.

Большое преимущество подобной работы состоит в возможности назначить разным интерфейсам маршрутизатора, например Ethernet 0 и Ethernet 1, один и тот же список доступа. Разрешается также указать, для фильтрации входящих

или выходящих пакетов на интерфейсе применять список доступа. Следовательно, ничто не мешает иметь список доступа на одном интерфейсе для фильтрации входящих пакетов, а на другом интерфейсе того же маршрутизатора – для фильтрации выходящих пакетов.

Создать список доступа несложно: вы просто составляете перечень директив и затем задаете его определенному интерфейсу маршрутизатора. Учтите только, что такой список должен содержать хотя бы одно предписание «разрешить».

При работе со списками доступа иногда возникают затруднения из-за наличия двух условных предписаний: «разрешить» и «отклонить». Вам придется определить, как именно вы будете распоряжаться данными директивами, чтобы корректно фильтровать трафик на маршрутизаторе.

Например, посредством предписания «разрешить» вы можете предоставлять доступ на маршрутизатор пакетам, поступающим из определенных сетей LAN вашей объединенной сети (для этого нужно указать в предписании все адреса сети, узлы которой должны получить доступ). Таким образом, в списке доступа будет несколько предписаний «разрешить». Затем требуется поместить в конце списка предписание «отклонить», которое запретит доступ для всех других сетей (это делается различными способами, в зависимости от типа трафика).

Или с помощью предписания «отклонить» запретите доступ определенным узлам или целым сетям, а потом поместите в конце списка предписания «разрешить», которые позволят узлам указанных вами сетей посылать пакеты на данный интерфейс маршрутизатора. Какую бы методику вы ни выбрали, вы не сумеете в одном предписании запретить доступ какому-либо адресу, а в другом – разрешить. Как только пакет совпадет с критерием предписания «разрешить», он сразу же будет пропущен, поэтому проверить его на соответствие следующему предписанию «отклонить» не удастся.

Создание списка доступа требует логических размышлений, а также умения таким образом размещать предписания, чтобы пропускать необходимые для маршрутизации пакеты и отсеивать ненужные. Составляя предписания, имейте в виду, что они не должны противоречить друг другу. Вы, конечно, не хотите иметь список доступа, отбрасывающий пакеты, для которых этот интерфейс – единственно возможный путь к конечному пункту. Рассмотрим некоторые сетевые протоколы и методику формирования списка доступа для каждого из них. Это поможет разобраться в принципах обращения с такими списками.

При работе со списками доступа для интерфейсов маршрутизатора, входящего в достаточно крупную сеть, придется использовать как директивы «разрешить», так и директивы «отклонить». После того как в списке доступа указаны все узлы и сети, в конце приводится обобщенное предписание «отклонить все» (deny all), запрещающее доступ для пакетов, которые не совпали ни с одним из предписаний «разрешить» или «отклонить».

Работа со списками доступа IP

Стандартный список доступа IP проверяет IP-адрес отправителя пакетов, которые должны фильтроваться на интерфейсе маршрутизатора. В качестве критерия для предписаний «разрешить» и «отклонить» в списке доступа служит IP-адрес отправителя.

При создании списка доступа, который будет использоваться на каком-либо интерфейсе маршрутизатора (например, Ethernet 0 или Serial 1), вам также необходимо указать, будет ли список доступа регулировать входящие или исходящие пакеты. На рис. 14.2 показан список доступа IP. В следующих разделах мы рассмотрим команды создания списка данных.

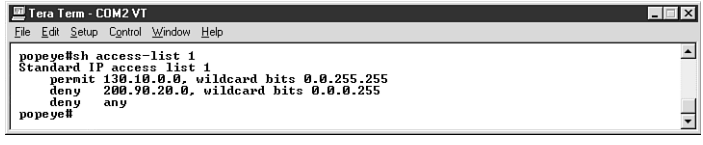


Рис. 14.2. Список доступа IP, который пакетам из одной сети разрешает доступ, а из другой – запрещает

Возьмем в качестве примера простую сеть и воспользуемся ее адресом при составлении списков доступа для некоторых интерфейсов маршрутизаторов в сети. На рис. 14.3 указана необходимая для этого информация.

Сначала займемся списком доступа для интерфейса Serial 0 маршрутизатора A. Допустим, пакеты, посланные с рабочей станции 1A узлам в сети 130.10.0.0, должны передаваться по выделенной линии между маршрутизаторами A и C. Однако вы не хотите, чтобы данное соединение WAN было маршрутом для какой-либо из сетей LAN (например, сети 200.90.20.0), обслуживаемой маршрутизатором B (поскольку маршрутизатор B напрямую связан с маршрутизатором C). Поэтому пакетам с рабочей станции A1 нужно в списке доступ разрешить, а всем другим пакетам (из других сетей LAN) – запретить.

Необходимо создать список доступа, а затем применить его на определенном интерфейсе. Но прежде чем приступить к разработке, следует изучить обобщенные маски, которые используются в списках доступа IP.

Наше знакомство со списками доступа ограничивается стандартными списками для таких протоколов, как IP. Однако вы можете применить расширенные списки доступа, чтобы провести дополнительную фильтрацию трафика данных. При работе с протоколом IP расширенные списки доступа позволяют сортировать пакеты на основе информации не только об IP-адресе отправителя, но и об IP-адресе получателя, а также на основе данных таких протоколов, как UDP и ICMP.

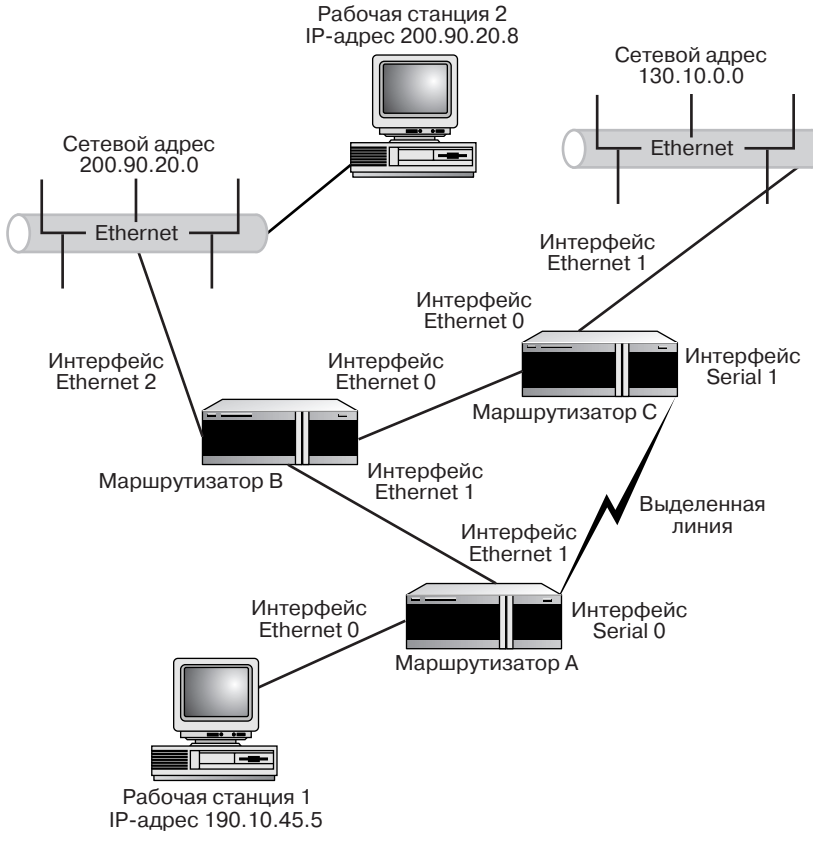


Рис. 14.3. Простая сеть, для которой требуются списки доступа

➢ Об IP-адресации рассказывалось в главе 10 (раздел «Как работать с адресами протокола IP»).

Обобщенные маски IP

IP-адреса, которые содержатся в базовых списках IP-адресов, могут быть адресами узлов, адресами подсетей или основными адресами сетей. Следовательно, нужен метод, позволяющий маршрутизатору определить, какие биты в начальном IP-адресе должны сопоставляться с адресом в списке доступа. Например, если в предписании «разрешить» или «отклонить» указан основной адрес сети 200.90.20.0, то при сопоставлении со списком доступа для определенного интерфейса маршрутизатор обязан работать именно с битами первых трех октетов.

Для этой цели предназначены *обобщенные маски* (wildcard mask). В обобщенной маске значение битов адреса, которые необходимо проверять, должно быть равно

Нужно различать обобщенные маски и маски подсети. Обобщенные маски используются только в списках доступа; их предназначение – дать маршрутизатору информацию о том, какие биты адреса сопоставлять со списком доступа.

Если вы хотите, чтобы маршрутизатор проверял на соответствие списку доступа все биты во всех октетах адреса, введите обобщенную маску 0.0.0.0 или наберите ключевое слово `host`, которое даст маршрутизатору такую же обобщенную маску из одних нулей. Если нужно распространить предписание «разрешить» или «отклонить» на все IP-адреса, не указанные в других предписаниях списка доступа, воспользуйтесь ключевым словом `any`. Оно окажется полезным, если вы применяете предписание `deny any`, которое запрещает доступ для всех IP-адресов, кроме заданных в предписаниях «разрешить».

нулю, а битов, не нуждающихся в проверке, – единице. Чтобы маршрутизатор проверял все биты первых трех октетов основного сетевого адреса, задайте обобщенную маску 0.0.0.255 (двоичный эквивалент – 00000000 00000000 00000000 11111111).

Как видите, наличие обобщенной маски упрощает работу с основными сетевыми адресами и адресами узлов. Достаточно присвоить всем битам октетов, которые вы собираетесь проверять, значение 0 (0 в десятичном представлении), а всем битам октетов, которые проверяться не будут, – значение 1 (255 в десятичной форме). Рассмотрим случай, когда вы имеете дело с сетями, разделенными на подсети. Допустим, требуется сообщить маршрутизатору, что определенным подсетям нужно разрешить доступ, а другим (из диапазона подсетей в вашей сети) – запретить. Для этого необходима обобщенная маска, которая предоставит маршрутизатору информацию о том, какие биты в IP-адресах пакетов проверять. Предположим, что сеть класса B разделена на шесть подсетей (см. табл. 14.1).

Таблица 14.1. Адреса шести подсетей в сети 130.10.0.0

Номер подсети	Адрес подсети
1	130.10.32.0
2	130.10.64.0
3	130.10.96.0
4	130.10.128.0
5	130.10.160.0
6	130.10.192.0

Составим предписание «отклонить» для подсетей 1, 2 и 3 (диапазон адресов подсетей от 130.10.32.0 до 130.10.96.0): `deny 130.10.32.0 0.0.31.255`. Здесь

после предписания «отклонить» (deny) идет IP-адрес первой подсети, а затем следует обобщенная маска. Как же удалось ее определить?

Первый октет адреса пакетов, на которые распространяется предписание «отклонить», имеет десятичное представление 130, следовательно, обобщенная маска для первого октета в двоичном представлении – 00000000, то есть 0 в десятичной форме. Это значит, что все биты в первом октете пакета должны соответствовать двоичному эквиваленту 130 (10000010). Второй октет отвечает двоичному эквиваленту 10 (00001010), поэтому его обобщенная маска в двоичном представлении – 00000000. Обобщенная маска для двух первых октетов имеет вид 0.0.

Дальше возникают сложности, поскольку из третьего октета для создания подсетей забирали биты. В подсети 1 значение третьего октета – 32, двоичный эквивалент – 00100000. Значит, в адресе каждого пакета маршрутизатор должен проверять на соответствие списку доступа третий бит третьего октета (отсчитываем восемь бит слева направо).

Во второй подсети значение третьего октета – 64 (в двоичной форме – 01000000), то есть маршрутизатор должен анализировать второй бит третьего октета. В подсети 3 значение третьего октета – 96 (двоичный эквивалент – 01100000), так что необходимо проверять второй и третий биты третьего октета.

Отсюда вывод, что обобщенная маска должна читаться слева направо как 00011111, поскольку в октете нужно анализировать первый бит (значение 128), а также второй и третий (значения 64 и 32). Проверять остальные биты, с четвертого по восьмой, нет необходимости, и их значения в обобщенной маске устанавливаются равными нулю («не проверять»). Данные биты имеют значение 16+ 8 + 4 + 2 + 1 = 31. Обобщенная маска первых трех октетов для предписания «отклонить» списка доступа будет выглядеть так: 0.0.31.

Теперь следует определить значение последнего октета обобщенной маски. Здесь приводится восьмибитная информация об адресе узла, которую анализировать не нужно (на соответствие списку доступа проверяется только третий октет). По этой причине четвертый октет будет равен двоичному значению числа 255, то есть 11111111. Обобщенную маску, запрещающую доступ всем пакетам из диапазона подсетей 130.10.32.0–130.10.96.0, можно записать как 0.0.31.255.

Помните, что обобщенная маска – это не маска подсети. Единственное их сходство состоит в том, что приходится переводить десятичные значения в двоичный код, чтобы определить, какие позиции в обобщенной маске будут представлены нулями, а какие – единицами.

Создание списка доступа

Составим список доступа, который позволяет пакетам от рабочей станции A1 (190.10.45.5) отправляться с интерфейса Serial 0 маршрутизатора A, но отбрасывает пакеты от всех других сетей IP. Закончив работу со списком, вы должны присвоить ему номер от 1 до 99.

Стандартный список доступа IP формируется следующим образом:

1. В приглашении привилегированного режима поместите команду `config t`, затем нажмите клавишу **Enter**. Вы войдете в режим глобальной конфигурации.
2. Чтобы получить первую строку списка доступа, наберите `access-list [list #] permit` или `deny [ip address] wildcard mask`; где параметр `[list #]` – это номер списка доступа от 1 до 99. Предписание может содержать параметр `permit` (разрешить) или `deny` (отклонить), но не оба сразу. Параметр `[ip address]` – это IP-адрес рабочей станции или сети. В нашем случае следует разрешить доступ для пакетов от рабочей станции A1 (190.10.45.5), поэтому команда примет вид `access-list 1 permit 190.10.45.5 0.0.0.0`. Нажмите клавишу **Enter**.
3. Доступ всем другим пакетам запретите командой `access-list 1 deny any` (рис. 14.4).

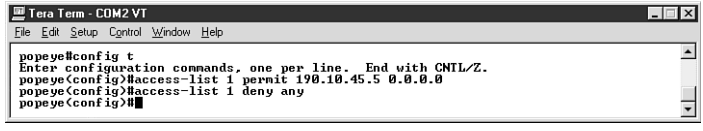


Рис. 14.4. Список доступа создается в режиме глобальной конфигурации

4. Воспользуйтесь клавишами **Ctrl**+**Z**, чтобы закончить сеанс конфигурации.
5. Нажмите **Enter** и вернитесь в привилегированный режим.

Вы можете просмотреть список доступа при помощи команды `show`. Введите в приглашении `show access-list 1` и нажмите **Enter** (рис. 14.5).

Рис. 14.5. Результат исполнения команды ***show access-list***

Присвоение интерфейсу списка доступа

Теперь, когда список доступа готов, можно приписать его определенному интерфейсу маршрутизатора, в нашем примере – интерфейсу Serial 0. Требуется также указать, что интерфейс должен проверять исходящие пакеты.

Список доступа присваивается интерфейсу Serial 0 следующим образом:

1. В приглашении привилегированного режима введите команду `config t`, затем нажмите клавишу **Enter**, чтобы войти в режим глобальной конфигурации.
2. Для входа в режим конфигурации интерфейса Serial 0 наберите команду `interface serial 0` и снова нажмите **Enter**.
3. В приглашении config-if напечатайте команду `ip access-group 1 out` (рис. 14.6). Далее нажмите **Enter**.

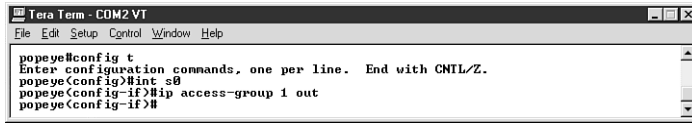


Рис. 14.6. Вы должны присвоить список доступа интерфейсу, а также указать, для входящих или исходящих пакетов предназначен этот список

4. Нажатием на клавиши **Ctrl+Z** завершите сеанс конфигурации.
5. Воспользуйтесь клавишей **Enter** для возвращения в привилегированный режим.

После того как вы присвоили интерфейсу список доступа, маршрутизатор начнет с его помощью фильтрацию входящих или исходящих пакетов. В список можно вносить дополнительные предписания «разрешить» и «отклонить». Новые директивы вводятся посредством той же команды, что и при создании первой строки списка. Они добавляются в конец списка, но перед предписанием «отклонить все» (предназначенным для блокировки тех IP-адресов, которые вы пропустили в других предписаниях «отклонить»).

Если вы обнаружили, что список доступа работает некорректно (после проверки трафика на интерфейсе), или вам нужен другой список с таким же номером, удалите свой список при помощи команды `no access-list 1`, указав номер списка доступа, который вы хотите удалить.

Создание стандартных списков доступа IPX

Стандартные списки доступа IPX разрешают или запрещают доступ пакетам в зависимости от их начального и конечного IPX-адреса. Списки доступа IPX нумеруются от 800 до 899 (данный диапазон для них зарезервирован) и имеют структуру, аналогичную структуре списков доступа IP, но на основе IPX-адресации для фильтрации входящих и исходящих пакетов.

Обычное предписание имеет вид `access list 800 deny [source network address] [destination network addess]`. Номер 800 сообщает маршрутизатору, что это список доступа IPX. Параметр `[source network address]` (сетевой адрес отправителя) – номер сети IPX, узлы которой представляют собой исходные источники пакетов. Параметр `[destination network address]` (сетевой адрес получателя) – IPX-адрес сети, являющейся конечным получателем пакетов.

В списках доступа IPX значение –1 исполняет роль обобщенной маски. Эта маска относится ко всем сетям IPX и может быть применена в предписаниях «разрешить» и «отклонить» при указании на все сети, не упомянутые в других директивах.

На рис. 14.7 изображена простая сеть IPX. Допустим, требуется список доступа, который будет отбрасывать все пакеты, отправляемые из сети 763B20F3 в сеть 02B2F4 через интерфейс Ethernet 0 маршрутизатора C. Как и при формировании любого списка доступа, тут необходимо выполнить два действия: составить список доступа и прикрепить его к соответствующему интерфейсу маршрутизатора[1].

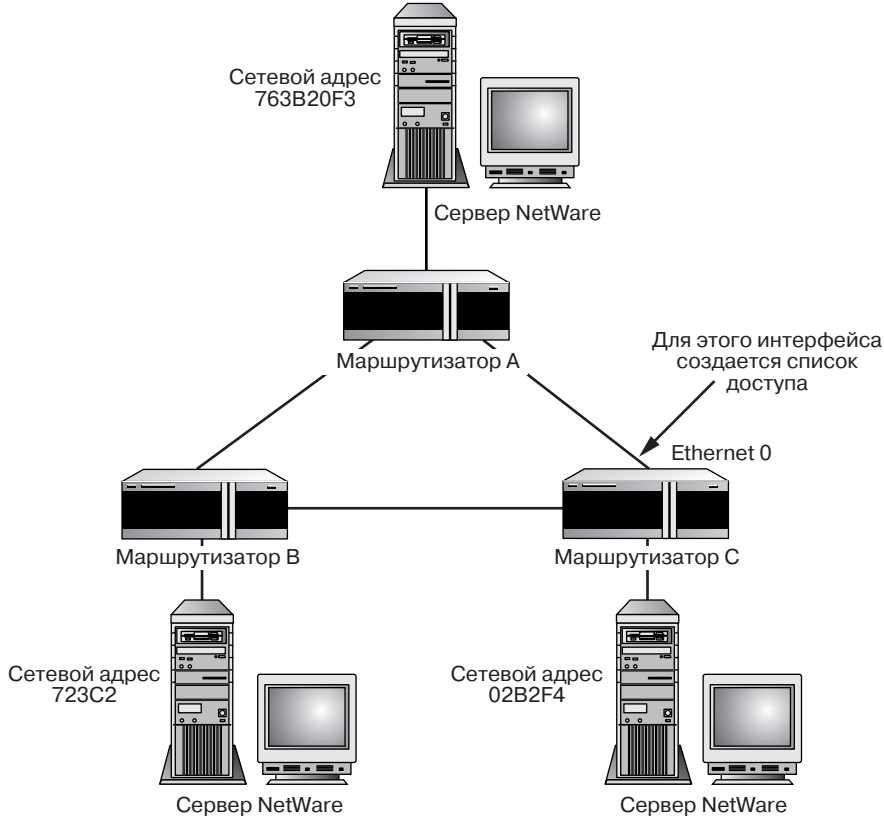


Рис. 14.7. Сеть NetWare, объединенная тремя маршрутизаторами

Список доступа IPX создается и приписывается интерфейсу маршрутизатора следующим образом:

1. В приглашении привилегированного режима введите команду `config t`, нажмите клавишу **Enter** и войдите в режим глобальной конфигурации.

[1] Адрес сети IPX состоит из 32 бит. В шестнадцатеричном виде он записывается восемью символами, по два символа на байт. Указанный в примере адрес сети IPX 02B2F4 (шесть символов) свидетельствует, что значение недостающего байта слева равно нулю. – *Прим. научн. ред.*

2. Чтобы сформировать список доступа, наберите команду `access-list 800` (любой номер списка IPX от 800 до 899), затем адрес сети, где находятся узлы-отправители пакетов, и адрес сети-получателя. Для рассматриваемого примера сети (см. рис. 14.6) напечатайте `access-list 800 deny 763B20F3 02B2F4` (адреса сетей отправителя и получателя). Потом нажмите **Enter**.
3. Составьте дополнительные предписания. Добавьте предписание `permit all` для всех остальных сетей IPX. Наберите `access-list 800 permit -1 -1` (разрешить доступ пакетам данных из всех сетей). Нажмите **Enter**.
4. Прикрепите список доступа к интерфейсу Ethernet 0 маршрутизатора, поместив команду `interface Ethernet 0` в приглашении режима глобальной конфигурации, далее нажмите клавишу **Enter**.
5. В строке config-if введите команду `ipx access-group 800 in` (так как список доступа будет фильтровать входящие пакеты данных). Нажмите **Enter**. Полученный список доступа представлен на рис. 14.8.

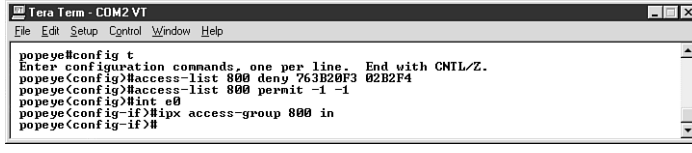


Рис. 14.8. Список доступа IPX, прикрепленный к интерфейсу Ethernet 0 маршрутизатора

6. Нажав клавиши **Ctrl**+**Z**, завершите сеанс конфигурации.
7. Воспользуйтесь клавишей **Enter**, чтобы вернуться в привилегированный режим.

Вы можете просмотреть список доступа при помощи команды `show`. Наберите команду `show access-list 800`, указав номер своего списка доступа, и нажмите **Enter**.

Операционная система Cisco IOS также позволяет создавать расширенные списки доступа IPX (аналогично расширенным спискам доступа IP), обеспечивающие дополнительную фильтрацию трафика в сети. Расширенные списки дают возможность сортировать пакеты по начальным и конечным адресам сетей/узлов, а также по данным таких протоколов стека IPX/SPX, как SAP и SPX. Информация о командах для работы с расширенными списками доступа имеется на компакт-диске Cisco IOS, который поставляется в комплекте с маршрутизатором.

➢ Сведения об адресации IPX приведены в главе 12 (раздел «Система IPX-адресации»).

Создание стандартных списков доступа AppleTalk

Разрешается создавать списки доступа для маршрутизаторов, которые работают с трафиком AppleTalk, система Cisco IOS резервирует для них номера от 600 до 699.

Данные списки способны фильтровать пакеты в зависимости от диапазона кабеля (диапазона адресов сетей в физическом сегменте объединенной сети AppleTalk). Например, предписание «разрешить» выглядит так: `access-list 600 permit cable-range 100-110`.

Списки доступа AppleTalk могут быть основаны на информации о зонах AppleTalk в предписаниях «разрешить» и «отклонить». Эти сведения позволяют легко идентифицировать части сети AppleTalk в предписаниях, поскольку зоны часто включают в себя несколько диапазонов кабеля. Предположим, что нужно запретить трафик из определенной зоны AppleTalk на интерфейсе маршрутизатора (на рис. 14.9 представлена часть сети AppleTalk).

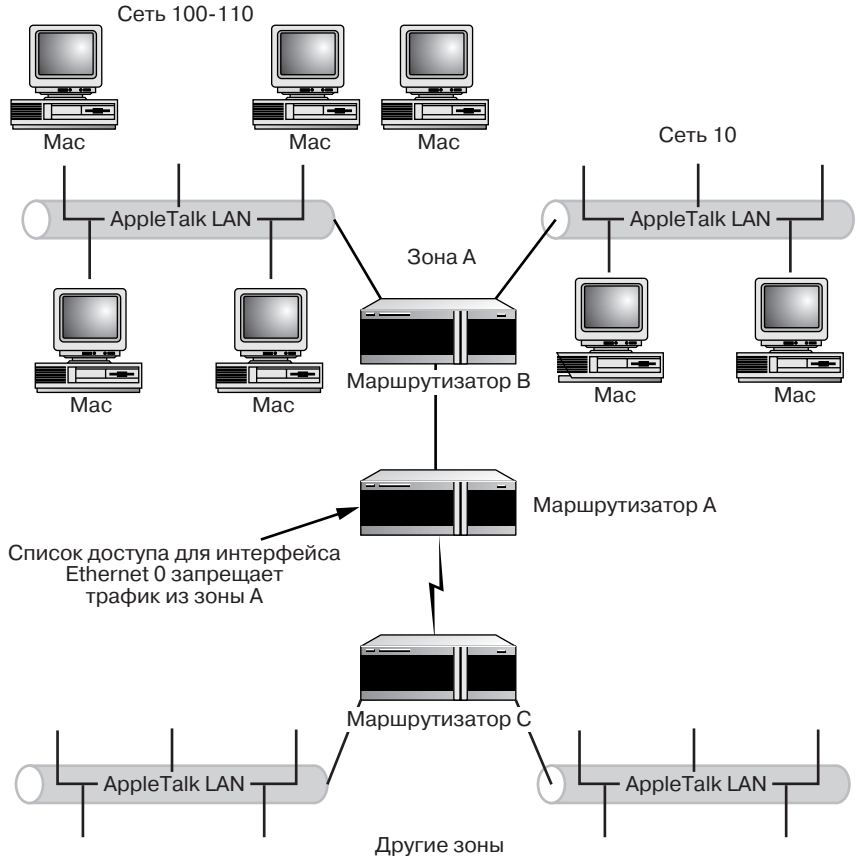


Рис. 14.9. Создание списков доступа для фильтрации трафика из заданных диапазонов кабеля и зон AppleTalk

Вам потребуется список доступа AppleTalk, который запретит доступ пакетов из зоны A (включающей сеть 100–110 и сеть 10) на интерфейс Ethernet 0 маршрутизатора A. Кроме того, необходимо указать, что пакеты данных из всех других зон сети должны беспрепятственно поступать на данный интерфейс.

> ***Сети AppleTalk используют имена объектов для обозначения серверов и других сетевых ресурсов. Допустимо составить предписания в списках доступа с помощью ключевого слова `object`, за которым следует название объекта, например `PrintServer`. Дополнительную информацию о стеке AppleTalk и системе Cisco IOS можно найти на Web-сайте www.cisco.com.***

Список доступа AppleTalk формируется и приписывается интерфейсу следующим образом:

1. В приглашении привилегированного режима поместите команду `config t`, после чего нажмите клавишу **Enter**. Вы окажетесь в режиме глобальной конфигурации.
2. Чтобы создать список доступа AppleTalk, введите команду `access-list 600` (любой номер списка AppleTalk от 600 до 699), затем информацию о зоне для тех пакетов, которые следует фильтровать. Для рассматриваемого примера сети (см. рис. 14.8) наберите `access-list 600 deny zone ZoneA` (командное слово `zone` (зона) показывает, что в качестве критерия указано имя зоны, в данном случае ZoneA). Далее нажмите клавишу **Enter**.
3. Составьте дополнительные предписания. Добавьте предписание `permit all` для всех остальных зон в сети. Напечатайте `access-list 600 permit additional-zones` (разрешить доступ пакетам из всех зон в сети). Нажмите **Enter**.
4. Прикрепите список доступа к интерфейсу Ethernet 0 маршрутизатора, поместив команду `interface Ethernet 0` в строке режима глобальной конфигурации, и нажмите **Enter**.
5. В строке config-if наберите `appletalk access-group 600`. Нажмите **Enter**. Готовый список доступа показан на рис. 14.10.

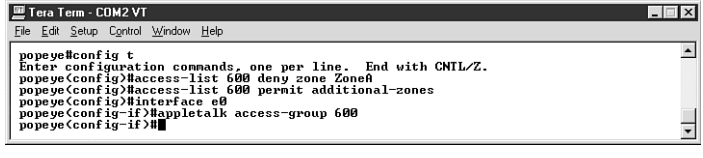


Рис. 14.10. Список доступа AppleTalk, прикрепленный к интерфейсу Ethernet 0 маршрутизатора

6. Воспользуйтесь клавишами **Ctrl**+**Z**, чтобы завершить сеанс конфигурации.
7. Нажмите **Enter** и вернитесь в привилегированный режим.

Просмотреть список доступа удобно с помощью команды `show access-list 600`, указав номер вашего списка. Работа со списками доступа AppleTalk несколько сложнее, чем со списками IP и IPX, так как для обозначения сетей и их частей используются зоны и диапазоны кабеля. Вам, скорее всего, придется иметь дело с небольшим количеством компьютеров Macintosh в сети, поэтому фильтровать трафик Macintosh потребуется в минимальной степени.

➢ AppleTalk-адресация рассматривается в главе 13, раздел «Адресация в стеке протоколов AppleTalk».

ГЛАВА 15

Конфигурирование протоколов WAN

Интерфейсы WAN

В предыдущих главах рассказывалось о соединении сетей LAN (таких, как сети Ethernet LAN с использованием сетевых протоколов IP, IPX и AppleTalk) и маршрутизаторов Cisco. Однако маршрутизаторы Cisco позволяют объединять сети при помощи протоколов WAN, а их последовательные интерфейсы обеспечивают функционирование различных технологий WAN, описанных в главе 3. Маршрутизаторы, которые подсоединяются к другим маршрутизаторам посредством технологии ISDN, оснащаются интерфейсом ISDN.

Ниже рассматриваются команды системы Cisco IOS, позволяющие конфигурировать различные WAN-протоколы маршрутизаторов. В последнее время применение соединений WAN стало дешевле, чем раньше. До сих пор компании могли использовать лишь недорогое соединение по линии 56K, теперь в ту же сумму обходится работа с протоколом Frame-Relay по линии T1.

> *Представитель одной из телефонных компаний сообщил, что стоимость линии T1, функционирующей на основе протокола Frame-Relay, на сегодняшний день составляет около трехсот долларов США в месяц – намного дешевле, чем два-три года назад. Если вы до сих пор работаете с линией 56K, узнайте, сколько стоит линия T1 с протоколом Frame-Relay: такая связь становится общедоступной.*

Ваш выбор, конечно, будет определяться стоимостью и скоростью линии. Прежде чем остановиться на соединении WAN, сопоставьте все «за» и «против».

Как правило, маршрутизаторы работают в качестве *оконечного оборудования данных* (Digital Terminal Equipment – DTE). Поэтому к последовательному порту маршрутизатора посредством кабеля DTE подключается устройство CSU/DSU – *аппаратура передачи данных*, или *оборудование провайдера* (Digital Communication

Equipment – DCE), которое, в свою очередь, подсоединяется к телефонной линии. Это устройство предоставляет тактовую частоту для синхронной передачи данных.

Можно быстро определить тип кадра, или инкапсуляцию (установка для протоколов WAN), на последовательном интерфейсе при помощи команды `show interface serial [interface number]`, где `[interface number]` – это номер последовательного порта. Чтобы, к примеру, проверить интерфейс Serial 0, сконфигурированный для протокола PPP, следует воспользоваться командой `show interface serial 0` (ее можно сокращать) – рис. 15.1.

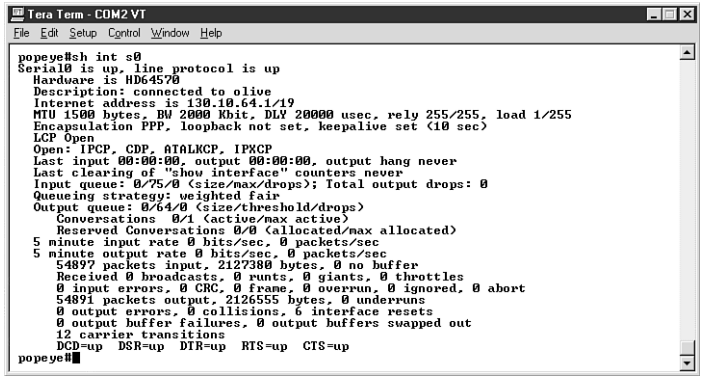


Рис. 15.1. Проверка типа кадра WAN на последовательных интерфейсах маршрутизатора

➢ Информация о протоколах X.25 и Frame-Relay приведена в главе 3, разделы «X.25» и «Frame-Relay». О других протоколах WAN, в частности HDLC и PPP, говорится в той же главе, раздел «Другие протоколы глобальных сетей». Последовательные интерфейсы рассматриваются в главе 6, раздел «Интерфейсы последовательного соединения».

Маршрутизатор способен работать в качестве устройства DCE. Так, данная книга писалась при помощи двух маршрутизаторов 2505, причем один из них был сконфигурирован как устройство DTE (кабель V.35 DTE), а другой – как устройство DCE (кабель V.35 DCE). Два этих кабеля связывались между собой, что создавало эффект WAN-соединения. Маршрутизатор DCE нужно было сконфигурировать таким образом, чтобы он предоставлял тактовую частоту, которую обеспечивает устройство CSU/DSU. Для установки тактовой частоты маршрутизатора была использована команда `clock rate` (в строке config-if конфигурируемого последовательного интерфейса). Тактовая частота составляет от 1200 до 8000000 бит/с в зависимости от связи. При помощи команды `show controller serial [interface number]` вы можете определить тип кабеля (DTE или DCE), который подсоединен к маршрутизатору.

Конфигурирование протокола HDLC

Протокол HDLC устанавливается как WAN-протокол по умолчанию для маршрутизаторов Cisco. Если данный протокол не задействован, вы можете включить его поддержку на маршрутизаторе с помощью несложной команды. Конфигурируя протокол HDLC, нужно указать такой параметр, как *пропускная способность* выделенной телефонной линии (например, линия 56К будет иметь пропускную способность 56 Кбит/с). При использовании IGRP в качестве протокола маршрутизации необходимо задавать пропускную способность, поскольку для протокола IGRP данный параметр – одна из метрик.

Если HDLC не задан в качестве WAN-протокола для маршрутизатора, вы можете назначить его для последовательного интерфейса. В таком случае конфигурирование производится следующим образом:

1. В строке привилегированного режима введите команду `config t`, затем нажмите клавишу **Enter**. Вы войдете в режим общей конфигурации.
2. Чтобы сконфигурировать интерфейс WAN, наберите в строке его имя, например `interface serial 0`. Снова нажмите **Enter**. Появится строка режима config-if.
3. Напечатайте `encapsulation HDLC`, затем нажмите **Enter**.
4. Если требуется задать пропускную способность для интерфейса, введите команду `bandwidth [kilobits/second]`, где `[kilobits/second]` – скорость линии. Например, для линии 56К укажите `bandwidth 56`, затем нажмите клавишу **Enter** (рис. 15.2).

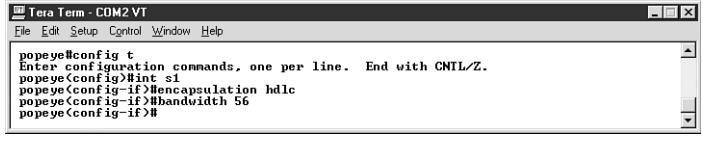


Рис. 15.2. Установка протокола HDLC в качестве WAN-протокола и настройка пропускной способности интерфейса

5. Воспользуйтесь клавишами **Ctrl**+**Z** для завершения конфигурирования.
6. Чтобы вернуться в строку привилегированного режима, нажмите **Enter**.

В маршрутизаторах, использующих модульные интерфейсы, имена портов определяются несколько иначе. Например, в случае маршрутизатора Cisco серии 7200 обращение к последовательному порту будет производиться командой `interfase serial slot/port`. Параметр `slot` соответствует номеру модуля, а `port` – номеру разъема на этом модуле.

Конфигурирование протокола PPP

Протокол связи «точка-точка» (Point-to-Point Protocol – PPP) – это протокол стека TCP/IP, который может использоваться для обеспечения соединения между маршрутизаторами по выделенным линиям (во многом аналогично протоколу HDLC). PPP – это протокол открытой системы, работающий с маршрутизацией IP, IPX и AppleTalk. Он легко конфигурируется с помощью команды `encapsulation`. Разрешается также задать пропускную способность соединения, как и в случае протокола HDLC. Конфигурирование протокола PPP для последовательного интерфейса производится следующим образом:

1. В строке привилегированного режима введите команду `config t`, затем нажмите клавишу **Enter**. Вы окажетесь в режиме общей конфигурации.
2. Чтобы сконфигурировать интерфейс WAN, наберите в строке его имя, например `interface serial 0`, и снова нажмите **Enter**. Появится строка режима config-if.
3. Напечатайте `encapsulation PPP`, затем нажмите **Enter**.
4. Если нужно задать пропускную способность для интерфейса, введите команду `bandwidth [kilobits/second]`, где `[kilobits/second]` – скорость линии. Например, для линии 56K укажите `bandwidth 56`, затем нажмите **Enter** (рис. 15.3).

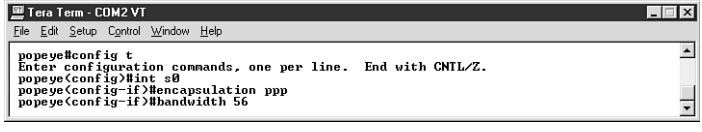


Рис. 15.3. Установка протокола PPP для последовательного интерфейса

5. Воспользуйтесь клавишами **Ctrl+Z** для завершения конфигурирования интерфейса.
6. Чтобы вернуться в строку привилегированного режима, нажмите **Enter**.

Вы можете применять команду `ping` для проверки правильности связи по линии WAN. Возьмем в качестве примера два маршрутизатора, взаимодействующих посредством WAN-соединения через интерфейсы Serial 0. Тип кадра WAN – PPP. Если известен IP-адрес последовательного интерфейса на другом конце WAN-соединения, допустимо проверить линию при помощи команды `ping [ip address]`. На

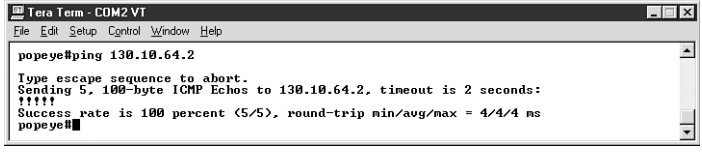


Рис. 15.4. Проверка работы WAN-соединения для последовательного интерфейса посредством команды ***ping***

рис. 15.4 показан результат исполнения данной команды. Конечный адрес – последовательный интерфейс маршрутизатора с IP-адресом 130.10.64.2 (такой возможности не будет, если последовательные порты сконфигурированы без IP-адресов).

Конфигурирование протокола X.25

Протокол X.25, созданный еще в 70-е годы, сейчас кажется очень старым (по сравнению, например, с Frame-Relay и другими более новыми и эффективными протоколами обработки пакетов данных), но по-прежнему используется для WAN-соединений между устройствами DTE (маршрутизаторами) и DCE (устройствами CSU/DSU).

Протокол X.25 применяет стандартную схему телефонной адресации X.121 (ее также называют *международной системой цифровых телефонных номеров*). Номер в данной системе включает от 1 до 14 цифр в десятичном коде и идентифицирует локальный X.121-адрес последовательного интерфейса, поэтому он должен быть сконфигурирован на маршрутизаторе, поддерживающем протокол X.25.

В зависимости от типа коммутатора X.25 потребуется указать размер пакетов, приходящих на маршрутизатор и уходящих с него через X.25-соединение (по умолчанию он равен 128 байтам). Кроме того, для различных коммутаторов, играющих роль входа в облако X.25, придется задать размер окна входящих и исходящих пакетов (по умолчанию он равен двум пакетам). Internet-провайдер предоставит вам необходимую информацию.

Конфигурирование протокола X.25 для последовательного интерфейса производится следующим образом:

1. В строке привилегированного режима наберите команду `config t`, затем нажмите клавишу **Enter**. Вы войдете в режим общей конфигурации.
2. Чтобы сконфигурировать интерфейс WAN, введите в строке его имя, например `interface serial 0`, и нажмите **Enter**. Появится строка режима config-if.
3. Напечатайте `encapsulation x25`, затем нажмите **Enter**.
4. Чтобы задать X.121-адрес интерфейса маршрутизатора, воспользуйтесь командой `x25 address [data link address]`, где `[data link address]` (адрес передачи данных) – это номер адреса в десятичном коде, предоставляемый вашим Internet-провайдером. Например, можно применить команду `x25 address 347650001` (где `347650001` – это X.121-адрес в десятичном представлении), а затем нажать клавишу **Enter**.
5. Для указания размера входящих пакетов напечатайте `x25 ips [bits]`, где `[bits]` (биты) – допустимый размер входящего пакета. Если вы задаете размер равным 256 битам, команда примет вид `x25 ips 256`. Нажмите **Enter**.
6. Допустимо также задать размер исходящих пакетов; для этой цели служит команда `x25 ops [bits]`. При размере 256 бит команда будет выглядеть так: `x25 ops 256`. Нажмите клавишу **Enter**.
7. Размер окна (на основании количества пакетов, поток которых нужно регулировать) для входящих пакетов на маршрутизаторе определяется посредством команды `x25 win [number of packets]`, где `[number of packets]` – количество пакетов. Если вы хотите установить этот размер равным пяти (для пяти пакетов данных), введите `x25 win 5` и нажмите **Enter**.

8. Чтобы задать размер окна для исходящих пакетов, воспользуйтесь командой `x25 wout [number of packets]`, например `x25 wout 5` (для пяти пакетов). Нажмите клавишу **Enter**. На рис. 15.5 показаны команды, описанные в пунктах 1–8, в том порядке, в котором они появляются на консоли маршрутизатора.

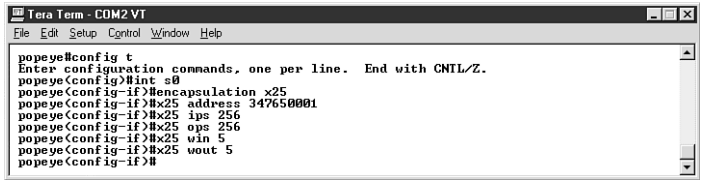


Рис. 15.5. Если вы задаете на последовательном интерфейсе инкапсуляцию X.25, вам придется указать размер окон, а также входящих и исходящих пакетов данных

9. Воспользуйтесь клавишами **Ctrl+Z** для того, чтобы завершить конфигурирование интерфейса.
10. Вернуться в строку привилегированного режима можно с помощью клавиши **Enter**.

Просмотреть установки протокола X.25 для последовательного интерфейса допустимо посредством команды `show interface [serial #]`, где `[serial #]` – это номер последовательного интерфейса, сконфигурированного для протокола X.25.

➢ Сведения о протоколе X.25 можно найти в главе 3, раздел «X.25».

Конфигурирование протокола Frame-Relay

Протокол Frame-Relay – это протокол канального уровня, который используется для обеспечения связи между устройствами DTE и DCE. Устройства DCE в сетях Frame-Relay (частных или открытых коммутируемых телефонных сетях) состоят из коммутаторов (рис. 15.6), а сама сеть обычно представлена в виде *облака*.

Протокол Frame-Relay работает с постоянными виртуальными линиями для сеансов связи между различными частями WAN. Такие виртуальные линии определяются при помощи *идентификационного номера передачи данных* (Data Link Connection Identifier – DLCI), предоставляемого провайдером услуг Frame-Relay. Данный номер обеспечивает связь между маршрутизатором и коммутатором (см. рис. 15.6), его необходимо указывать при конфигурировании протокола Frame-Relay.

Для протокола Frame-Relay также можно сконфигурировать другой параметр – *локальный интерфейс управления* (Local Management Interface – LMI). Интерфейс

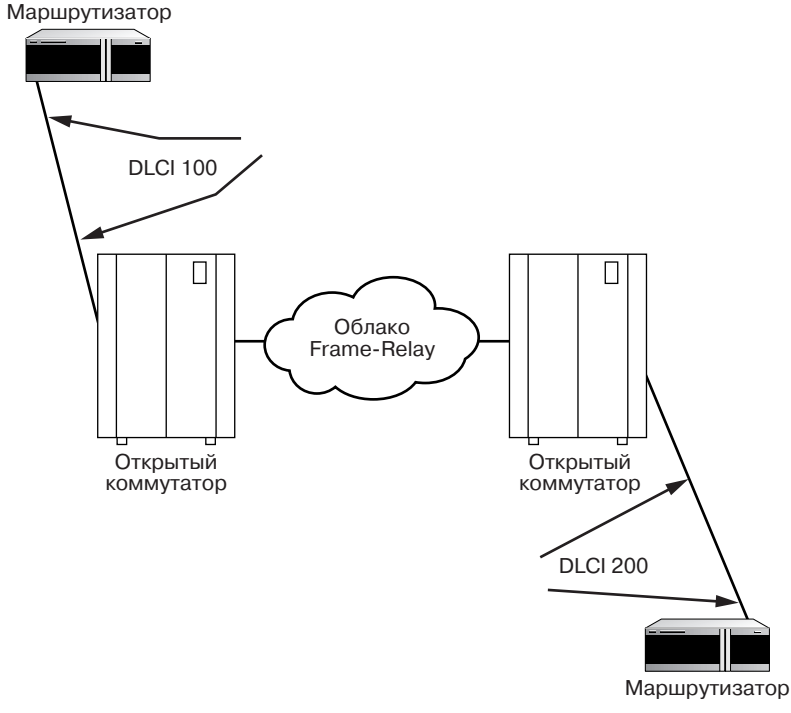


Рис. 15.6. Протокол Frame-Relay используется для связи между маршрутизаторами и открытыми коммутаторами

LMI – это стандарт сигналов, который используется для связи между маршрутизатором и коммутатором Frame-Relay. Маршрутизаторы Cisco поддерживают три типа интерфейсов LMI:

- cisco – типы Cisco, Northern Telecom, DEC и StrataCom LMI;
- ansi – тип American National Standards LMI;
- q933a – стандартный тип International Telecommunications LMI.

Конфигурирование протокола Frame-Relay осуществляется аналогично настройке других протоколов WAN. Для последовательного интерфейса это производится следующим образом:

1. В строке привилегированного режима наберите `config t`, затем нажмите клавишу **Enter**. Вы войдете в режим общей конфигурации.
2. Чтобы сконфигурировать интерфейс WAN, введите в строке его имя, например `interface serial 0`. Нажмите **Enter**. Строка изменится на config-if.
3. Напечатайте `encapsulation frame`, затем нажмите **Enter**.

4. Указать DLCI-номер для соединения между маршрутизатором и коммутатором Frame-Relay можно с помощью команды `frame-relay interface-dlci [#]`, где `[#]` – это DLCI-номер линии между маршрутизатором и коммутатором. Например, если DLCI-номер равен 100, команда примет вид `frame-relay interface-dlci 100`. Нажмите клавишу **Enter**.
5. Посредством команды `frame-relay interface-dlci 100` перейдите в строку `dlci` для конфигурации параметров по виртуальной линии DLCI. Чтобы вернуться в режим конфигурирования интерфейса, воспользуйтесь командой `int s0` и нажмите **Enter**.
6. Для конфигурирования интерфейса LMI (только в том случае, если версия IOS более старая, чем 11.2), наберите `frame-relay lmi-type []`, где `lmi type` (тип интерфейса LMI) – это тип cisco, ansi или q933a. Если вы укажете LMI ansi, команда будет выглядеть так: `frame-relay lmi-type ansi`. Затем нажмите клавишу **Enter** (рис. 15.7).

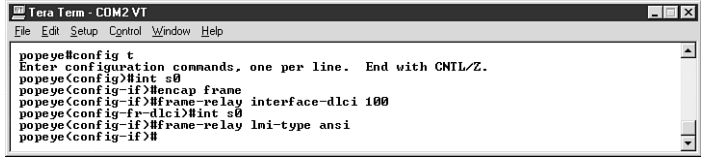


Рис. 15.7. Конфигурирование последовательного интерфейса для работы с протоколом Frame-Relay

7. Нажмите клавиши **Ctrl**+**Z** для завершения конфигурирования интерфейса.
8. Чтобы вернуться в строку привилегированного режима, воспользуйтесь клавишей **Enter**.

> ***Начиная работать с версией IOS 11.2, маршрутизатор попытается автоматически определить тип интерфейса LMI, который используется в линии между ним и коммутатором. Для этого он пошлет запрос коммутатору Frame-Relay, полученный ответ будет содержать информацию о типе или типах интерфейса LMI в линии. Затем маршрутизатор автоматически изменит свою конфигурацию с учетом последнего типа LMI, сведения о котором он получил от коммутатора (если коммутатор отправил несколько сообщений о типе интерфейса LMI).***

С помощью команд `show interface serial [interface number]`, `show frame-relay lmi` и `frame-relay map` можно просмотреть параметры конфигурации протокола Frame-Relay. Команда `show frame-relay lmi` выводит список ошибочных сообщений, полученных и отправленных маршрутизатором, а также список LMI-сообщений. На рис. 15.8 показан результат исполнения этой команды

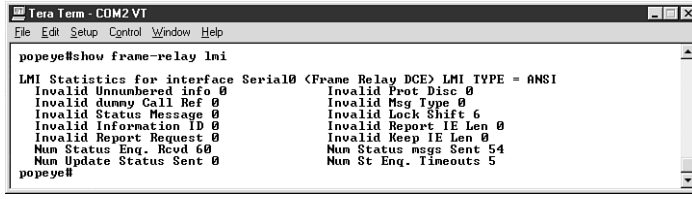


Рис. 15.8. Определение типа интерфейса LMI маршрутизатора

(вы можете запускать ее в строке пользовательского или привилегированного режима).

С помощью команды `show frame-relay map` можно просмотреть, какие DLCI-номера заданы сетевым протоколам, сконфигурированным для маршрутизатора. Например, на рис. 15.9 представлен DLCI-номер 100, присвоенный протоколам IP, IPX и AppleTalk.

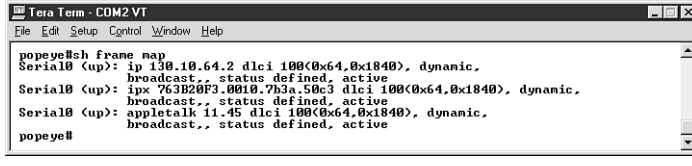


Рис. 15.9. Просмотр информации о DLCI-номерах протоколов

Один из интерфейсов маршрутизатора может быть сконфигурирован для различных DLCI-номеров (виртуальных линий) при помощи *интерфейсов низшего уровня*, или *подинтерфейсов*. Так, когда вы настроили интерфейс Serial 0, в строке конфигурации разрешается указать, что вы желаете настроить последовательный интерфейс Serial 0.1, где 1 – первый интерфейс низшего уровня, а затем присвоить ему DLCI-номер.

Конфигурирование протокола ISDN

Протокол ISDN (Integrated Services Digital Network) – это цифровая служба связи, которая работает в существующих телефонных линиях. Различают две его разновидности: *протокол ISDN базовой скорости* (Basic Rate ISDN – BRI) и *протокол ISDN высокой скорости* (Primary Rate ISDN – PRI).

При конфигурировании протокола ISDN необходимо убедиться, что у маршрутизатора имеется встроенный интерфейс ISDN. В противном случае вам придется купить *адаптер*, или *ISDN-модем*, и подключить его к одному из последовательных интерфейсов маршрутизатора.

Протокол ISDN несколько отличается от других протоколов WAN, которые мы рассмотрели в данной главе: он представляет собой физическое средство

перемещения данных от маршрутизатора в открытую телефонную сеть, а не тип кадра. Когда вы сконфигурируете на маршрутизаторе протокол ISDN, потребуется указать тип кадра, например PPP или Frame-Relay.

Рассмотрим порядок конфигурирования протокола ISDN BRI на маршрутизаторе. Протокол BRI состоит из двух каналов, причем каждый обеспечивает пропускную способность 64 Кбит/с (их можно объединить для поддержания пропускной способности 128 Кбит/с). Эти каналы должны быть определены при помощи *идентификационного номера службы* (Service Profile Identifier – SPID). SPID-номера присваиваются всем каналам коммутатора, которые соединяют маршрутизатор, поддерживающий протокол ISDN, и телефонную систему.

> ***Если вы предполагаете соединить два маршрутизатора напрямую (посредством V.35-кабелей DTE и DCE), вам необходимо настроить маршрутизатор как устройство DCE. При конфигурировании последовательного интерфейса введите команду `frame-relay interface-type dce` в строке config-if. Далее необходимо указать тактовую частоту маршрутизатора, который вы используете как устройство DCE. Команда `frame-relay switching` в строке общей конфигурации обеспечивает работу маршрутизатора в качестве коммутатора протокола Frame-Relay.***

> ***Разрешается сконфигурировать протокол ISDN для выделенного соединения или соединения по запросу, при котором маршрутизатор конфигурируется для дозвона и подключения с целью пересылки данных. Допустимо сконфигурировать маршрутизатор и для ответа на входящие звонки. Дополнительную информацию о протоколах BRI и PRI можно найти на Web-сайте www.cisco.com или на компакт-диске, который поставляется в комплекте с маршрутизатором Cisco.***

При конфигурировании протокола ISDN необходимо также указать *тип коммутатора* – идентификационный код производителя коммутатора ISDN, к которому вы подключаетесь. После того как вы введете SPID-номера и определите тип коммутатора, останется лишь задать тип кадра (например, PPP или HDLC).

Конфигурирование протокола BRI ISDN для интерфейса ISDN производится следующим образом:

1. В строке привилегированного режима напечатайте `config t`, затем нажмите клавишу **Enter**. Вы войдете в режим общей конфигурации.
2. Чтобы задать тип коммутатора для соединения ISDN, введите команду `isdn switch type basic-[]`, где вместо квадратных скобок следует ввести идентификационный код производителя для того типа коммутатора, к которому вы подключаетесь. Нажмите клавишу **Enter**.

3. Теперь можно приступать к конфигурированию интерфейса ISDN. Наберите команду `int bri [number]`, где параметр `[number]` – это номер интерфейса BRI маршрутизатора, например BRI 0 или BRI 1. Нажмите **Enter**.
4. В строке config-if введите тип кадра (например, `encap ppp`) и нажмите **Enter**.
5. Для указания SPID-номера двух каналов ISDN B, введите в строке config-if команду `isdn spid1 [SPID #]`, где `[SPID #]` – это телефонный номер для определенного канала, предоставляемый провайдером услуги (допустим, 6125551234). Для данного примера команда примет вид `isdn spid1 6125551234`. Нажмите клавишу **Enter**.
6. Чтобы задать SPID-номер второго канала, повторите команду `isdn spid2 [SPID #]` в строке config-if, набрав номер второго канала, и нажмите **Enter**.
7. После того как вы ввели всю информацию, воспользуйтесь клавишами **Ctrl**+**Z** для завершения сеанса конфигурирования.

Команда `show int bri [number]` позволяет просматривать конфигурацию. Для сохранения новой конфигурации в памяти NVRAM маршрутизатора применяется команда `copy running-config startup-config`.

➢ Сведения о протоколе ISDN представлены в главе 3 (раздел «Коммутация каналов»), а о памяти NVRAM – в главе 7 (раздел «Устройство маршрутизатора Cisco»).

ГЛАВА 16

Конфигурирование маршрутизатора при помощи Cisco ConfigMaker

Программа Cisco ConfigMaker

Cisco ConfigMaker – это базовая программа конфигурирования маршрутизатора. Вы можете бесплатно загрузить ее с Web-сайта компании Cisco, кроме того, она поставляется на компакт-диске вместе с новыми версиями операционной системы Cisco IOS. Cisco ConfigMaker используется для конфигурирования вашего маршрутизатора (или даже всех маршрутизаторов в сети) и загрузки созданных конфигураций на маршрутизаторы через сеть. Если сеть еще не настроена для работы, загрузить конфигурацию удобно с компьютера, на котором установлен Cisco ConfigMaker и который подключен к маршрутизатору через консоль.

Программа Cisco ConfigMaker проста в применении, но она не заменит команд системы Cisco IOS. Как правило, она используется для быстрой настройки маршрутизатора, но не его максимально эффективного конфигурирования, что возможно только из командной строки. Кроме того, Cisco ConfigMaker не поддерживает команд мониторинга маршрутизатора (в частности, команду `show`, хотя и допускает команду `ping`).

Для работы с этой программой на маршрутизаторе следует установить Cisco IOS 11.2 или более новую версию (в момент написания книги последней версией Cisco IOS являлась 12.0). Проверить, какая версия IOS установлена на маршрутизаторе, удобно с помощью команды `show version`, введенной с консоли маршрутизатора в строке пользовательского или привилегированного режима.

Если ваша версия Cisco IOS не поддерживает Cisco ConfigMaker, эту программу можно использовать для создания сетевой диаграммы, а также для упрощения конфигурирования протоколов LAN и их систем адресации на интерфейсах маршрутизатора.

Загрузка Cisco ConfigMaker

Если вы не получили программу Cisco ConfigMaker вместе с новой версией IOS или с маршрутизатором, вы можете загрузить ее с Web-сайта компании Cisco, заполнив регистрационную форму. Несложно загрузить Cisco ConfigMaker даже в том случае, если у вас нет маршрутизатора Cisco, однако данная программа не будет работать с маршрутизаторами других производителей.

Выполните нижеприведенную последовательность действий:

1. В Internet-браузере введите адрес http://www.cisco.com/warp/public/734/configmkr. Нажмите клавишу **Enter**.
2. На открывшейся странице выберите пункт **To Download Cisco ConfigMaker, Click Here** (Для загрузки Cisco ConfigMaker щелкните здесь). Откроется страница с регистрационной формой. Заполните форму и нажмите на пункт **Submit** (Согласен). Появится несколько ссылок на сайты FTP, содержащие файл инсталляции программы. Выберите сайт FTP и загрузите файл.
3. После завершения загрузки установите Cisco ConfigMaker на вашем компьютере.

Установка Cisco ConfigMaker

Программа Cisco ConfigMaker работает с такими операционными системами, как Microsoft Windows 95/98, Windows NT 4.0 и Windows 2000. Ниже приведены базовые системные требования:

- компьютер 486 (рекомендуется Pentium);
- 16 Мб RAM;
- 20 Мб на жестком диске;
- монитор SVGA 800×600, не менее 256 цветов;
- CD-ROM (для установки программы с компакт-диска).

Установить Cisco ConfigMaker можно с компакт-диска (если вы получили программу вместе с маршрутизатором или новой версией IOS) или после загрузки дистрибутивного файла из Internet.

Для инсталляции программы с компакт-диска вставьте диск в CD-ROM. Процесс установки начнется автоматически, останется только выполнять указания, появляющиеся на экране.

Если вы устанавливаете программу с помощью дистрибутивного файла, дважды щелкните мышью по значку файла, чтобы запустить процедуру инсталляции. Подсказки будут отображаться на экране.

Конфигурирование сети

Работая в Cisco ConfigMaker, вы создаете схему или диаграмму вашей сети, обозначая маршрутизаторы, сетевые коммутаторы, сети LAN, корпоративные сети

и другие устройства соответствующими пиктограммами. Как правило, для этого нужно взять определенное устройство (например, маршрутизатор Cisco) и ввести его в диаграмму общей сети, указав имя и пароли устройства (для входа на маршрутизатор и для работы в привилегированном режиме). Необходимо также определить сетевые протоколы – IP, IPX или AppleTalk, – которые будет поддерживать маршрутизатор.

При помощи особых подпрограмм-мастеров Cisco ConfigMaker способен выполнять множество задач. *Подпрограмма сетевой адресации* используется для адресации интерфейсов различных маршрутизаторов, а *подпрограмма доставки конфигурации* – для доставки созданной конфигурации маршрутизатору.

Запустите программу Cisco ConfigMaker, войдя в меню **Пуск** Windows (**Пуск ⇒ Программы ⇒ Cisco ConfigMaker**) или дважды щелкнув по иконке **ConfigMaker**, которая была помещена на Рабочий стол Windows после установки программы.

На экране появится окно Cisco ConfigMaker (рис. 16.1). Если вы запускаете программу впервые, то можете сначала войти в режим тренировки; но в данной

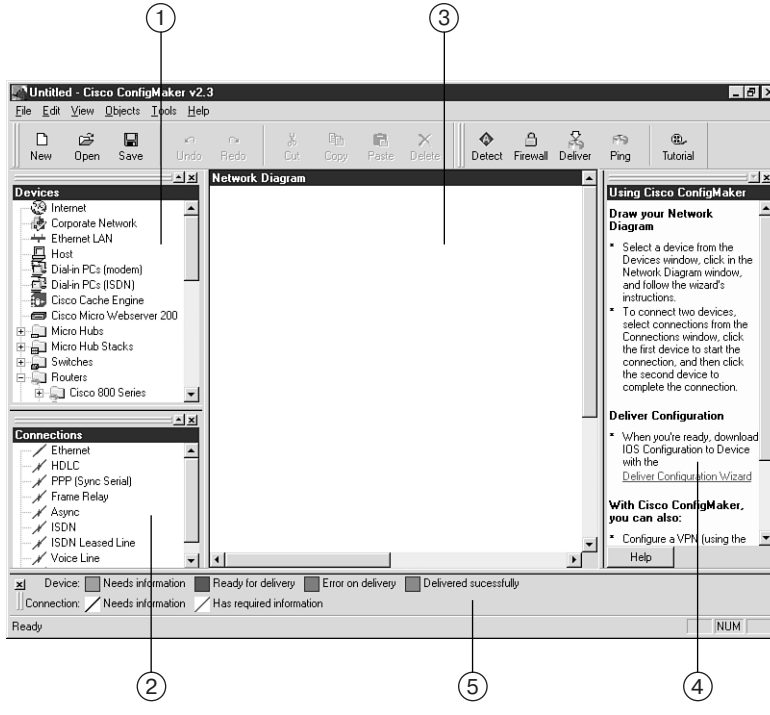


Рис. 16.1. Программа Cisco ConfigMaker упрощает создание сетевых диаграмм: 1 – окно устройств; 2 – окно соединений; 3 – окно сетевой диаграммы; 4 – окно задач; 5 – строка состояния

книге мы сразу приступим к работе. Щелкните по кнопке **No**, при этом диалоговое окно режима тренировки будет удалено с экрана.

Окно Cisco ConfigMaker разделено на несколько основных областей:

- *окно устройств* содержит пиктограммы для устройств Cisco, в частности маршрутизаторов, коммутаторов и концентраторов. Кроме того, здесь находятся иконки для других объектов, таких как сети LAN и корпоративные сети;
- *окно соединений* включает в себя пиктограммы для различных типов соединений, которые можно установить между устройствами в сетевой диаграмме. Здесь имеются LAN-соединения, например Ethernet, и WAN-соединения, скажем HDLC и PPP;
- *окно сетевой диаграммы* предназначено для создания сетевой диаграммы посредством пиктограмм из вышеназванных окон;
- *окно задач* охватывает список задач, которые необходимо выполнить для создания сетевой диаграммы и подключения к ней всех устройств. Чтобы увеличить свободное место в окне диаграммы, окно задач можно скрыть, убрав соответствующий флажок с помощью команд **View** ⇒ **Task List** (Вид⇒ Список задач). Чтобы отобразить скрытое окно, достаточно повторить указанные действия;
- *строка состояния* предоставляет информацию по устройствам при загрузке конфигурации с Cisco ConfigMaker.

Теперь можно приступать к созданию сети. Начать следует с добавления к конфигурации всех сетевых устройств, включая маршрутизаторы.

Добавление сетевых устройств

К сети легко добавить маршрутизаторы и другие объекты, например сети LAN. Мы расскажем, как настроить два объекта – маршрутизатор 2505 и сеть Ethernet LAN – в окне сетевой диаграммы. Начнем с маршрутизатора:

1. Чтобы добавить в окно маршрутизатор 2505, найдите в списке устройств соответствующую папку и щелкните по символу **+** (плюс) слева от нее. На экране появится список всех маршрутизаторов семейства 2505 (рис. 16.2).
2. Щелкните по иконке **2505**, а затем в окне сетевой диаграммы. Появится подпрограмма установки маршрутизатора Cisco 2505.
3. В строке **Device Name** (Название устройства) введите имя, которое вы хотите присвоить маршрутизатору (в данном случае будет использоваться имя Popeye). Затем щелкните по кнопке **Next** (Далее).
4. В следующем окне подпрограммы введите пароль для входа на маршрутизатор и пароль привилегированного режима (рис. 16.3), а затем снова щелкните по кнопке **Next**.

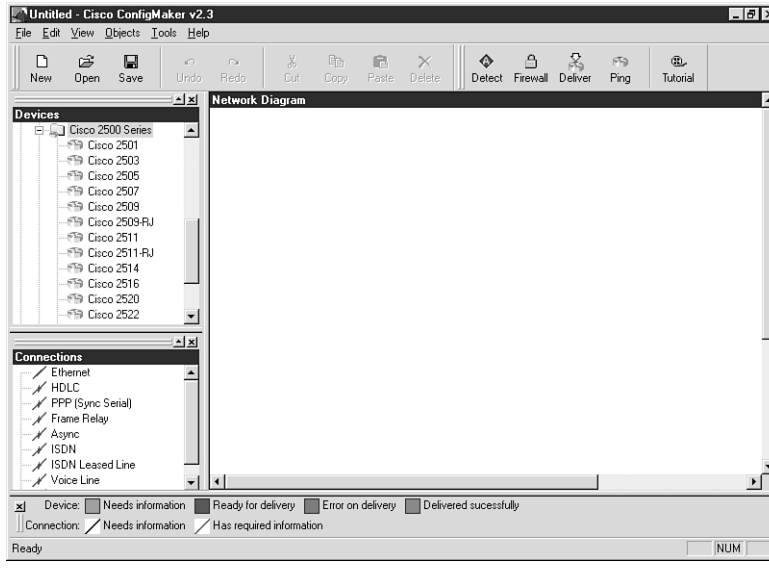


Рис. 16.2. Папки со списками маршрутизаторов соответствующих серий

Рис. 16.3. Поля ввода имени маршрутизатора и паролей

5. Далее появится запрос о том, какие сетевые протоколы следует задействовать для данного маршрутизатора. По умолчанию устанавливается IP, но вы можете добавить протоколы IPX и AppleTalk (рис. 16.4). Выберите нужные сетевые протоколы и щелкните по кнопке **Next**.
6. Подпрограмма выдаст сообщение о том, что маршрутизатор был добавлен к сетевой диаграмме. Щелкните по кнопке **Finish** (Готово) для завершения процедуры.

В окне сетевой диаграммы появится сконфигурированный маршрутизатор (его пиктограмму удобно перемещать при помощи мыши). Теперь добавим к диаграмме сеть LAN, которую можно подсоединить к маршрутизатору. Для этого нужно

Рис. 16.4. Определение необходимых протоколов

найти в окне устройств иконку **Ethernet LAN**, щелкнуть по кнопке **icon** (Пиктограмма), а затем щелкнуть в окне сетевой диаграммы – там, где вы хотите расположить иконку сети LAN.

Теперь в окне сетевой диаграммы имеются маршрутизатор и сеть LAN (рис. 16.5). Их необходимо подключить через соответствующее соединение.

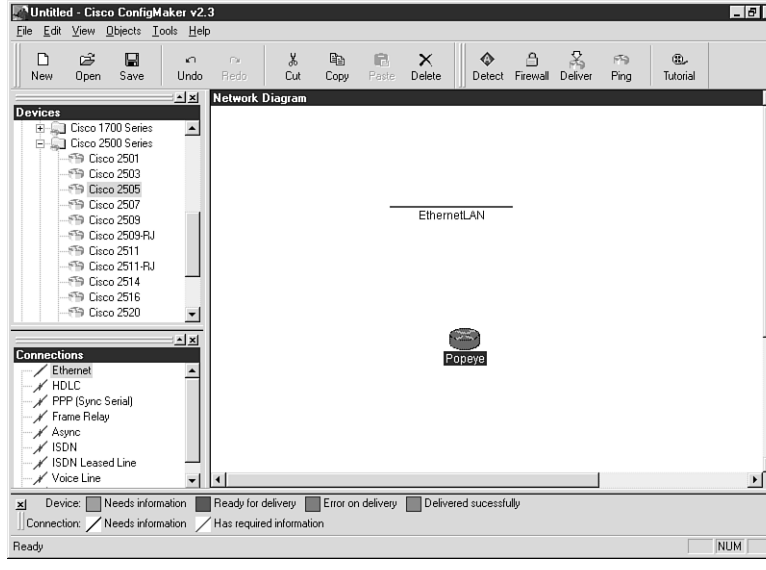


Рис. 16.5. Соединение сетей LAN и маршрутизаторов, добавленных в сетевую диаграмму

Если вы ошиблись при выборе иконки устройства или соединения, нажмите клавишу Esc и удалите иконку до того, как перенести ее в окно сетевой диаграммы. Если вы уже поместили устройство в окно диаграммы, выберите его и нажмите клавишу Delete (Удалить).

Соединение сети LAN и маршрутизатора

Чтобы установить взаимодействие сети LAN и маршрутизатора, необходимо выбрать соответствующий тип подключения в окне соединений и затем поместить его между маршрутизатором и сетью LAN. Также нужно ввести информацию о системе адресации: IP-адрес интерфейса маршрутизатора и маску подсети. Если в качестве поддерживаемых протоколов вы указали IPX и AppleTalk, следует описать систему адресации для каждого протокола.

Маршрутизатор и сеть LAN можно связать следующим образом:

1. Между сетью и маршрутизатором нужно установить соединение Ethernet (поскольку добавлена сеть Ethernet LAN). Щелкните по иконке **Ethernet Connection** (Соединение Ethernet) в окне соединений.
2. Щелкните по пиктограмме маршрутизатора, а затем – по значку сети Ethernet LAN, чтобы задать между ними соединение Ethernet.
3. Когда вы щелкнете по второй иконке (**Ethernet LAN**), появится окно подпрограммы установки соединения Ethernet, которая помогает связать сеть Ethernet LAN и интерфейс Ethernet маршрутизатора. Затем щелкните по кнопке **Next**.
4. На экране появится запрос о вводе IP-адреса и маски подсети для интерфейса Ethernet маршрутизатора с именем Popeye (если указан протокол IPX, нужно задать сетевой IPX-адрес, если AppleTalk – диапазон кабеля и имя зоны). Введите IP-адрес интерфейса маршрутизатора (рис. 16.6).

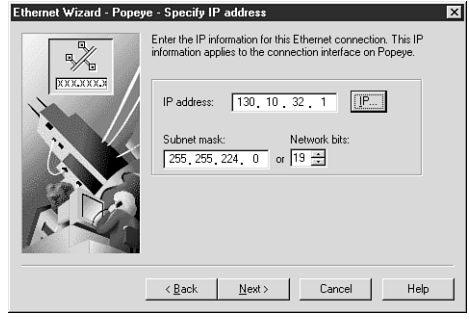


Рис. 16.6. Ввод IP-адреса и маски подсети для интерфейса маршрутизатора

5. В строке **Subnet Mask** (Маска подсети) впишите маску подсети интерфейса, а также количество битов сетевого адреса и количество битов, которые использовались для создания подсетей (см. главу 10).
6. Щелкните по кнопке **Next**.
7. В последнем окне подпрограммы появится сообщение о том, что соединение установлено. Щелкните по кнопке **Finish** для завершения работы с подпрограммой.

Теперь маршрутизатор может взаимодействовать с сетью LAN. Просмотреть тип адресации соединения (интерфейса маршрутизатора) удобно с помощью команд **View ⇒ Attributes ⇒ IP Address**, **IPX Address** или **AppleTalk Address** (Вид⇒ Параметры ⇒ IP-адрес, IPX-адрес, AppleTalk-адрес) – в зависимости от используемого типа сетевой адресации. Для маршрутизатора допустимо задействовать несколько систем адресации, поэтому в подменю **Attributes** (Параметры) разрешается указать несколько пунктов.

Подменю **Attributes** служит и для того, чтобы пометить интерфейсы маршрутизатора, которые присутствуют в сетевой диаграмме. Воспользуйтесь командами **View ⇒ Attributes ⇒ Port Number** (Вид ⇒ Параметры ⇒ Номер порта). На рис. 16.7 представлено соединение между маршрутизатором и сетью Ethernet LAN, сопровождаемое номером интерфейса и информацией по IP-адресации.

Если вы щелкнете по кнопке IP в окне подпрограммы установки соединения Ethernet, где вводится IP-адрес и маска подсети для интерфейса маршрутизатора, будет выдана информация о диапазоне свободных адресов в заданной подсети. Кроме того, вы узнаете сетевой адрес той подсети, из которой взят текущий IP-адрес. При расчете диапазона IP-адресов в подсети (см. главу 10) для проверки вычислений можно воспользоваться IP-калькулятором.

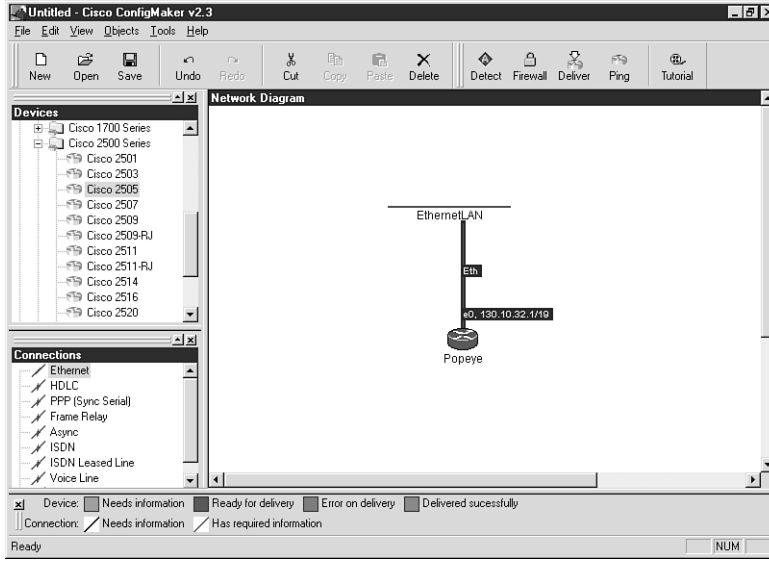


Рис. 16.7. Меню View предназначено для просмотра системы адресации, а также для указания адресов в сетевой диаграмме

В следующем разделе речь пойдет о том, как использовать Cisco ConfigMaker для создания соединения между маршрутизаторами.

Соединение двух маршрутизаторов

Как было сказано выше, маршрутизаторы могут взаимодействовать посредством кабеля LAN (через соединение Ethernet в Cisco ConfigMaker) или посредством удаленного доступа через последовательное подключение с помощью протокола WAN (PPP или Frame-Relay). При помощи Cisco ConfigMaker удобно создать последовательное соединение между маршрутизаторами на диаграмме. Сначала к диаграмме нужно добавить другой маршрутизатор (его тип не имеет значения, допустимо задать даже такой, который не используется в вашей компании). Поместите в диаграмму второй маршрутизатор серии 2505 (рис. 16.8) и подключите его к первому посредством протокола WAN:

1. Оба маршрутизатора должны присутствовать в окне сетевой диаграммы. Щелкните по пиктограмме подключения WAN (например, **PPP**) в окне соединений.
2. Щелкните по значку первого, а затем второго маршрутизатора, чтобы указать, где вы желаете создать подключение.
3. Откроется подпрограмма установки для того протокола WAN, который вы указали (PPP или HDLC). В примере выбран протокол PPP.
4. Щелкните по кнопке **Next**, чтобы приступить к созданию соединения.

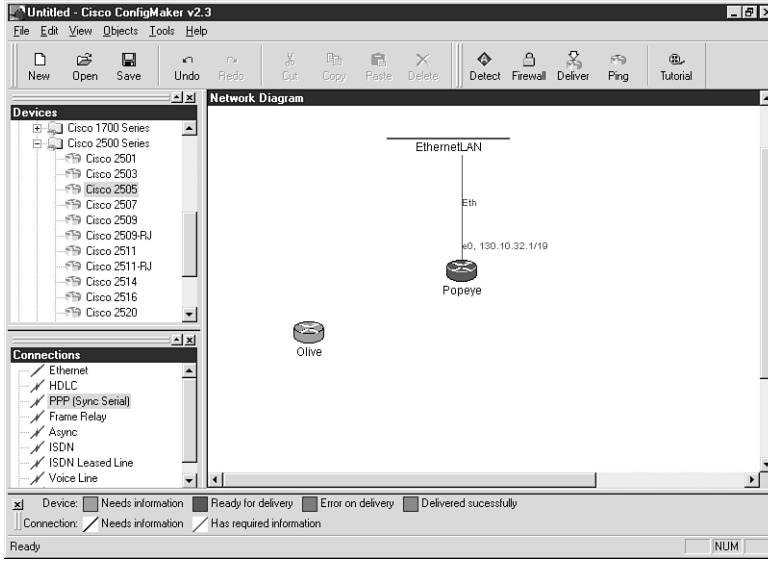


Рис. 16.8. Два маршрутизатора в диаграмме можно связать при помощи протокола WAN

5. Далее следует задать последовательный интерфейс (например, Serial 0), который нужно сконфигурировать для работы с протоколом WAN (рис. 16.9). Щелкните по кнопке **Next**.

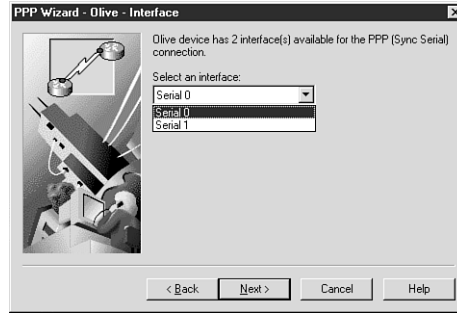


Рис. 16.9. Выбор последовательного порта, который требуется сконфигурировать для установления соединения WAN с другим маршрутизатором

6. Теперь необходимо ввести сведения о системе адресации для выбранного последовательного порта (рис. 16.10). Укажите IP-адрес и маску подсети для последовательного интерфейса второго маршрутизатора (поскольку маршрутизатор поддерживает только протокол IP), затем щелкните по кнопке **Next**.

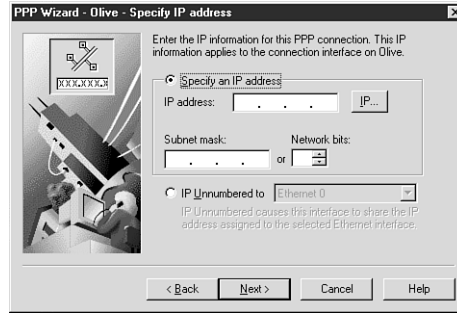


Рис. 16.10. Задание системы адресации для выбранного последовательного интерфейса

7. Определите последовательный интерфейс второго маршрутизатора и щелкните по кнопке **Next**.
8. Введите данные о системе адресации (IP-адрес и маску подсети) – см. пункт 6. Щелкните по кнопке **Next**.
9. На вопрос, нужно ли создавать резервное соединение, ответьте **No Backup** (Не создавать резервного соединения). Эта опция устанавливается по умолчанию. Щелкните по кнопке **Next**.

10. Появится сообщение, что соединение WAN успешно установлено. Щелкните по кнопке **Finish**.

Соединение появится в окне сетевой диаграммы (рис. 16.11). Если включен атрибут **View Addressing** (Просмотр адресации), будут выведены сведения о системе адресации последовательных интерфейсов двух маршрутизаторов.

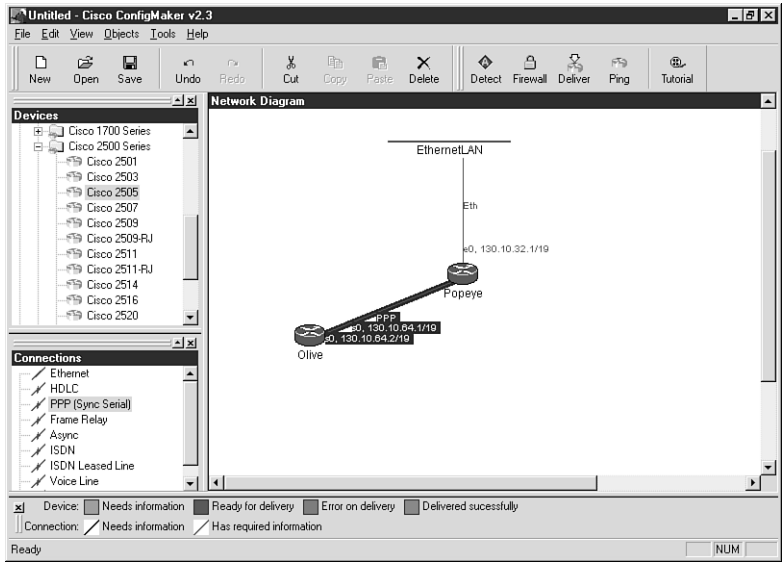


Рис. 16.11. Новое соединение WAN появится в окне сетевой диаграммы

Доставка конфигурации маршрутизатору

Программу Cisco ConfigMaker удобно использовать для создания диаграммы всей сети, связывая сети LAN, хосты или маршрутизаторы с маршрутизаторами. В окнах устройств и соединений доступны все возможные аппаратные устройства и типы подключений. Полученную конфигурацию допустимо применять для работы маршрутизаторов.

Загружать конфигурацию на маршрутизатор можно при помощи подключенного к той же сети компьютера, на котором установлена Cisco ConfigMaker. Однако перед отправкой конфигурации по сети вы должны задать компьютеру и маршрутизаторам IP-адреса, для чего следует повторно настраивать маршрутизаторы с консоли.

На маршрутизатор, который еще не настроен, конфигурацию легко загрузить с подсоединенного к сети компьютера, где установлена Cisco ConfigMaker.

Подключение компьютера к маршрутизатору производится аналогично подключению консоли компьютера.

Перед тем как отправлять конфигурацию, нужно убедиться, что программа будет сообщать верную информацию о том последовательном порте компьютера, который используется как порт конфигурации. По умолчанию устанавливается порт COM1.

Если требуется изменить установки COM-порта, выберите **View** ⇒ **Options** (Вид ⇒ Параметры). В появившемся диалоговом окне укажите нужный COM-порт, затем щелкните по кнопке **OK**.

Доставка конфигурации через порт консоли выполняется следующим образом:

1. Откройте в Cisco ConfigMaker сетевую диаграмму, содержащую ту конфигурацию, которую необходимо доставить маршрутизатору. Укажите соответствующую иконку маршрутизатора (рис. 16.12). В данном примере выбрана конфигурация для маршрутизатора 2 (Popeye).

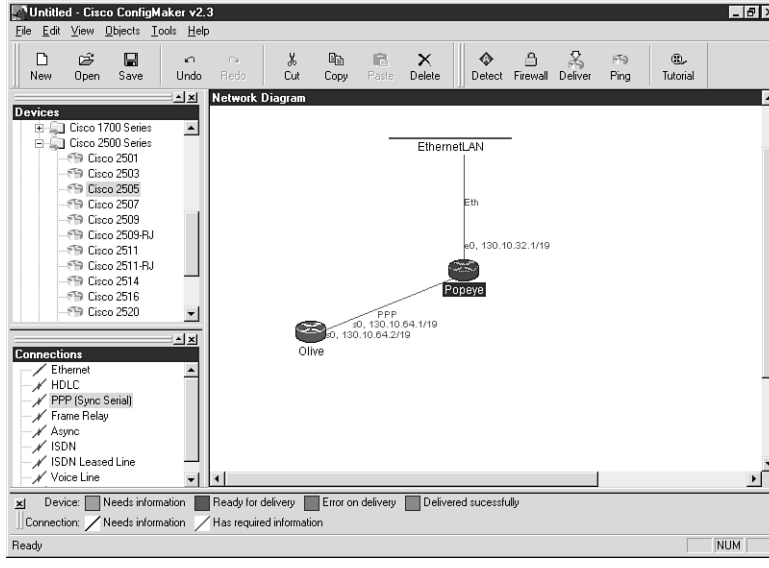


Рис. 16.12. Отметьте маршрутизатор, которому нужно доставить конфигурацию

2. Щелкните по кнопке **Deliver** (Доставить) в строке состояния Cisco ConfigMaker. Откроется подпрограмма доставки конфигурации для того маршрутизатора, который вы задали в сетевой диаграмме. Щелкните по кнопке **Next**.
3. Далее Cisco ConfigMaker напомнит вам о том, что ни одна другая программа не должна использовать COM-порт, который будет задействован для доставки конфигурации (если данный компьютер служит консолью, отключите программное обеспечение эмуляции терминала).

4. Щелкните по кнопке **Next**.
5. В окне подпрограммы появится строка состояния для доставки конфигурации (рис. 16.13). Текущая конфигурация маршрутизатора (если таковая есть) будет удалена, а после перезагрузки маршрутизатора новая конфигурация сохранится в памяти NVRAM.

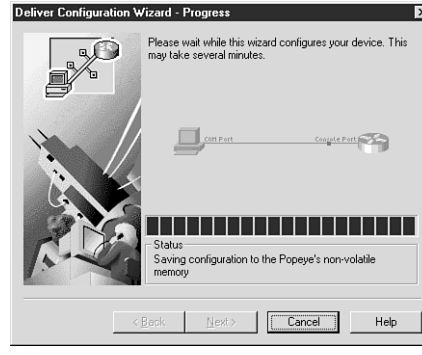


Рис. 16.13. Просмотр строки состояния для доставки конфигурации

6. В открывшемся диалоговом окне подпрограммы можно увидеть имя маршрутизатора, метод доставки (консоль), а также дату и точное время завершения доставки. Нажмите клавишу **Finish** для выхода из подпрограммы.

Теперь маршрутизатор готов функционировать с загруженной конфигурацией. Проверить ее настройку удобно посредством команды `show startup-config`: на экране должны появиться те же установки, которые имеются в вашей сетевой диаграмме Cisco ConfigMaker.

После завершения работы с сетевой диаграммой щелкните по кнопке **Save** (Сохранить) в строке состояния Cisco ConfigMaker. В диалоговом окне **Save as** (Сохранить как) введите имя сетевой диаграммы, а в окне **Save In** (Сохранить в) – путь сохранения файла. Затем снова щелкните по кнопке **Save**.

Чтобы выйти из программы, воспользуйтесь командами **File** ⇒ **Exit** (Файл ⇒ Выход). Cisco ConfigMaker удобна для получения дополнительных сведений о конфигурации аппаратных средств и программного обеспечения различных маршрутизаторов и устройств, производимых компанией Cisco.

➢ О подключении консоли компьютера к маршрутизатору рассказывается в главе 7, раздел «Подсоединение к консоли».

Программа Cisco ConfigMaker работает так же, как и любое стандартное приложение Windows. Чтобы получить дополнительную информацию, воспользуйтесь встроенной в программу справочной системой.

ГЛАВА 17

Сервер TFTP

Сервер TFTP

Возможность сохранения конфигурации маршрутизатора не только в памяти NVRAM, но и в другом месте позволяет сберечь время и усилия, затраченные на ее создание, поскольку настройка является основным фактором, определяющим работу маршрутизатора. Сделав резервную копию конфигурации маршрутизатора, вы будете уверены в том, что в случае неполадки легко восстановите систему. При повторной настройке маршрутизатора удобнее пользоваться командой `copy` для копирования новых параметров из текущей конфигурации в стартовую, находящуюся в памяти NVRAM маршрутизатора. Разрешается также скопировать текущую или стартовую конфигурацию на подключенный к сети компьютер.

Упрощенный протокол передачи данных (Trivial File Transfer Protocol – TFTP) – это транспортный протокол стека TCP/IP, использующийся для перемещения файлов с маршрутизатора на компьютер, который работает с программным обеспечением для сервера TFTP. Этот протокол похож на протокол FTP, применяемый для пересылки файлов в сети Internet (ваш Web-браузер поддерживает протокол FTP), но не требует ввода имени пользователя и пароля (отсюда и название «упрощенный»). Необходимо указать только IP-адрес компьютера, работающего с программным обеспечением для сервера TFTP, и вы сможете скопировать созданный файл конфигурации на сервер. Также разрешается использовать серверы TFTP для копирования файла конфигурации на маршрутизатор, а также для обновления (или изменения) установленной операционной системы IOS путем копирования нового файла IOS в память маршрутизатора. Так как большинство маршрутизаторов не имеют жестких дисков, серверы TFTP служат хранилищами их резервных файлов (например, скопированных или альтернативных конфигураций). На рис. 17.1 показаны различные варианты обмена файлами между маршрутизатором и сервером TFTP.

Итак, сервер TFTP представляет собой компьютер, на котором функционирует программное обеспечение для сервера TFTP. Поскольку имя пользователя и пароль не требуются, для подключения к серверу достаточно ввести только его IP-адрес.

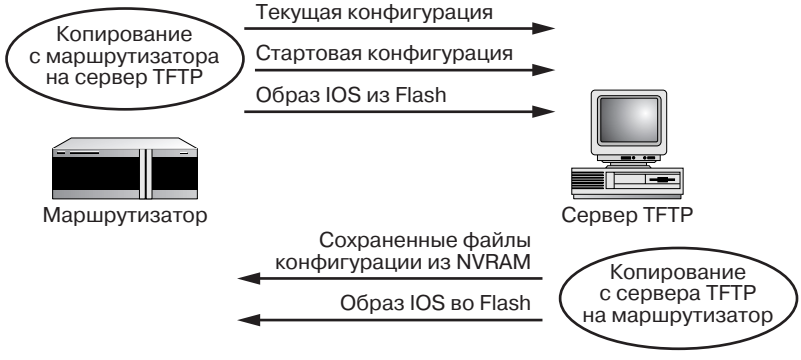


Рис. 17.1. Копирование файлов с маршрутизатора на сервер TFTP и обратно

Вы, вероятно, неоднократно загружали файлы с сайтов FTP и вас наверняка не спрашивали об имени пользователя или пароле. Многие сайты FTP в сети Internet анонимные. Зайти на такие сайты разрешается, не вводя имя пользователя и пароль (в противном случае паролем послужит ваш IP-адрес или адрес электронной почты). Если же вы обращаетесь на защищенный сайт FTP, эти параметры указывать обязательно.

➢ О том, как использовать команду Copy с файлами конфигурации, рассказывается в главе 9, раздел «Проверка памяти маршрутизатора».

Программное обеспечение для сервера TFTP

Доступно несколько различных пакетов программного обеспечения для серверов TFTP. Зарегистрированным пользователям своей продукции компания Cisco бесплатно предоставляет приложение для поддержки такого сервера (его можно загрузить с Web-сайта http://www.cisco.com).

Если вы хотите работать с программным обеспечением для другого сервера TFTP, воспользуйтесь поисковой системой в сети Internet (ключевые слова – TFTP server). На Web-сайте, расположенном по адресу www.solarwinds.net, имеется программное обеспечение для TFTP-сервера компании SolarWinds, которая производит программы для маршрутизаторов Cisco. Обратите внимание: большинство различных пакетов программного обеспечения для серверов TFTP функционируют одинаково. Сначала запускается ПО для сервера, а затем выполняются соответствующие команды на маршрутизаторе. Сервер TFTP достаточно пассивен, но многие его приложения открываются в отдельном окне, где отображается строка состояния для копирования на сервер и обратно.

Если вам нужно программное обеспечение для сервера TFTP компании Cisco, войдите на Web-сайт www.cisco.com, указав имя пользователя и пароль (они пре-

доставляются дилером компании Cisco, у которого вы приобрели маршрутизатор). Затем на домашней странице щелкните по кнопке **Software Center**[1] (Программное обеспечение).

В открывшемся окне щелкните по кнопке **Other Software** (Другие программы). Вы перейдете на страницу, где расположена ссылка для загрузки необходимого ПО (рис. 17.2). Щелкните по ней и выберите путь для установки программного обеспечения на вашем компьютере. После завершения загрузки вы можете инсталлировать программу (см. следующий раздел).

Рис. 17.2. Загрузка программного обеспечения для сервера TFTP с Web-сайта компании Cisco

Установка программного обеспечения для сервера TFTP компании Cisco

Установить программное обеспечение для сервера TFTP компании Cisco удобнее всего на рабочей станции Windows 95/98, которая находится в одной сети с маршрутизатором (то есть маршрутизатор по умолчанию используется как входной интерфейс для сервера TFTP). Например, если порт Ethernet 0 маршрутизатора сконфигурирован с IP-адресом 10.16.0.1, этот номер нужно ввести как входной интерфейс по умолчанию для рабочей станции. Кроме того, IP-адрес рабочей станции должен располагаться в том же диапазоне подсети, что и порт Ethernet 0. Так

[1] В настоящее время с сайта Cisco программное обеспечение для сервера TFTP может получить и неавторизированный пользователь. – *Прим. научн. ред.*

как сеть класса A разделена на 14 подсетей (это определяется по первому октету IP-адреса входного интерфейса по умолчанию), а первая подсеть задействована в сети Ethernet, подсоединенной к порту Ethernet 0 маршрутизатора, диапазон доступных IP-адресов составит от 10.16.0.1 до 10.32.255.254. Рабочая станция играет роль сервера TFTP, поэтому ее IP-адрес должен находиться в указанном диапазоне. В данном случае в диалоговом окне свойств протокола TCP/IP выбран адрес 10.16.0.4 (рис. 17.3).

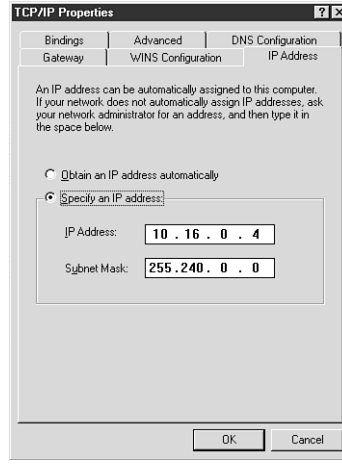


Рис. 17.3. Убедитесь, что рабочей станции, которая будет выступать в качестве сервера TFTP, присвоен соответствующий IP-адрес

После того как вы указали IP-адрес, можно приступать к инсталляции на рабочей станции программного обеспечения для сервера TFTP. Установка ПО компании Cisco выполняется следующим образом:

1. С помощью программы Windows Explorer найдите папку, в которую вы поместили ПО.
2. Дважды щелкните по иконке **Cisco TFTP**, чтобы запустить программу инсталляции.
3. Прочитав выведенное сообщение, щелкните по кнопке **Next** и напечатайте путь для установки программного обеспечения сервера TFTP или поместите его в папку, выбранную по умолчанию.
4. Укажите другую папку при помощи кнопки **Browse** (Обзор) или выберите путь по умолчанию. Щелкните по кнопке **Next**.
5. Появится папка с иконками для программ TFTP. Вы можете перенести их в другую папку, отметив ее в списке. Снова щелкните по кнопке **Next**.
6. Будет произведена установка программного обеспечения. Щелкните по кнопке **Finish**, чтобы завершить процесс инсталляции.

Если вы используете сервер DHCP, например сервер NT 4 и протокол DHCP, рабочим станциям в сети будут автоматически присваиваться IP-адреса. В таком случае на сервере DHCP следует заблокировать адрес рабочей станции, выполняющей функцию сервера TFTP, и задать этот адрес в окне свойств протокола TCP/IP (см. рис. 17.3).

После установки программного обеспечения на рабочей станции можно обмениваться файлами с сервером. В следующем разделе рассказывается, как скопировать файл конфигурации на сервер TFTP.

Копирование файлов на сервер TFTP

Файлы стартовой конфигурации из памяти NVRAM или файл текущей конфигурации из памяти RAM разрешается копировать на сервер TFTP. Допустим, имеется стартовая конфигурация, сохраненная в памяти NVRAM, которую требуется скопировать на сервер TFTP перед тем, как вносить в нее изменения (так вы сможете восстановить прежнюю стартовую конфигурацию маршрутизатора, если произведенные изменения будут неудачными).

Копирование стартовой конфигурации на сервер TFTP производится так:

1. Запустите программное обеспечение сервера TFTP на рабочей станции, выполнив команды **Пуск ⇒ Программы ⇒ Cisco TFTP Server**. Откроется диалоговое окно сервера TFTP – серый экран, где в строке состояния отображен IP-адрес сервера TFTP, работающего с программным обеспечением сервера TFTP компьютера.
2. Войдите в привилегированный режим из консоли маршрутизатора с помощью команды `enable` и пароля.
3. В командной строке маршрутизатора наберите `copy startup-config tftp` и нажмите клавишу **Enter**.
4. Введите IP-адрес хоста для удаленного доступа и IP-адрес сервера TFTP (в нашем примере – 10.16.0.4). Затем нажмите **Enter**.
5. Укажите имя файла, который необходимо записать на сервер. По умолчанию имя маршрутизатора сопровождается словом `confg` (например, `cisco2505-confg`). Задайте имя файла конфигурации для копирования или примите имя по умолчанию, а затем нажмите **Enter**.
6. Программа запросит подтверждение (рис. 17.4). Нажмите клавишу **Enter** для подтверждения (в противном случае введите `n`, и вы вернетесь в строку привилегированного режима).

Файл будет сохранен на сервере TFTP. Запись в строке `Writing router name-config. !! [OK]` обозначает, что копирование прошло успешно. В окне сервера TFTP можно найти запись об успешном выполнении копирования (рис. 17.5).

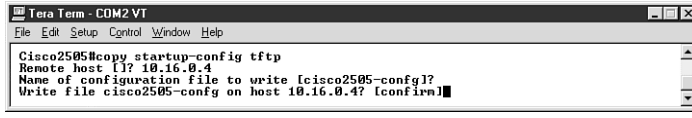


Рис. 17.4. Подтвердите правильность IP-адреса сервера TFTP и имени файла, который желаете скопировать

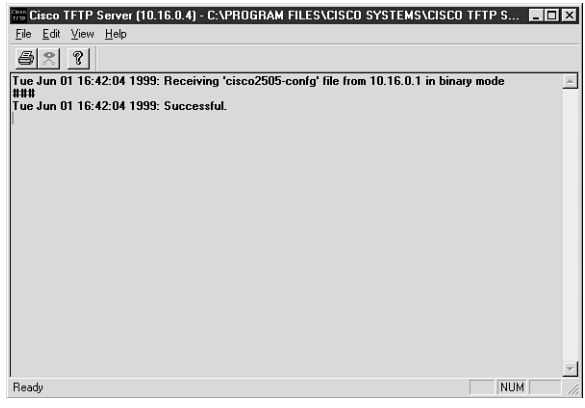


Рис. 17.5. В окне сервера TFTP имеется информация о выполненном копировании

Копирование текущей конфигурации из памяти RAM производится аналогично. Единственное отличие состоит в том, что в пункте 3 нужно ввести команду `copy running-config tftp`.

Копирование файлов с сервера TFTP

Копирование файлов с сервера TFTP выполняется так же легко, как и действие, описанное в предыдущем разделе. Вы можете переписывать файл конфигурации с сервера TFTP в память NVRAM маршрутизатора или напрямую в память RAM как новую текущую конфигурацию. Файл, сохраненный в памяти NVRAM, становится не только новой текущей конфигурацией, но и стартовой после перезагрузки маршрутизатора.

Вы можете просмотреть скопированный файл при помощи программы Windows Explorer на рабочей станции, играющей роль сервера TFTP. Щелкните по иконке Мой компьютер правой кнопкой мыши и выберите в меню пункт Проводник. По умолчанию папка для сервера TFTP устанавливается так: C:\Cisco Systems\Cisco TFTP Server. Проверьте эту папку в программе Windows Explorer, и вы увидите копию файла конфигурации, которую туда записали.

Рассмотрим процесс копирования файла конфигурации с сервера в память NVRAM:

1. Запустите программное обеспечение сервера TFTP на рабочей станции.
2. С консоли маршрутизатора войдите в привилегированный режим при помощи команды `enable` и пароля.
3. В командной строке маршрутизатора наберите `copy tftp startup-config`, затем нажмите клавишу **Enter**.
4. Далее задайте IP-адрес хоста для удаленного доступа и IP-адрес сервера TFTP (в нашем примере 10.16.0.4). Затем нажмите **Enter**.
5. Укажите в строке имя файла, который требуется скопировать с сервера (если при копировании файла на сервер вы выбрали имя по умолчанию, вводить новое имя не нужно). Нажмите клавишу **Enter**.
6. Для подтверждения (рис. 17.6) снова нажмите **Enter**.

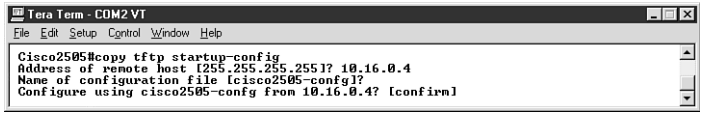


Рис. 17.6. Введите IP-адрес сервера и имя файла и нажмите клавишу Enter для подтверждения

Файл загрузится на маршрутизатор и станет активной конфигурацией (а также будет сохранен в памяти NVRAM). На маршрутизаторе появится сообщение `[OK]`, обозначающее, что копирование прошло успешно. Теперь можете вернуться на сервер TFTP, где вы также получите подтверждение безошибочного завершения процедуры.

Загрузка новой версии IOS с сервера TFTP

Как видите, копировать файлы на сервер TFTP и обратно достаточно несложно (по сравнению с созданием подсетей IP или с конфигурированием маршрутизатора). Сервер TFTP также может использоваться для записи различных версий IOS в память Flash RAM маршрутизатора, что упрощает обновление операционной системы.

Компания Cisco периодически выпускает новые версии IOS для своих маршрутизаторов. Так, во время написания данной книги вышла версия 12. Конечно, здесь, как и в любой новой операционной системе, были найдены ошибки, поэтому после выхода новой версии IOS появилось несколько дополнений. Исправленные варианты создаются даже для устаревших версий IOS компании Cisco, например 11. За дополнительной информацией обращайтесь на сайт www.cisco.com.

Чтобы загрузить новые файлы операционной системы, нужно заключить соответствующее соглашение с дилером компании Cisco, у которого вы приобрели маршрутизатор. Вам необходимо знать номер подписанного контракта и зарегистрироваться на сайте компании Cisco. На рис. 17.7 показана Web-страница, где имеются ссылки на файлы различных версий IOS и программа-планировщик системы IOS, которая позволит выбрать новые версии IOS для вашего маршрутизатора (так, если вам нужен маршрутизатор Cisco 2505, на странице программы-планировщика отобразятся только те версии IOS, которые поддерживаются этим устройством).

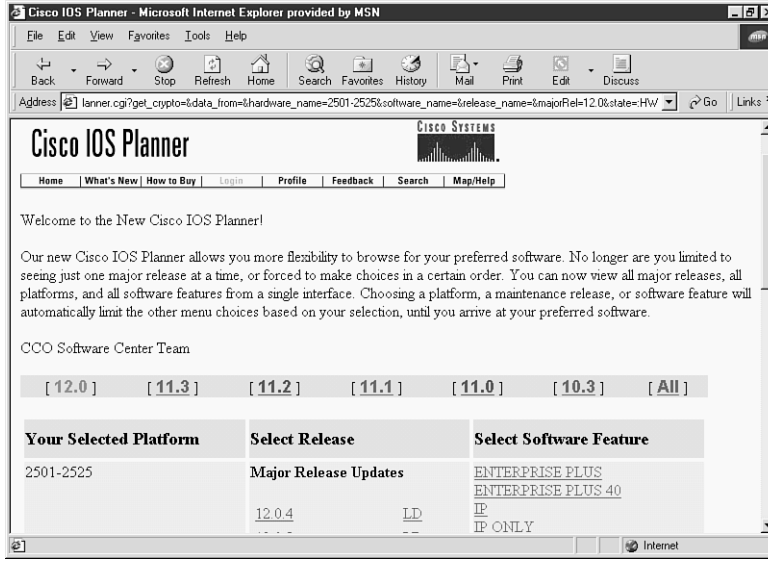


Рис. 17.7. Программа-планировщик IOS на Web-странице компании Cisco

Для загрузки новой версии IOS в память Flash RAM маршрутизатора скопируйте соответствующий файл с Web-сайта компании Cisco (или с компакт-диска, если вы приобрели обновление системы IOS) и поместите его в корневой каталог сервера TFTP. По умолчанию для этого каталога задается путь C:\Cisco Systems\Cisco TFTP Server. Воспользуйтесь программой Windows Explorer для копирования или перемещения файла в нужный каталог.

Теперь все готово к копированию новой версии системы IOS в память Flash RAM маршрутизатора. Помните, что новая версия IOS заменит предыдущую. При копировании допустимо указать, что вы не желаете очищать память Flash RAM: в таком случае в памяти будут записаны две версии IOS. Однако маршрутизатор 2505 имеет объем памяти Flash RAM 8 Мб, поэтому вы, к сожалению, не сможете сохранить более одной версии системы IOS.

Если новая копия не работает, значит, сервер TFTP не найден в сети. Убедитесь, что рабочая станция подсоединена к сети и IP-адрес рабочей станции/сервера TFTP находится в том же диапазоне подсети, что и порт Ethernet маршрутизатора, который обслуживает эту подсеть. Если при такой проверке вы не обнаружили ошибок, протестируйте сервер TFTP командой `ping`. Введите в строке консоли маршрутизатора команду `ping IP Address`, где `IP Address` – это IP-адрес рабочей станции/сервера TFTP, а затем нажмите клавишу Enter. Если неисправность не будет найдена, переустановите программное обеспечение сервера TFTP.

После того как вы скопировали файл IOS на сервер TFTP, переместите его в память Flash RAM маршрутизатора:

1. Запустите программное обеспечение сервера TFTP на рабочей станции.
2. С консоли маршрутизатора войдите в привилегированный режим посредством команды `enable` и пароля.
3. В командной строке маршрутизатора наберите `copy tftp flash`, затем нажмите клавишу **Enter**.
4. Появится сообщение о начале копирования, и работа маршрутизатора будет остановлена на время обновления версии IOS. Для продолжения нажмите клавишу **Enter**.
5. Введите IP-адрес хоста для удаленного доступа и IP-адрес сервера TFTP (в нашем примере 10.16.0.4). Затем нажмите **Enter**.
6. Укажите в строке имя файла IOS на сервере TFTP, который вы желаете скопировать. Убедитесь, что отмеченный файл – это файл IOS; для примера мы используем имя 80114109.bin, то есть имя файла версии IOS 11.2. Для продолжения нажмите **Enter**.
7. Назначьте имя файла для копирования. Введите имя файла IOS по умолчанию (как указано в пункте 6) и нажмите клавишу **Enter**.
8. Подтвердите удаление всей информации из памяти Flash RAM маршрутизатора перед копированием новой версии IOS, нажав **Enter**. Так как в памяти Flash RAM содержится текущая версия IOS, программа повторно запросит подтверждения. Снова нажмите клавишу **Enter**.
9. Чтобы сохранить измененную конфигурацию системы, напечатайте `yes`, затем нажмите **Enter**. Рис. 17.8 иллюстрирует порядок ввода команд на маршрутизаторе Cisco 2505 при выполнении обновления версии операционной системы IOS.
10. Еще раз подтвердите удаление всей памяти Flash RAM: введите `yes` и нажмите **Enter**.

Текущая версия системы IOS будет удалена и заменена новой. На маршрутизаторе появится несколько сообщений о ходе выполнения операции. Весь процесс

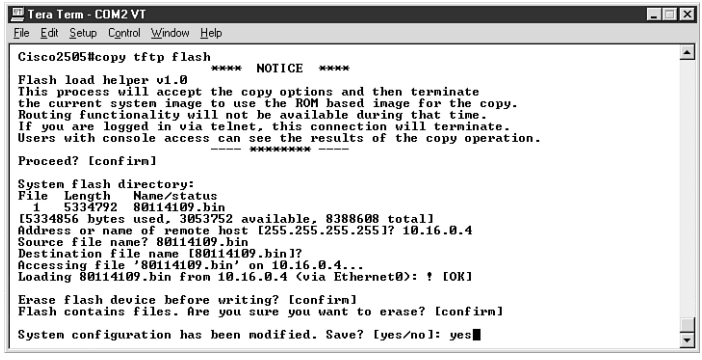


Рис. 17.8. Вам потребуется несколько раз подтвердить копирование новой версии IOS в память Flash RAM маршрутизатора

может занять несколько минут, поскольку файлы IOS бывают достаточно большими (например, файл для версии 11.2 занимает более 6 Мб). Если вы посмотрите на диалоговое окно сервера Cisco TFTP, то заметите, что при выполнении копирования на экране повторяются символы #.

После завершения копирования произойдет перезагрузка маршрутизатора. Чтобы войти в пользовательский режим, нажмите клавишу **Enter** и введите пароль для консоли (если требуется). Проверить версию IOS удобно с помощью команды `show flash`. Теперь в памяти Flash RAM маршрутизатора находится новый файл IOS (его имя соответствует данным, введенным вами в пункте 6).

Чтобы создать резервную копию памяти Flash RAM на случай возникновения неполадок в работе маршрутизатора, текущий файл IOS можно скопировать на сервер TFTP. Для этого введите в строке привилегированного режима команду `copy flash tftp`, а затем – IP-адрес сервера и другую информацию, как указывалось выше.

Сервер TFTP служит удобным хранилищем для различных файлов конфигураций и обновлений IOS. Он предоставляет место для резервных копий, которого нет на маршрутизаторе.

ГЛАВА 18

Устранение неисправностей в работе маршрутизатора

Хотя тема устранения неисправностей в соединениях и конфигурациях маршрутизатора настолько обширна, что заслуживает написания отдельной книги (или книг), мы решили закончить рассказ о сетях и маршрутизаторах Cisco кратким описанием методики исправления возможных неполадок.

Устранение неисправностей аппаратных средств

При работе вы можете столкнуться с повреждением контроллера интерфейса маршрутизатора и прочими поломками, которые часто приводят к нарушению функционирования интерфейса и даже к выходу из строя самого маршрутизатора.

Другие проблемы в сети, как правило, подразделяются на две категории: повреждение систем соединения и неверная конфигурация маршрутизатора. С некоторыми неисправностями в соединениях, например с повреждением последовательного кабеля маршрутизатора или аппаратной неполадкой, легко справиться, заменив сетевой коммутатор или отрезок сетевого кабеля. Разумеется, вы не сможете устранить ряд серьезных проблем, допустим повреждение АТС телефонной компании. С определенными неисправностями вы в состоянии справиться сами, с другими – нет; иногда приходится сидеть и ждать (в то время как пользователи вашей сети не могут получить доступ к сетевым ресурсам).

Что касается проблем с конфигурацией, то при модификации структуры сети необходимо изменить соответствующие параметры настройки, и наоборот: чтобы избавиться от проблем в сети, придется подкорректировать начальную конфигурацию. Далее в этой главе описываются возможные трудности с конфигурацией и методы исправления неполадок при работе с различными сетевыми протоколами.

Проблемы с маршрутизаторами

Аппаратные проблемы маршрутизатора могут быть вызваны неисправностью контроллеров интерфейсов, блоков памяти RAM, процессора и даже вентилятора.

И как это ни примитивно, прежде всего следует проверить, подведено ли питание к маршрутизатору и включен ли он.

В главе 6 речь шла об основных принципах работы интерфейсов маршрутизатора. Различные сетевые и WAN-интерфейсы маршрутизатора подключены к контроллерам, которые установлены либо на материнской плате маршрутизатора (например, для маршрутизаторов серии 2505), либо на карте интерфейса, расположенной в каком-либо из доступных слотов маршрутизатора (в частности, для маршрутизаторов Cisco серии 4500).

Один из способов проверки интерфейса маршрутизатора – использование команды `show interfaces`. Если при выполнении этой команды интерфейс и линейный протокол на экране показаны с пометкой `up` (рис. 18.1), значит, интерфейс функционирует нормально; если же контроллер интерфейса не работает, он не будет выведен в качестве доступного. Если интерфейс в порядке (обозначен `up`), а линейный протокол нет (помечен как `down`), неисправность нужно искать в конфигурации, а не в аппаратных средствах.

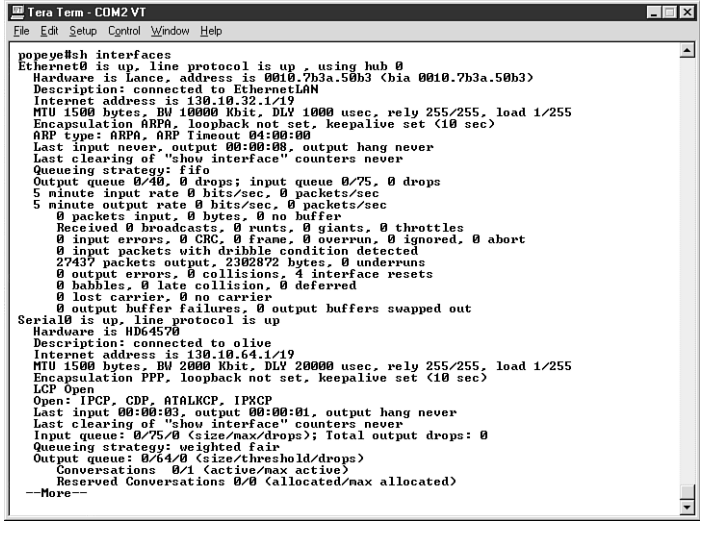


Рис. 18.1. Для проверки интерфейсов маршрутизатора используется команда ***show interfaces***

Вы также можете проверить контроллеры маршрутизатора. Команда `show controllers` выдает сведения о контроллерах различных интерфейсов. На рис. 18.2 показан результат исполнения команды `show controller ethernet`.

Необходимо уделить внимание и такому компоненту маршрутизатора, как вентилятор: это одна из самых дешевых его частей и одновременно одна из самых значимых. Если вентилятор неисправен, устройство перегреется (аналогично компьютеру со сломанным вентилятором) и произойдет перезагрузка. Поэтому, если

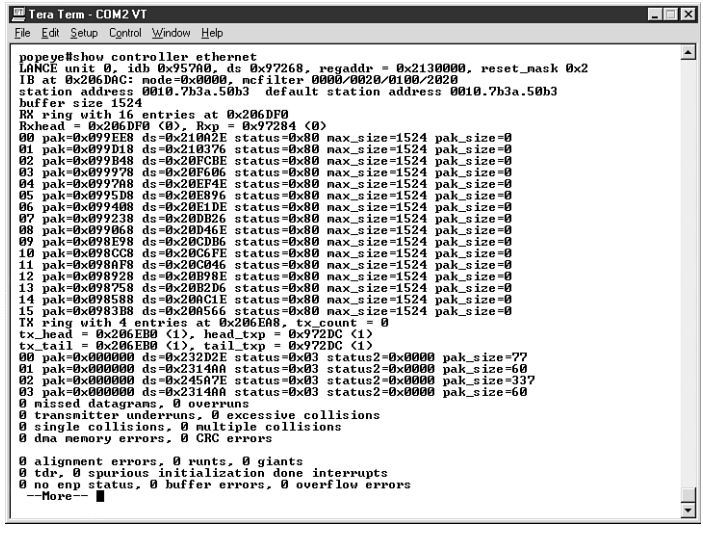


Рис. 18.2. Просмотр информации о различных контроллерах, установленных на маршрутизаторе

маршрутизатор постоянно перезагружается после непродолжительного времени работы, включите его и послушайте, работает ли вентилятор (некоторые из маршрутизаторов Cisco последних серий имеют комплексные системы охлаждения, где можно увидеть показатель температуры устройства).

> ***Последовательный интерфейс может перестать функционировать из-за плохого контакта в кабеле V.35. Всегда проверяйте различные соединения LAN и WAN с маршрутизатором: неплотно подключенный кабель способен создать впечатление аппаратной неисправности.***

Если маршрутизатор перестал работать, трудно определить, была неисправность аппаратной или программной. Воспользуйтесь командой `show stacks`, чтобы прочитать сообщения об ошибках, которые были записаны в памяти в момент сбоя (представители сервисной службы компании Cisco применяют эту команду, чтобы выяснить, какой тип неполадки послужил причиной сбоя).

Время от времени возникают ситуации, когда у маршрутизатора не хватает памяти (или скорости процессора) для обработки направляемого на него трафика. В таком случае следует включить в сеть дополнительные маршрутизаторы для уменьшения трафика или улучшить (путем добавления или замены) некоторые компоненты (например, память), а иногда и заменить маршрутизатор устройством другой серии.

Сетевые администраторы находят *критические ресурсы*, или *узкие места* в сети (критический ресурс – это устройство, замедляющее трафик) при помощи специального пакета программного обеспечения для управления сетью[1]. Такой пакет, например CiscoWorks, обеспечивает мониторинг устройств, протоколов и других частей сети и позволяет просматривать текущее состояние сети. При работе с крупными сетями необходимо использовать подобные программы для управления сетью и различными сетевыми устройствами.

Независимо от того, с аппаратной или программной неисправностью вы столкнулись, устранять ее нужно последовательно. Сначала выясните, в чем суть проблемы. Затем соберите необходимую информацию (для этого используются некоторые команды маршрутизатора). После сбора данных проверяйте наличие каждой из возможных неполадок до тех пор, пока не найдете действительную. Если суетиться и одновременно изменять несколько параметров системы, вы вряд ли сможете обнаружить и устранить причину неисправности.

Другие аппаратные неполадки

Аппаратные неисправности, влияющие на функционирование маршрутизатора, имеют отношение к устройствам, которые связаны с ним напрямую.

В сетях Ethernet сетевые коммутаторы и концентраторы подключаются к порту Ethernet маршрутизатора. Если в работе коммутатора возникает сбой, перестает действовать и соединение LAN маршрутизатора, при этом адреса узлов в сети LAN становятся недоступными для других узлов в сети.

У сетевых коммутаторов на корпусе имеется лампа, по которой легко определить, функционирует устройство или нет. Если коммутатор включен, питание к нему подсоединено, но он по-прежнему не функционирует, необходимо заменить коммутатор.

Когда проблемы возникают с отдельными узлами в сети LAN, нужно проверить их работу. Особенностью сетевых коммутаторов являются индикаторные лампы, которые загораются в том случае, если порт коммутатора подключается к узлу через соответствующий кабель. Лампа не горит из-за неисправности кабеля (см. следующий раздел) либо порта сетевого коммутатора.

Аналогичные проблемы могут возникать при взаимодействии маршрутизатора и сетей Token Ring. К маршрутизатору подключается устройство доступа Token Ring (MAU), которое обеспечивает связь узлов в сети LAN с маршрутизатором. Если возникает сбой в работе блока доступа, перестает функционировать и соединение между сетью LAN и маршрутизатором.

Неисправности в устройствах, основанных на соединениях WAN, тоже могут создавать проблемы для сети. Маршрутизаторы часто подключаются к устройствам

[1] В англоязычной литературе критический ресурс обозначается термином *bottleneck*, что в дословном переводе означает «бутылочное горло». – *Прим. научн. ред.*

CSU/DSU, которые обеспечивают связь с выделенными линиями или сетями для передачи пакетов данных. Когда устройство CSU/DSU перестает действовать, нарушается соединение WAN между маршрутизатором и сетью.

Если аппаратная неисправность вызвана неполадкой в оборудовании провайдера, вы не сможете устранить ее самостоятельно. Вам придется подождать восстановления связи. На случай неисправностей администраторы часто создают в сети резервные соединения между маршрутизаторами. Допустим, что между двумя маршрутизаторами имеется связь Frame-Relay. Вы можете сконфигурировать маршрутизатор таким образом, чтобы он мог подключиться к другому маршрутизатору через модем. Телефонная линия модема не способна работать с такой скоростью, как соединение Frame-Relay, но в состоянии предоставить резервный путь передачи пакетов данных на случай сбоя.

Неисправности в кабельных соединениях

Причиной неисправностей в кабельных соединениях сети LAN может быть короткое замыкание, обрыв или другая проблема. Если вы считаете, что причина неполадки заключается в самом кабеле, воспользуйтесь соответствующими приборами для тестирования кабеля, например вольтметром или рефлектометром измерения временного интервала.

Цифровой вольтметр представляет собой простое устройство, которое можно подсоединить к кабелю для тестирования на обрыв и короткое замыкание. Вы узнаете, в рабочем состоянии кабель или нет, имеется ли обрыв или короткое замыкание. При наличии короткого замыкания нужно заменить кабель. Если есть обрыв, проверьте кабель и найдите место обрыва.

Рефлектометр измерения временного интервала – более сложный прибор, который способен не только выдать информацию о наличии короткого замыкания или обрыва в кабеле, но и обнаружить место неполадки. Для этого рефлектометр посылает по кабелю короткие импульсы и использует блок определения временного интервала для того, чтобы вычислить пройденное импульсом расстояние.

Сетевые кабели часто приходят в негодность. Вы можете случайно задеть кабель, передвигая мебель, или пролить на него воду, что приводит к короткому замыканию. Поэтому при наличии неисправности сначала проверьте кабель и лишь затем приступайте к проверке других устройств.

➢ О сетевых кабелях рассказывалось в главе 1, раздел «Сетевые кабели».

Резюме

Неисправность в соединении далеко не всегда вызвана аппаратным сбоем маршрутизатора. Произведите последовательную проверку всех устройств, описанных в данном разделе, а также их подключений к маршрутизатору. Поскольку маршрутизаторы практически постоянно работают (вам редко приходится включать и выключать их), они могут функционировать очень долго (пока не сломается вентилятор или рабочие условия не выйдут за рамки нормальных).

Защитить маршрутизатор от сбоев в сети можно при помощи некоторых устройств. Если прекратится подача питания, то блок бесперебойного питания будет подавать электроэнергию на маршрутизатор; сетевой фильтр предохранит маршрутизатор от перепадов напряжения в сети. Маршрутизатор во многом аналогичен компьютеру, поэтому для него нужно обеспечить соответствующие рабочие условия.

Устранение неисправностей в интерфейсах LAN

Устранять неисправности в соединениях маршрутизаторов и сетей LAN удобно при помощи информации, которая появляется на консоли маршрутизатора после ввода некоторых команд операционной системы IOS. Одним из наиболее мощных диагностических средств служит команда `show`. Ниже эта команда рассматривается применительно к двум распространенным типам сетей LAN – Ethernet и Token Ring.

➢ Сведения о сетевых архитектурах Ethernet и Token Ring приведены в главе 1, раздел «Виды сетевых архитектур».

Устранение неисправностей в сетях Ethernet

Ethernet – это пассивная сетевая архитектура, которая в качестве методики сетевого доступа использует *множественный доступ с опросом несущей и обнаружением конфликтов* (Carrier Sense Multiple Access with Collision Detection – CSMA/CD). Проблемы, связанные с данной сетевой архитектурой, могут быть вызваны конфликтами в сети. Причина таких конфликтов заключается в обрыве кабеля, наличии отрезков кабеля, длина которых превышает допустимую, а также в неисправностях сетевых карт, приводящих к чрезмерно напряженному сетевому трафику.

Команда `show interfaces ethernet [interface number]` позволяет просмотреть информацию по интерфейсам Ethernet. На рис. 18.3 представлен результат исполнения данной команды для интерфейса Ethernet 0 на маршрутизаторе Cisco 2505.

Хотя при первом взгляде на экран может показаться, что информации слишком мало, на самом деле ее достаточно для устранения неисправностей в интерфейсах Ethernet. Кроме того, данная команда уведомляет об использовании других ресурсов маршрутизатора, например памяти RAM. В нижеприведенном списке разъясняется, какие именно сведения предоставляет команда `show interfaces ethernet [interface number]`:

- `Ethernet0 is up, line protocol is up` сообщает, что интерфейс в норме и линия для протоколов Ethernet также функционирует. Если интерфейс не работает (помечен как `down`), проверьте соединение LAN с интерфейсом. Если соединение действует, попробуйте восстановить работоспособность интерфейса в режиме конфигурации. Для этого войдите в режим configuration-if и протестируйте интерфейс, введя команду `shut` (Отключение интерфейса),

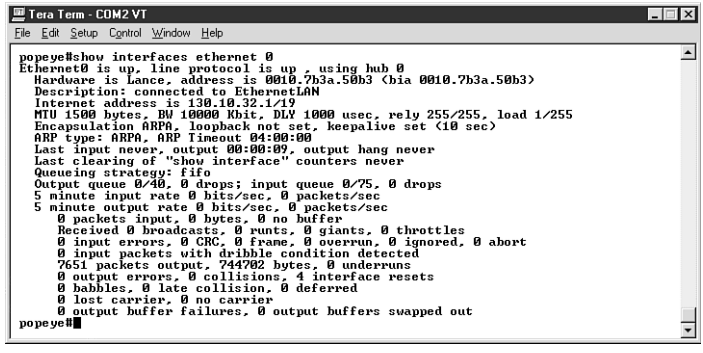


Рис. 18.3. Просмотр сведений об интерфейсе Ethernet 0 маршрутизатора

а затем команду `no shut` (Повторное включение), после чего интерфейс может вернуться к нормальной работе;

- `Hardware address` выводит шестнадцатеричный MAC-адрес интерфейса;
- `Internet address` предоставляет IP-адрес и маску подсети, приписанные интерфейсу (об IP-адресации рассказывается ниже, в разделе «Обнаружение и устранение неисправностей протокола TCP/IP»);
- `MTU` выдает максимальный размер обрабатываемого кадра в байтах;
- `BW` описывает пропускную способность интерфейса, измеряемую в килобитах в секунду;
- `rely` вычисляет надежность линии при том условии, что линия 255/255 считается абсолютно надежной. Чем меньше первое число в расчете, тем ненадежнее соединение интерфейса (по причине неисправных линий и т.д.);
- `load` измеряет текущую нагрузку интерфейса. Считается, что интерфейс загружен максимально при значении 255/255 (это число указывает на чрезмерно высокий трафик, для обслуживания сети в таком случае требуется добавить еще один интерфейс или маршрутизатор);
- `Encapsulation` определяет тип кадра Ethernet, заданный для интерфейса (по умолчанию устанавливается 802.2 Ethernet). Если он не соответствует типу кадров вашей сети (например, сеть NetWare с типом кадра 802.3), его следует изменить. Введите команду `arp` в строке config-if интерфейса и задайте соответствующий тип кадра Ethernet – например, `arpa` или `snap`;
- `collisions` показывает количество конфликтов на интерфейсе. Большое число указывает, что в сети имеется обрыв кабеля или неисправная сетевая карта, которая вызывает чрезмерный трафик, либо свидетельствует о том, что в сети LAN задействованы слишком длинные кабели.

Итак, всего одна команда операционной системы IOS предоставляет большой объем данных о состоянии интерфейса и трафика. Проблемы с интерфейсом Ethernet могут быть вызваны наличием неисправностей в самой сети LAN (например, большим числом конфликтов).

Поиск неисправностей в сетях Token Ring

В качестве методики доступа к сети LAN сетевая архитектура Token Ring использует *передачу маркера*. Устройство, имеющее маркер, может передавать информацию, другие устройства должны ждать получения маркера. Поэтому проблемы в сетях Token Ring не связаны с конфликтами при пересылке пакетов данных, как в сетях Ethernet.

Для просмотра информации по интерфейсам Token Ring служит команда `show interfaces tokenring [interface number]`. Аналогично команде `show interfaces` для Ethernet, она показывает состояние интерфейса, выводит аппаратный адрес и адрес протокола интерфейса, а также сведения о надежности интерфейса. Некоторые параметры команды схожи с настройками, которые указываются для порта Ethernet (например, `Hardware Address`, `Internet Address`, `MTU`, `BW` и `Rely`); другие установки имеют отношение к функциональным особенностям сетей LAN с архитектурой Token Ring, например к скорости перемещения данных по кольцу:

- `Token ring is up` сообщает о том, что интерфейс функционирует. Если интерфейс перестал работать (помечен как `down`), его можно восстановить в режиме configuration-if;
- `Hardware address` выводит шестнадцатеричный MAC-адрес интерфейса;
- `Internet address` определяет IP-адрес и маску подсети, приписанные интерфейсу (IP-адресация описывается ниже, в разделе «Обнаружение и устранение неисправностей протокола TCP/IP»);
- `MTU` предоставляет сведения о максимальном размере обрабатываемого кадра в байтах;
- `BW` указывает пропускную способность интерфейса в килобитах в секунду;
- `rely` вычисляет надежность линии при том условии, что линия 255/255 считается абсолютно надежной. Данный расчет для интерфейса производится каждые пять минут;
- `load` измеряет текущую нагрузку интерфейса. Загруженность 255/255 считается максимальной (это число указывает на то, что данный интерфейс маршрутизатора не в состоянии обслужить такую крупную сеть Token Ring LAN);
- `Ring Speed` определяет скорость сети Token Ring LAN, к которой подсоединен маршрутизатор. Все устройства в сети Token Ring, включая маршрутизатор, должны передавать сообщения по кольцу с одинаковой скоростью (4 или 16 Мб/с): любое несоответствие приведет к нарушению в потоке данных. Чтобы проверить, какая скорость у маршрутизатора, введите команду `show running-config`. Если скорость нужно изменить, воспользуйтесь командой `ring-speed` в режиме config-if в консоли маршрутизатора для данного интерфейса;
- `Restarts` отображает количество перезагрузок интерфейса. Для порта Token Ring значение данного параметра всегда должно быть равно 0. В противном случае в сети Token Ring LAN имеется неполадка, вызвавшая перезагрузку интерфейса.

Устранение неисправностей в интерфейсах Token Ring требует очень хорошего знания принципов работы сетей Token Ring LAN. Например, чтобы избежать перегрузки колец, сеть Token Ring LAN понадобится разделить на дополнительные сегменты. И хотя в данном разделе приводится основная информация по установкам интерфейсов Token Ring, вам следует более детально изучить сетевую архитектуру Token Ring. Все документы по этой сетевой архитектуре можно получить на сайте www.ibm.com (сайт создателей Token Ring).

Устранение неисправностей в интерфейсах WAN

Устранение неисправностей в интерфейсах WAN аналогично интерфейсам LAN. Для просмотра необходимой информации предназначена команда `show interface serial [interface number]`. Однако есть некоторая сложность: в последовательном соединении между маршрутизаторами могут использоваться различные WAN-протоколы (PPP или Frame-Relay). Кроме того, имеет значение и такой фактор, как состояние выделенных линий вашего провайдера.

Рассмотрим команду `show interface serial [interface number]` и то, как предоставляемая ею информация помогает при выявлении неисправностей (на рис. 18.4 показан результат исполнения команды `show interface serial 0` для маршрутизатора 2505):

- `Serial0 is up` сообщает, что интерфейс функционирует. Если интерфейс не работает (помечен как `down`), проверьте соединение между ним и устройством CSU/DSU, а также кабель. Возможно, неисправна телефонная линия, к которой вы подключаетесь (если устройство CSU/DSU в порядке, узнайте у провайдера, действует ли линия: позвоните ему и оцените состояние маршрутизатора на другом конце соединения). Можете попробовать восстановить работу интерфейса в режиме конфигурации (как было показано в разделе, посвященном интерфейсам Ethernet);
- `line Protocol is up` указывает, что задействованные WAN-протоколы используют данную линию. Если линейный протокол не работает (помечен как `down`), ваш маршрутизатор, вероятно, неправильно сконфигурирован (для проверки применяйте команду `show running-config`) либо тот маршрутизатор, к которому вы подсоединяетесь, не сконфигурирован для работы с соответствующим протоколом. Причиной проблемы также может быть неисправность в сети провайдера или в оборудовании связи;
- `Internet address` выводит IP-адрес и маску подсети, заданные интерфейсу (IP-адресация рассматривается ниже, в разделе «Обнаружение и устранение неисправностей протокола TCP/IP»);
- `MTU` предоставляет информацию о максимальном размере обрабатываемого кадра в байтах;
- `BW` определяет пропускную способность интерфейса в килобитах в секунду. Данный параметр интерфейса устанавливается в строке config-if при помо-

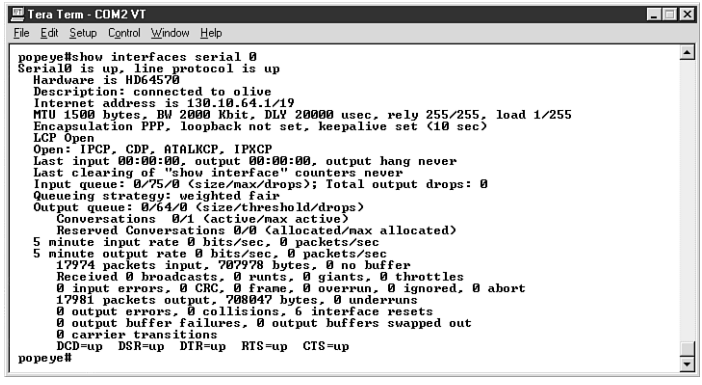


Рис. 18.4. Просмотр информации о последовательном интерфейсе маршрутизатора

Чтобы проверить, поступает ли сигнал от устройства CSU/DSU, воспользуйтесь блоком проверки сигнала (breakout box). Отсоедините устройство CSU/DSU от маршрутизатора и подключите его к данному блоку. Если сигнала нет, значит, выделенная линия неисправна или не подключена к устройству CSU/DSU.

щи команды `bandwidth`. Пропускная способность должна соответствовать скорости линии, к которой подсоединен последовательный интерфейс маршрутизатора;

- `rely` вычисляет надежность линии при том условии, что линия 255/255 считается абсолютно надежной. Чем меньше первое число в расчете, тем ненадежнее соединение интерфейса (по причине неисправных линий и т.д.);
- `load` измеряет текущую нагрузку интерфейса. Загруженность 255/255 считается максимальной (это число указывает на чрезмерно высокий трафик, для обслуживания сети LAN в таком случае требуется добавить еще один интерфейс или маршрутизатор);
- `Encapsulation` отображает название протокола WAN, назначенного интерфейсу. Он должен соответствовать тому WAN-протоколу маршрутизатора, который указан для другого конца соединения. Кроме того, WAN-протокол необходимо задать для того типа услуги, который вы получаете от провайдера (не устанавливайте протокол PPP, если вы подключаетесь к коммутатору Frame-Relay);
- `CRC` показывает число циклических проверок на избыточность, которые завершились неуспешно для входящих пакетов. Таким образом, легко выяснить, что телефонная линия содержит много шумов или что последовательный кабель между маршрутизатором и устройством CSU/DSU слишком длинный.

Здесь приводится только описание информации, которую выдает команда `show` для последовательного интерфейса маршрутизатора, а также методы обнаружения неисправностей в системе. Устранение описанных неполадок требует большого опыта по конфигурированию и работе с соединениями WAN в сети. Например, проверка подключений dial-up и ISDN – это целая наука. Чем больше времени вы проведете, изучая линии WAN, тем проще вам будет находить и устранять неисправности.

> ***Если вы сконфигурировали маршрутизатор как устройство DCE, на нем при помощи команды `clock rate` в строке config-if нужно задать счетчик времени для последовательного соединения. Правильный отсчет времени должен быть в интервале от 1200 до 800000000 бит/с. Проверить, был ли интерфейс сконфигурирован как устройство DCE, удобно посредством команды `show controllers serial [interface number]`. После ее выполнения вы получите информацию о счетчике времени, установленном для линии, а также о типе кабеля, подсоединенного к интерфейсу (DCE или DTE).***

Обнаружение и устранение неисправностей протокола TCP/IP

TCP/IP – это крупный стек протоколов, при работе с которым может возникать ряд проблем. В главе 10 уже говорилось, что разделение сетей IP на подсети крайне сложно, поэтому большинство неполадок в сетях IP вызвано неправильным конфигурированием маршрутизатора или узла в сети. Если, например, рабочая станция сконфигурирована с IP-адресом, который уже присвоен другой рабочей станции, такая станция функционировать не будет.

Рассмотрим наиболее частые неисправности, возникающие в сетях IP. Ниже приводится перечень распространенных проблем с описанием методов их устранения:

- неправильно сконфигурирован шлюз по умолчанию – когда вы устанавливаете рабочие станции и серверы в сети LAN, подсоединенной к маршрутизатору, в качестве шлюза по умолчанию для сети LAN (и всех компьютеров в ней) устанавливается IP-адрес интерфейса маршрутизатора, который напрямую подключен к сети LAN. Если рабочая станция не может связаться с сетью, проверьте этот шлюз (или его IP-адрес);
- на одном из устройств не задействована маршрутизация – используйте команду `show ip route` для того, чтобы проверить, сконфигурирован ли маршрутизатор для маршрутизации. Если в таблице маршрутизации нет соответствующих указаний, значит, устройство не конфигурировалось;
- не работает маршрутизирующий протокол – для создания таблицы маршрутизации нужно задействовать маршрутизирующий протокол. При проверке

пользуйтесь командой `show running-config` (данный протокол должен соответствовать тому, который задействован для других устройств в сети);

- не сконфигурирован IP-адрес для интерфейса – удостовериться, что интерфейсы были сконфигурированы с IP-адресами (за исключением тех последовательных соединений, которые могут быть сконфигурированы без IP-адресов), удобно при помощи команды `show ip interfaces`.

> ***В главе 14 рассматривались стандартные списки доступа IP. Если вы будете назначать списки доступа интерфейсам маршрутизатора, не представляя, как они повлияют на трафик, то совершите большую ошибку. Откажитесь от списка доступа, если вы не уверены, что он будет отбрасывать ненужный трафик и пропускать через интерфейс маршрутизатора необходимые пакеты.***

Команда ping

Команда `ping` – очень удобное средство проверки сетевых соединений между маршрутизаторами в сети (или узлами связи). Эта команда направляет узлу с указанным IP-адресом пакет ICMP. Если узел получил пакет, он отсылает его обратно. Время, которое пакет затратил на перемещение, измеряется в миллисекундах.

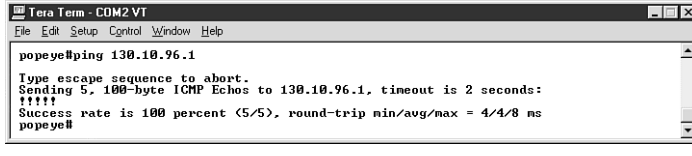


Рис. 18.5. Проверка соединения между маршрутизатором и узлами в сети

Чтобы воспользоваться командой `ping`, введите `ping [ip address]`, где `[ip address]` – IP-адрес интерфейса маршрутизатора или узла в сети, которому будет адресован пакет. На рис. 18.5 показан результат исполнения команды `ping` для двух маршрутизаторов.

Существует расширенная команда `ping`, которая позволяет задать тип протокола для отправляемого пакета данных (поскольку эта команда может использоваться с протоколами IPX и AppleTalk), размер пакета, а также временной интервал для ответа. Введите `ping` и нажмите клавишу **Enter**. Укажите сведения, которые последовательно запросит расширенная команда `ping`, нажимая клавишу **Enter** (так вы принимаете ответ по умолчанию). На рис. 18.6 показан результат исполнения расширенной команды `ping`.

> ***Команды `ping` и `trace` можно использовать в пользовательском или привилегированном режиме.***

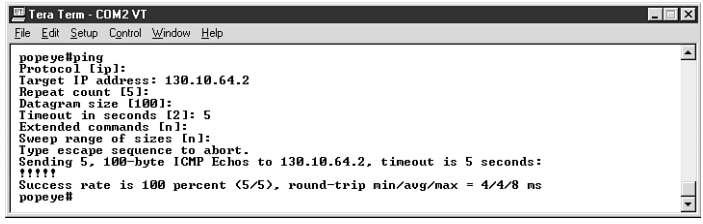


Рис. 18.6. Результат выполнения расширенной команды ***ping***

Команда trace

Для устранения неисправностей в соединениях предназначена команда `trace`, при помощи которой легко проследить путь пересылки пакетов от источника до получателя. Таким образом, вы можете определить, работают ли те устройства, которые должны участвовать в передаче пакетов между исходным маршрутизатором и конечным узлом. Чтобы воспользоваться командой `trace`, введите `trace [ip address]`.

На рис. 18.7 показан результат исполнения этой команды. Здесь выявленный маршрут состоит из одного напрямую подсоединенного маршрутизатора с IP-адресом 130.10.64.2. Временной интервал для прохождения пакета данных составил 4 мс.

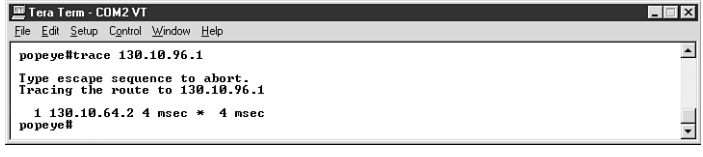


Рис. 18.7. Просмотр пути между двумя маршрутизаторами в сети

Обнаружение и устранение неисправностей протокола IPX

Если сеть сконфигурирована для протокола IPX, возможны те же проблемы, что и при работе с протоколом IP. Неправильно введенные сетевые номера IPX-интерфейсов маршрутизатора приводят к возникновению неполадок так же, как и ошибочные IP-адреса интерфейсов. Рассмотрим список неисправностей, наиболее часто встречающихся в сетях, которые работают с протоколом IPX:

- неверно сконфигурированные клиенты – поскольку сети Novell полностью ориентированы на сервер, для связи с сервером NetWare программное обеспечение клиента должно быть правильно сконфигурировано на всех рабочих станциях. Именно сервер идентифицирует каждого пользователя сети, по-

этому проверьте, одинаковы ли версии программного обеспечения клиента и сервера;

- слишком много клиентов – сервер NetWare устанавливается при помощи дискеты с определенным количеством лицензий, приобретенных для компьютеров-клиентов. Если число клиентов превысит количество лицензий, сервер откажет пользователю в доступе к сети. Чтобы проверить, сколько клиентов в настоящий момент работает в сети, пользуйтесь командой `load monitor` на сервере NetWare;
- проблемы с кадрами Ethernet – NetWare поддерживает несколько различных типов кадров, в частности Ethernet 802.2 и Ethernet 802.3. Если вы ошибочно присвоили интерфейсу LAN маршрутизатора тип кадра, который не соответствует кадрам, используемым хостами и серверами NetWare, у маршрутизатора возникнут затруднения при пересылке пакетов. Проверьте тип кадра при помощи команды `show ipx interface brief` (результат исполнения данной команды для маршрутизатора 2505 показан на рис. 18.8).

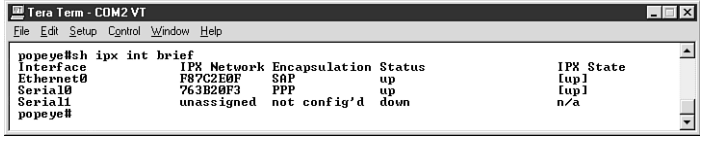


Рис. 18.8. Проверка типа кадра интерфейсов, для которых была задействована IPX-маршрутизация

Итак, при сбоях в работе маршрутизатора вам в первую очередь нужно проверить конфигурацию и установки интерфейсов. Другие проблемы могут быть вызваны неисправностями в аппаратных средствах и кабелях. Поскольку протокол IPX обычно задействуется для сетей LAN, перед подключением такой сети к маршрутизатору убедитесь в том, что она работает. Если потом возникнут неполадки, вы будете знать, что они вызваны неисправностью в маршрутизаторе, а не в сети.

Допустимо использовать расширенную команду `ping` для проверки узлов в сети (или интерфейсов маршрутизатора) при помощи их IPX-адреса, представленного в виде «сетевой номер.номер узла».

➢ IPX-адресация рассматривалась в главе 12, раздел «Конфигурирование IPX-маршрутизации».

Обнаружение и устранение неисправностей протокола AppleTalk

Сети AppleTalk LAN обычно невелики (по сравнению с сетями IP и IPX); в таких сетях проще устранять неполадки в кабелях и аппаратных средствах, поскольку

задействовано меньшее число компьютеров. Совсем иначе дело обстоит с ошибками в конфигурации и программном обеспечении.

Когда пользователи компьютеров Apple Macintosh ищут определенный ресурс в сети AppleTalk, они применяют встроенную программу Chooser (Селектор). Если конфигурация маршрутизатора не соответствует диапазонам кабеля и именам зон, которые заданы в подсоединенной сети AppleTalk, то при маршрутизации возникнут проблемы и пользователи не смогут найти запрошенные ресурсы.

Диапазоны кабеля задаются сетевым администратором, но вы должны помнить, что два сегмента сети LAN не могут быть сконфигурированы с одинаковыми сетевыми номерами или диапазонами кабеля (в противном случае маршрутизация будет затруднена).

> *Стек протоколов AppleTalk существует в двух версиях. Версия 1 не допускает использования диапазонов кабеля, а требует ввода единого сетевого адреса для сетевого сегмента. Если вы направите трафик через сеть AppleTalk, в которой применяются обе версии AppleTalk, при маршрутизации могут возникнуть проблемы. Рекомендуется усовершенствовать маршрутизаторы и другие устройства так, чтобы они поддерживали версию 2 стека протоколов AppleTalk.*

Для устранения неисправностей в сетях AppleTalk предназначены две команды – `ping` и `debug appletalk routing`. Напомним, что команда `ping` позволяет проверить, имеется ли соединение между маршрутизатором и узлом связи в сети, а также работает ли интерфейс маршрутизатора. Команда `debug` дает возможность просмотреть информацию о маршрутах в сети AppleTalk и сообщения о конфликтующих сетевых номерах.

Чтобы использовать команду `ping` для адресов AppleTalk, введите `ping appletalk [network number.node address]`. Например, нужно проверить соединение между вашим маршрутизатором и портом Ethernet 0 другого маршрутизатора, который сконфигурирован для протокола AppleTalk. Наберите `ping appletalk 12.176` (для протокола AppleTalk также разрешается применять расширенную команду `ping`) – рис. 18.9.

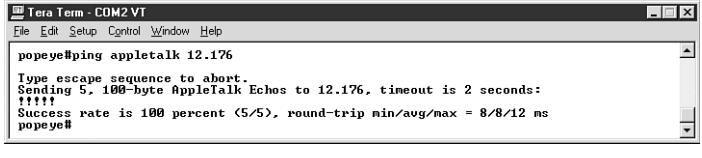


Рис. 18.9. Проверка состояния узла связи в сети AppleTalk

Команда привилегированного режима `debug` проста в работе, но требует значительных ресурсов маршрутизатора, например памяти, поэтому ее не стоит постоянно держать в активном режиме. Отключить ее можно с помощью команды `no debug all`, которая вводится так: `debug appletalk routing` (рис. 18.10).

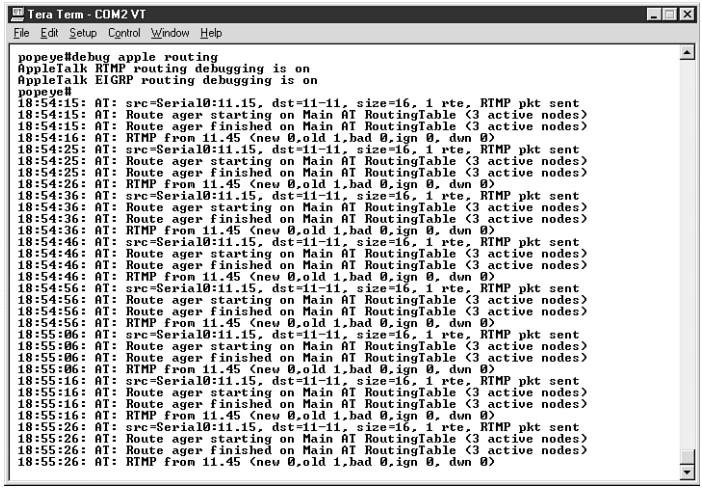


Рис. 18.10. Мониторинг обновлений информации о маршрутизации протокола AppleTalk

Резюме

В данной главе рассказывалось о некоторых основных способах устранения неисправностей аппаратных средств, сетевых архитектур (например, Ethernet) и сетевых протоколов (в частности, протокола IP), но пока не упоминалось о карте сети. Каждый сетевой администратор должен иметь постоянно обновляемую карту сети, где обозначена система адресации и местоположение таких устройств, как маршрутизаторы, соединения и серверы.

Сетевая карта (или сетевая диаграмма) используется для поиска адресов узлов, которые необходимо задать для команд `ping`, протокола Telnet и т.п. При помощи данной карты легко представить структуру сети, чтобы эффективно управлять ее работой.

Создать сетевую карту несложно. Существуют специальные программы (например, Visio Standard от компании Visio), упрощающие разработку сетевых диаграмм. В других версиях программы Visio, в частности Enterprise, имеется полный комплект пиктограмм, которые могут понадобиться для любого сетевого устройства. Эти значки на диаграмме будут понятны любому сетевому администратору.

Даже если вы не используете программу создания сетевых диаграмм, перенесите сетевую карту на компьютер посредством программы для работы с графическими изображениями: тогда при изменении структуры сети вы легко сможете скорректировать сетевую диаграмму. Она поможет вам, если возникнут проблемы с сетью.

ПРИЛОЖЕНИЕ 1

Сводные таблицы основных команд маршрутизатора

В данном приложении представлен перечень команд операционной системы Cisco IOS, которые описаны в книге. Команды разделены на несколько групп, каждой из которых посвящена отдельная таблица (команды в таблицах приведены в алфавитном порядке). Работать с данными таблицами следует лишь после того, как вы прочтете всю книгу: тогда несложно понять, для чего используется каждая команда.

Поскольку некоторые команды могут иметь различные применения – например, `show` служит для изучения работы маршрутизатора и для устранения неисправностей, – одна и та же команда будет встречаться в нескольких таблицах. Однако объединение по назначению упрощает поиск необходимой группы связанных между собой команд.

Например, чтобы найти команду операционной системы IOS для работы с протоколом IP или AppleTalk, удобно обратиться к определенной таблице, включающей команды для работы с протоколом IP или команды для работы с протоколом AppleTalk. Каждая команда вводится в строке соответствующего режима, после чего требуется нажать клавишу **Enter**.

Команды для проверки работы маршрутизатора

Эти команды дают возможность проверить состояние интерфейсов и другие параметры маршрутизатора (табл. П1.1). Если нет других указаний, команды используются в приглашении пользовательского или привилегированного режима.

Таблица П1.1. Команды для проверки работы маршрутизатора

Команда	Результат исполнения
`show CDP Neighbor`	Выводит список устройств, которые напрямую подключены к вашему маршрутизатору через сеть LAN или последовательное соединение
`show clock`	Показывает установки даты и времени на маршрутизаторе
`show flash`	Предоставляет информацию о файле IOS или файлах, которые содержатся в памяти Flash RAM маршрутизатора, а также об общем объеме памяти Flash RAM и объеме используемой памяти

Таблица П1.1. Команды для проверки работы маршрутизатора (окончание)

Команда	Результат исполнения
`show history`	Выдает список последних 10 команд
`show hub`	Показывает сведения о состоянии портов концентратора на маршрутизаторе 2505
`show interface ethernet [interface number]`	Сообщает о текущей конфигурации указанного интерфейса Ethernet
`show interface serial [interface number]`	Выводит текущую конфигурацию указанного интерфейса Serial
`show interfaces`	Представляет список всех интерфейсов маршрутизатора, их текущую конфигурацию и тип кадра; показывает, работает интерфейс или нет
`show processes`	Сообщает об использовании ресурсов процессора (CPU)
`show protocol`	Открывает список маршрутизирующих протоколов, сконфигурированных на маршрутизаторе
`show version`	Определяет версию операционной системы IOS, с которой работает маршрутизатор

Команды для работы с памятью маршрутизатора

Команды для работы с памятью маршрутизатора позволяют получить информацию, записанную в памяти NVRAM, в частности сведения о текущей или стартовой конфигурации. При помощи данных команд разрешается копировать и удалять файлы конфигурации из памяти маршрутизатора. В список включены команды для записи и считывания конфигурации маршрутизатора и файлов с версиями операционной системы IOS с сервера TFTP и на него. Если нет других указаний, команды вводятся в строке пользовательского или привилегированного режима (табл. П1.2).

Таблица П1.2. Команды для работы с памятью маршрутизатора

Команда	Результат исполнения
`copy flash tftp`	Команда привилегированного режима для копирования файла с версией операционной системы IOS из памяти Flash маршрутизатора на сервер TFTP
`copy running-config startup-config`	Команда для сохранения текущей конфигурации в памяти NVRAM маршрутизатора
`copy startup-config tftp`	Команда привилегированного режима для копирования стартовой конфигурации из памяти NVRAM на сервер TFTP
`copy tftp flash`	Команда привилегированного режима для копирования файла, содержащего версию IOS, с сервера TFTP в память Flash RAM маршрутизатора
`copy tftp startup-config`	Команда привилегированного режима, позволяющая переписать файл стартовой конфигурации с сервера TFTP в память NVRAM маршрутизатора

Таблица П1.2. Команды для работы с памятью маршрутизатора (окончание)

Команда	Результат исполнения
`erase startup-config`	Команда для удаления стартовой конфигурации из памяти NVRAM маршрутизатора
`show running-config`	Команда привилегированного режима, отображающая текущую конфигурацию в памяти RAM маршрутизатора
`show startup-config`	Команда привилегированного режима, которая показывает конфигурацию маршрутизатора, записанную в памяти NVRAM. После перезагрузки маршрутизатора эта конфигурация запускается автоматически

Команды для конфигурирования пароля и имени маршрутизатора

Приведенные команды служат для изменения различных паролей маршрутизатора, включая пароль для входа на маршрутизатор и секретный пароль для входа в привилегированный режим (табл. П1.3). В списке также содержится команда, с помощью которой можно изменить имя маршрутизатора. Все команды списка используются в режиме конфигурации.

Таблица П1.3. Команды для конфигурирования пароля и имени маршрутизатора

Команда	Результат исполнения
`enable secret password [password]`	Команда глобальной конфигурации, которая позволяет изменять пароль привилегированного режима маршрутизатора
`hostname [name]`	Команда глобальной конфигурации, определяющая имя маршрутизатора
`line console 0`	Команда, открывающая доступ в режим конфигурации консоли, чтобы ввести пароль для входа на маршрутизатор
`line vty 0 4`	Команда, позволяющая войти в режим конфигурации виртуального терминала, чтобы ввести его пароль
`password [password]`	Команда, используемая для ввода пароля: в режиме конфигурации консоли после исполнения команды `line console 0` и в режиме конфигурации виртуального терминала после команды `line vty 0 4`

➢ Как получить пароль, который вы забыли, рассказывалось в главе 8, раздел «Замена потерянного пароля».

Команды для конфигурирования интерфейса

Нижеприведенные команды предназначены для конфигурирования различных интерфейсов маршрутизатора (табл. П1.4). В список включена команда общей конфигурации `config` (команда привилегированного режима, которую нужно ввести для входа в режим конфигурации). Команды для конфигурирования интерфейсов, использующих определенный сетевой протокол или протокол WAN, представле-

ны в соответствующих таблицах (например, в таблице по командам для работы с протоколом WAN).

Таблица П1.4. Команды для конфигурирования интерфейса

Команда	Результат исполнения
`config`	Команда привилегированного режима, которая позволяет войти в режим глобальной конфигурации
Ctrl+Z	Хотя данная команда не является командой конфигурирования интерфейса, она используется для завершения сеанса конфигурирования маршрутизатора
`enable cdp`	Команда, выводящая список подсоединенных маршрутизаторов (вы должны быть в режиме конфигурации config-if, затем можно использовать команду `show cdp neighbor` маршрутизатора)
`encapsulation [encapsulation type]`	Специальная команда конфигурирования интерфейса, которая позволяет задать тип кадра для интерфейса LAN или Serial маршрутизатора
`interface ethernet [interface number]`	Команда глобальной конфигурации, которая дает возможность сконфигурировать параметры для указанного интерфейса Ethernet
`interface serial [interface number]`	Команда глобальной конфигурации, предназначенная для конфигурирования параметров указанного интерфейса Serial

Команды для работы с протоколом IP

Эти команды применяются для конфигурирования IP-адресации интерфейсов и включения IP-маршрутизации на маршрутизаторе. В табл. П1.5 представлены команды для работы с протоколами RIP и IGRP.

Таблица П1.5. Команды для работы с протоколом IP

Команда	Результат исполнения
`access-list [list #] permit` или `deny [ip address] [wildcard mask]`	Команда глобальной конфигурации для создания списка доступа протокола IP. Необходимо указать адрес сети или узла, доступ к которым будет разрешен или запрещен, а также обобщенную маску. Данная команда повторяется для каждой строки, которая появляется в списке доступа. Диапазон номеров списка (`list #`) для списков доступа протокола IP: 1–99
`debug ip igrp transaction`	Команда привилегированного режима, которая позволяет просмотреть статистику сообщений протокола IGRP маршрутизатора
`debug ip rip`	Команда привилегированного режима, которая выводит сообщения протокола RIP, отправленные и полученные маршрутизатором
`ip access-group [list number] out` или `in`	Команда конфигурации интерфейса, с помощью которой интерфейсу можно задать список доступа протокола IP. Параметр `out` или `in` используется для того, чтобы сообщить, какой трафик фильтровать: идущий на указанный интерфейс (`in`) или от него (`out`)

Таблица П1.5. Команды для работы с протоколом IP (окончание)

Команда	Результат исполнения
`ip address [ip address] [subnet mask]`	Команда используется в режиме config-if для присвоения адреса IP интерфейсу маршрутизатора. Команда `ip address` сопровождается IP-адресом (`ip address`) и маской подсети (`subnet mask`), назначенными для интерфейса
`ip routing`	Команда глобальной конфигурации, которая позволяет маршрутизатору работать с IP-маршрутизацией
`ip unnumbered [interface` или `logical interface]`	Эта команда режима config-if дает возможность назначить последовательный интерфейс без IP-адреса. Параметр `[interface` или `logical interface]` определяет интерфейс маршрутизатора (например, порт Ethernet), который имеет IP-адрес
`network [major network number]`	Команда используется вместе с командами `router zip` и `router igrp` для того, чтобы обозначить, к каким сетям IP напрямую подсоединен маршрутизатор
`no debug all`	Команда привилегированного режима, используемая для выключения режима отладки
`no ip routing`	Команда глобальной конфигурации, которая запрещает IP-маршрутизацию для маршрутизатора
`router igrp [autonomous system number]`	Команда глобальной конфигурации, которая разрешает маршрутизацию протокола IGRP. Параметр `autonomous system number` – это номер автономной системы для домена маршрутизации, к которому относится маршрутизатор (если такая система существует)
`router rip`	Команда глобальной конфигурации, которая включает маршрутизацию протокола RIP
`show access – list [list number]`	Команда, позволяющая просмотреть указанный список доступа. Параметр `[list number]` – это номер, который вы присвоили списку доступа при создании
`show ip interface [interface type and number]`	Команда, с помощью которой можно увидеть конфигурацию протокола IP для определенного интерфейса маршрутизатора
`show ip protocol`	Команда, предоставляющая сведения о пакетах маршрутизирующего протокола, которые были отправлены и получены маршрутизатором (например, рассылки протокола RIP)
`show up route`	Команда, показывающая таблицу маршрутизации протокола RIP или IGRP
`telnet [ip address]`	Команда пользовательского и привилегированного режима, которая позволяет войти на сервер через удаленный доступ

Команды для работы с протоколом IPX

Эти команды используются для конфигурирования IPX-адресации интерфейсов и включения IPX-маршрутизации (табл. П1.6 – команды для работы с протоколом IPX RIP).

Таблица П1.6. Команды для работы с протоколом IPX

Команда	Результат исполнения
`access list [list #] permit` или `deny [source network address] [destination network address]`	Команда глобальной конфигурации, с помощью которой создаются списки доступа протокола IPX с номерами от 800 до 899
`access-list [list #] permit` или `deny 1 1`	Команда вводится при формировании списка доступа протокола IPX. Она позволяет разрешить или запретить доступ ко всем сетям и узлам, которые не указаны в других строках списка
`debug ipx routing activity`	Команда привилегированного режима, которая дает возможность просмотреть пакеты протокола IPX RIP, полученные и отправленные маршрутизатором
`ipx access-group [list #] in` или `out`	Команда режима конфигурации config-if, которая позволяет задать список доступа протокола IPX для интерфейса маршрутизатора. Требуется указать, какие пакеты должны фильтроваться: приходящие на маршрутизатор (`in`) или уходящие с него (`out`)
`ipx network [network number] encapsulation [frame type]`	Команда конфигурации интерфейса (режима config-if), предназначенная для определения сетевого адреса IPX интерфейса Ethernet маршрутизатора. Кроме того, с помощью данной команды разрешается задавать интерфейсу тип кадра Ethernet
`ipx routing`	Команда глобальной конфигурации, которая позволяет маршрутизатору работать с IPX-маршрутизацией
`no debug ipx routing activity`	Команда, отключающая режим отладки протокола IPX
`show access-list [list #]`	Команда, которая служит для просмотра списка доступа протокола IPX или списка другого типа
`show ipx interface`	Команда пользовательского и привилегированного режимов, разрешающая просмотреть список интерфейсов маршрутизаторов, которые работают с маршрутизацией IPX
`show ipx route`	Команда, выводящая таблицу маршрутизации протокола IPX маршрутизатора
`show ipx traffic`	Команда, информирующая о полученных и отправленных пакетах IPX

Команды для работы с протоколом AppleTalk

Нижеприведенные команды используются при конфигурировании протокола AppleTalk и просмотра конфигурации AppleTalk (табл. П1.7).

Таблица П1.7. Команды для работы с протоколом AppleTalk

Команда	Результат исполнения
`access-list [list #] deny` или `permit zone [zone name]`	Команда общей конфигурации, которая позволяет вносить строки в список доступа на основании названий зон. Списки доступа протокола AppleTalk имеют диапазон номеров от 600 до 690

Таблица П1.7. Команды для работы с протоколом AppleTalk (окончание)

Команда	Результат исполнения
`access-list [list #] deny` или `permit cable range [cable range]`	Команда глобальной конфигурации, предназначенная для создания списка доступа протокола AppleTalk
`appletalk access-group [list #]`	Команда режима config-if, которая прикрепляет список доступа протокола AppleTalk к указанному интерфейсу маршрутизатора
`appletalk cable-range [cable-range number]`	Команда конфигурации интерфейса, с помощью которой задается диапазон кабеля протокола AppleTalk для указанного интерфейса
`appletalk routing`	Команда глобальной конфигурации, которая задействует AppleTalk-маршрутизацию
`appletalk zone [zone name]`	Команда конфигурации интерфейса, позволяющая назначать имя зоны AppleTalk для определенного интерфейса
`show appletalk global`	Команда, которая предоставляет информацию о количестве сетей и зон, доступных в сети, а также о временных интервалах для запросов протокола ZIP и рассылок протокола RTMP
`show appletalk interface`	Команда, сообщающая об интерфейсах маршрутизатора и их конфигурации для работы с протоколом AppleTalk
`show appletalk interface brief`	Команда, выводящая сведения об интерфейсах маршрутизатора и их конфигурации для работы с протоколом AppleTalk
`show appletalk interface e0`	Команда, с помощью которой можно получить данные о конфигурации AppleTalk для указанного интерфейса маршрутизатора
`show appletalk zone`	Команда, информирующая о зоне и сети для любой доступной зоны

Команды для работы с протоколами WAN

Данные команды применяются при конфигурировании протоколов WAN для последовательных интерфейсов маршрутизатора (табл. П1.8). В список включена команда для конфигурирования протоколов Frame-Relay и X.25 на маршрутизаторе.

Таблица П1.8. Команды для работы с протоколами WAN

Команды	Результат исполнения
`bandwidth [bandwidth]`	Команда режима config-if для определения пропускной способности интерфейса Serial
`clock rate [clock rate]`	Команда режима config-if для установки счетчика времени интерфейса Serial в том случае, если маршрутизатор используется как устройство DCE
`encapsulation [WAN protocol]`	Команда режима config-if для задания типа кадра WAN интерфейса Serial (например, PPP, HDLC и т.д.)
`frame-relay interface-dlci [dlci #]`	Команда режима config-if, позволяющая ввести номер DLCI на интерфейсе, который сконфигурирован для работы с протоколом Frame-Relay

Таблица П1.8. Команды для работы с протоколами WAN (окончание)

Команды	Результат исполнения
`frame-relay lmi-type [LMI type]`	Команда режима config-if, которая задает тип LMI для интерфейса, сконфигурированного под протокол Frame-Relay
`isdn spid [spid channel designation] [SPID #]`	Команда глобальной конфигурации, с помощью которой вводится уникальный номер SPID для каждого канала ISDN
`isdn switch type basic-[switch identifier]`	Команда глобальной конфигурации, определяющая тип коммутатора ISDN, к которому подключен маршрутизатор
`show frame-relay lmi`	Команда, выводящая статистику ошибок соединения Frame-Relay маршрутизатора
`show frame-relay map`	Команда, отображающая схему распределения DLCI на интерфейсах маршрутизатора
`x25 address [data link address]`	Команда режима config-if, которая используется для ввода адреса передачи данных протокола X.25, если этот протокол задан в качестве типа инкапсуляции
`X25 ips [bits]`	Команда режима config-if, предназначенная для указания размера входящего пакета для интерфейса X.25
`x25 ops [bits]`	Команда режима config-if, определяющая размер исходящего пакета для интерфейса X.25
`x25 win [number of packets]`	Команда режима config-if, которая применяется для задания размера входящего окна интерфейса X.25
`x25 wout [number of packets]`	Команда режима config-if, указывающая размер исходящего окна интерфейса X.25

Команды для устранения неисправностей

Представленные команды служат для устранения неполадок на маршрутизаторе (табл. П1.9). В список включены команды `ping` и `trace`.

Таблица П1.9. Команды для устранения неисправностей

Команды	Результат исполнения
`ping [node address]`	Команда, используемая для проверки соединения между двумя маршрутизаторами (команда ping, за которой следует IP-адрес или адрес узла в формате протокола AppleTalk либо IPX), а также между узлами в сети
`show controller`	Команда, позволяющая оценить состояние контроллеров интерфейсов маршрутизатора
`show interface [interface type] [interface number]`	Команда, которая дает возможность просмотреть все параметры, относящиеся к указанному интерфейсу маршрутизатора
`show stacks`	Команда, сообщающая об ошибках, которые были записаны в памяти маршрутизатора в момент перезагрузки
`trace [ip address]`	Команда, показывающая путь между маршрутизатором и другим маршрутизатором или узлом в сети. Также используется с адресами протокола AppleTalk

Дополнительные команды

В табл. П1.10 содержатся некоторые дополнительные команды, например команда создания баннера и команда установки времени и даты для маршрутизатора.

Таблица П1.10. Дополнительные команды операционной системы IOS

Команды	Результат исполнения
`banner motd [banner end character]`	Команда глобальной конфигурации, которая позволяет создать баннер при входе на маршрутизатор. Последний знак при вводе баннера может быть любым (кроме цифры); он свидетельствует о том, что ввод текста баннера окончен
Ctrl+Z	Хотя это не команда конфигурирования интерфейса, она используется для завершения сеанса конфигурирования маршрутизатора
`disable`	Команда выхода из привилегированного режима и возврата в пользовательский режим
`enable`	Команда входа в привилегированный режим. Чтобы войти в него, вам, возможно, придется ввести пароль
`quit`	Команда пользовательского и привилегированного режима, которая дает возможность завершить сеанс работы с маршрутизатором
`reload`	Команда привилегированного режима, предназначенная для перезагрузки маршрутизатора
`set clock`	Команда привилегированного режима, которая позволяет устанавливать время и дату на маршрутизаторе

ПРИЛОЖЕНИЕ 2

Спецификации различных серий маршрутизаторов Cisco

Выбор маршрутизатора

При разработке любой крупной сети (или небольшой сети, являющейся ее частью) необходимо учитывать, что аппаратные средства, которые войдут в будущую сеть, должны не только выполнять свои функции, но и иметь способность к усовершенствованию и расширению возможностей на случай увеличения сети или изменения ее структуры. Такая способность стала важнейшим фактором, определяющим выбор задействованных аппаратных средств. Поэтому маршрутизаторы должны не только решать свои текущие задачи, но и обеспечивать перспективу потенциального улучшения или изменения оборудования без полной перестройки сети.

Компания Cisco производит различные сетевые устройства (маршрутизаторы, коммутаторы, сетевые коммутаторы и т.д.) – их слишком много, чтобы мы смогли рассказать обо всех. Ниже рассматриваются маршрутизаторы Cisco, использующиеся для обслуживания небольших и средних сетей. На рис. П2.1 показана диаграмма сети, которая состоит из нескольких существующих в действительности сетей целого ряда компаний и одного муниципалитета. В данном приложении приводится краткое описание каждого типа маршрутизаторов, используемых для обслуживания такой сети.

Маршрутизаторы серии Cisco 7500

Серия Cisco 7500 – это маршрутизаторы нового поколения, которые обычно служат в качестве *пограничных*, или *корневых*, и обеспечивают пересылку пакетов данных между маршрутными доменами. Маршрутизатор 7513 (см. рис. П2.1) играет роль пограничного между корпоративной сетью и сетью Internet (обратите внимание, что между ними установлена защитная система).

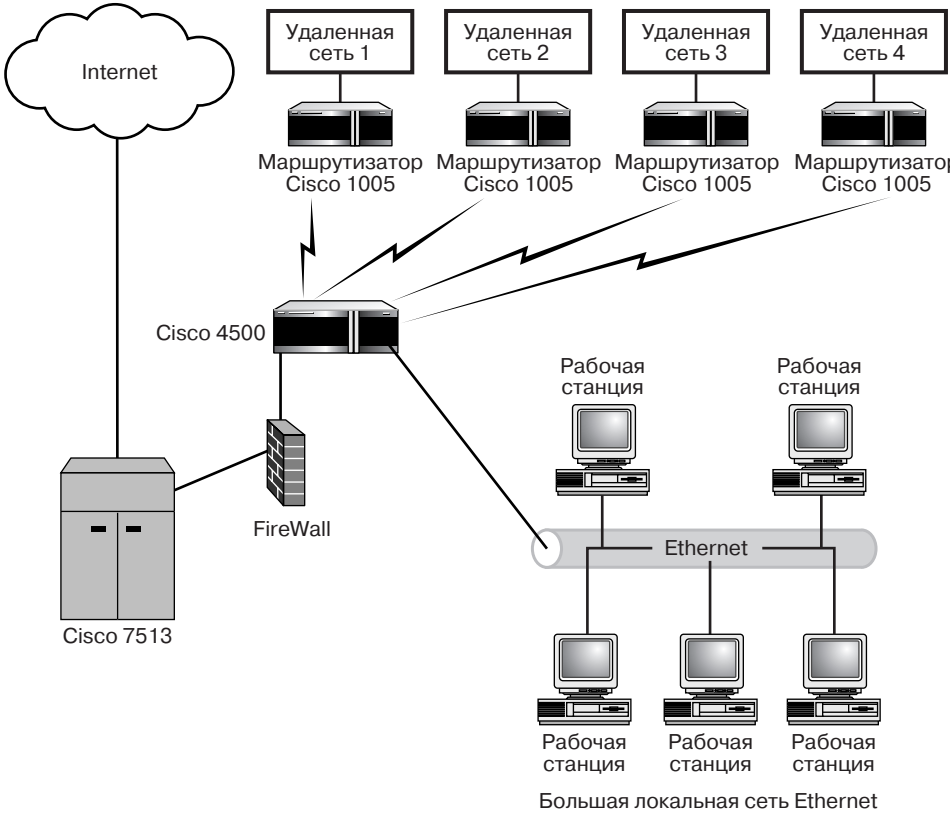


Рис. П2.1. Для обеспечения связи между сетями LAN используются маршрутизаторы Cisco различных типов

Маршрутизатор 7513 производится с 11 слотами, причем слоты устроены таким образом, что вы можете снимать и устанавливать интерфейсные карты непосредственно во время работы устройства. Данный маршрутизатор оснащается различными интерфейсами, включая Ethernet, Fast Ethernet, Token Ring, FDDI, T-1, Synchronous serial и первичный интерфейс ISDN. Он также может быть сконфигурирован с двойным резервным источником питания и с двойным процессором. В табл. П2.1 показаны аппаратные возможности базового маршрутизатора 7513.

Таблица П2.1. Спецификации маршрутизатора Cisco 7513

Характеристика	Значение
Источники питания	Два
Память Flash RAM	В стандартной поставке 16 Мб, расширяется до 220 Мб
Стандартная память RAM	32 Мб, расширяется до 128 Мб
Количество слотов для интерфейсов	11

Таблица П2.1. Спецификации маршрутизатора Cisco 7513 (окончание)

Характеристика	Значение
Количество слотов для процессоров и тип процессора	Два слота, процессор MIPS RISC
Вес	30 кг

Маршрутизаторы серии Cisco 4500

Маршрутизаторы серии Cisco 4500 считаются устройствами уровня распределения трафика и применяются в центральных точках соединения для небольших сетей LAN и удаленных сайтов в сети. Обратите внимание, что на рис. П2.1 маршрутизатор этой серии используется в качестве центрального распределительного пункта для удаленных офисов (которые подсоединяются к нему посредством маршрутизаторов доступа) и центральной сети LAN (подключенной напрямую через интерфейс LAN).

Маршрутизаторы серии Cisco 4500 модульные, поэтому в их интерфейсные слоты легко устанавливать различные интерфейсные карты с разным количеством портов. Хотя их обычно относят к устройствам средней мощности, они способны работать со многими интерфейсными картами, поддерживая Ethernet, Fast Ethernet, Token Ring, FDDI, Serial, ISDN и другие интерфейсы.

Маршрутизаторы серии 4500, напротив, не функционируют с интерфейсными картами, которые можно переустанавливать при включенном маршрутизаторе, а также не поддерживают резервные источники питания (табл. П2.2).

Таблица П2.2. Спецификации маршрутизатора Cisco серии 4500

Характеристика	Значение
Источники питания	Один внутренний источник питания
Память Flash RAM	4 Мб в стандартной поставке, расширяется до 16 Мб
Стандартная память RAM	4 Мб, расширяется до 16 Мб
Количество слотов для интерфейсов	Три слота
Количество слотов для процессоров и тип процессора	Один слот, процессор 100 МГц IDT Orion RISC
Вес	5,6 кг

Мы указали в таблицах спецификаций вес маршрутизаторов, чтобы вы представили, насколько эти устройства различаются по размерам. Так, маршрутизатор серии 7513 весит около 30 кг, а маршрутизатор серии 2500 – всего 4 кг, поэтому его можно носить в руках, как ноутбук.

Маршрутизаторы серии Cisco 2500

Маршрутизаторы серии Cisco 2500 – это недорогие устройства уровня доступа. На рис. П2.2 показан маршрутизатор серии 2500, а в табл. П2.3 представлены его характеристики. Устройства этой серии оснащены большим числом портов, чем другие маршрутизаторы, обслуживающие филиалы компаний, например серия 1000. Они поддерживают синхронные и асинхронные последовательные интерфейсы, Ethernet, Token Ring и ISDN.

Таблица П2.3. Спецификации маршрутизатора Cisco 2505

Характеристика	Значение
Источники питания	Один внутренний источник питания
Память Flash RAM	8 Мб
Стандартная память RAM	4 Мб, расширяется до 16 Мб
Количество слотов для интерфейсов	Нет слотов. Два последовательных порта, один интерфейс Ethernet в виде восьмипортового сетевого коммутатора
Количество слотов для процессора и тип процессора	Процессор 20 Мгц 68030
Вес	4 кг

Рис. П2.2. Маршрутизатор серии 2500

Маршрутизаторы серии Cisco 1000

Маршрутизаторы серии Cisco 1000 – это небольшие устройства, предназначенные для связи удаленных сетей LAN и сети WAN (или общей сети). На рис. П2.1 показано, как маршрутизаторы Cisco 1005 используются удаленными сетями для соединения с маршрутизатором серии 4500 посредством последовательного интерфейса и протокола WAN. Поскольку основной задачей устройств серии 1000 является обеспечение доступа к сети, их часто называют маршрутизаторами класса доступа.

Маршрутизатор Cisco 1005 оснащается одним последовательным интерфейсом (с 60-контактным последовательным портом, который устанавливается на всех маршрутизаторах Cisco – см. рис. П2.3). Последовательный интерфейс поддерживает как синхронную, так и асинхронную связь, поэтому для взаимодействия с маршрутизатором серии 4500 могут использоваться различные протоколы WAN, включая PPP, Frame-Relay или HDLC.

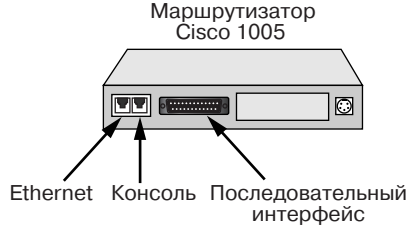


Рис. П2.3. Маршрутизатор Cisco 1005 поддерживает один интерфейс Ethernet и один последовательный интерфейс

Поскольку маршрутизатор Cisco 1005 предназначен для поддержки удаленной сети, он оснащен только одним портом Ethernet, который может быть подключен к сетевому коммутатору, соединенному с рабочими станциями Ethernet в сети (табл. П2.4).

Таблица П2.4. Спецификации маршрутизатора Cisco 1005

Характеристика	Значение
Источники питания	Один внешний источник питания
Память Flash RAM	Нет встроенной Flash RAM, слот PCMCIA предоставляет возможность установки карты Flash
Стандартная память RAM	8 Мб
Количество слотов для интерфейсов	Нет слотов. Два интерфейса
Количество слотов для процессора и тип процессора	Процессор MC68360
Вес	2,5 кг

Заключение

Хотя маршрутизаторы и различаются по мощности процессора и количеству поддерживаемых интерфейсов, у них есть общее свойство: все они работают с одной операционной системой – Cisco IOS. Следовательно, не так уж сложно сконфигурировать различные типы устройств, не пропустив ни одной важной детали. Все команды и установки практически одинаковы для всех маршрутизаторов, поэтому

достаточно изучить операционную систему, чтобы эффективно работать с любым числом сетевых устройств.

В заключение рекомендуем посетить Web-сайт компании Cisco, расположенный по адресу www.cisco.com. Там вы найдете не только спецификации по всей продукции компании Cisco, но и официальную документацию, руководства пользователя и даже бесплатное программное обеспечение, которое легко загрузить на свой компьютер. Хотя при первом посещении может показаться, что сайт довольно сложен для изучения, позже вы поймете, что там содержится колоссальное количество информации по сетевым технологиям.

Глоссарий

Автономная система (Autonomous System). При использовании маршрутизирующих протоколов, которые требуют от маршрутизаторов значительных ресурсов памяти и процессорного времени, сеть часто разделяют на домены маршрутизации. В сетях IP домен маршрутизации называется автономной системой. См. также *Пограничный маршрутизатор*.

Агенты (Agents). Особые программы, используемые протоколом SNMP для контроля работы сети. См. также *Протокол SNMP*.

Адаптер терминала (Terminal Adapter), или *модем ISDN*. Данное устройство используется при соединении узла, сконфигурированного для связи по ISDN, и телефонной системы. См. также *Сеть ISDN*.

Алгоритмы маршрутизации по вектору расстояния (Distance-Vector Routing Algorithms). Алгоритмы динамической маршрутизации, с помощью которых маршрутизатор отправляет всю таблицу маршрутизации соседним маршрутизаторам (с которыми установлено прямое соединение). При этом создается система обновлений, реагирующая на любое изменение в сети.

Аппаратные адреса MAC (Addresses Media Access Control). Адреса MAC указаны на чипах ROM сетевых интерфейсных карт. Каждый адрес MAC уникален.

Архитектура Ethernet. Наиболее распространенная сетевая архитектура. Ethernet обеспечивает доступ к сети посредством методики CSMA/CD (множественный доступ с контролем несущей и обнаружением конфликтов).

Архитектура Token Ring. Созданная компанией IBM сетевая архитектура, которая представляет собой логическое кольцо и использует методику передачи маркера для доступа к среде передачи. Архитектура Token Ring функционирует на скорости 4 или 16 Мбит/с. Компания IBM разрабатывает и поддерживает сети LAN на основе архитектуры Token Ring.

Асинхронная связь (Asynchronous Communication). Последовательные соединения для передачи данных. При проверке доставки сообщений устройству-получателю эти соединения применяют начальные и конечные биты.

Баннер (Banner). Сообщение, которое появляется на экране при входе на маршрутизатор с консоли или виртуального терминала.

Безопасность общих ресурсов (Share-level Security). Используется в сетях с непосредственным доступом. Для доступа к любому общему ресурсу требуется ввести пароль. См. также *Сеть с непосредственным доступом*.

Бесперебойный источник питания (Uninterruptible Power Supply – UPS). Устройство, которое предоставляет электроэнергию батареи другому устройству, например маршрутизатору, в случае прекращения подачи питания.

Биты высших разрядов (High-Order Bits). Первые четыре бита любого октета IP-адреса (слева направо).

Биты низших разрядов (Lower-Order Bits). Последние четыре бита любого октета IP-адреса (справа налево).

Ближайший сосед вверх по кольцу (NeArest Upstream Neighbor – NAUN). В сети Token Ring компьютер, который отправляет маркер следующему компьютеру в логическом кольце.

Ближайший сосед вниз по кольцу (NeArest Downstream Neighbor – NADN). В сети Token Ring ближайшим соседом будет рабочий узел, расположенный вниз по кольцу от данного узла. См. также *Ближайший сосед вверх по кольцу*.

Виртуальные загружаемые модули (Virtual Loadable Modules Netware – VLMs). Программные модули, которые создают и поддерживают сетевые сеансы между клиентом и сервером в сети IPX/SPX.

Виртуальный интерфейс (Virtual Interface). См. *Логический интерфейс*.

Виртуальный канал (Virtual Circuit). Маршрут, установленный через облако WAN таким образом, что все пакеты данных перемещаются по назначению вдоль одного пути. Применение виртуальных линий связи в сетях с коммутацией пакетов данных позволяет увеличить скорость передачи информации.

Виртуальный терминал (Virtual Terminal). Компьютер или маршрутизатор, который использует протокол Telnet для доступа к другому маршрутизатору.

Вольтметр (Voltmeter). Устройство, которое может быть присоединено к кабелю для тестирования на короткое замыкание или обрыв.

Выделенные линии (Leased Lines). Выделенные телефонные линии для постоянного соединения между сетями через сеть PSTN или другого провайдера. Обычно выделенные линии являются цифровыми.

Глобальные команды (Global Commands). Команды конфигурации, которые записываются в одну строку и влияют на настройку маршрутизатора в целом, например hostname и enable secret.

Датаграммы (Datagrams), или *пакеты*. Информация в виде потока битов.

Диапазон кабеля (Cable Range). Обозначение сегмента в сети AppleTalk, которое задается сетевым администратором. Диапазон кабеля может состоять из одного

номера, указывающего на наличие одной сети на сетевом кабеле, или нескольких номеров, определяющих количество таких сетей.

Динамические алгоритмы (Dynamic Algorithms). Таблицы маршрутизации, которые динамически создаются маршрутизирующим протоколом.

Домен NT (NT Domain). Сеть, обслуживаемая сервером NT – первичным контроллером домена (Primary Domain Controller).

Задержка (Delay). Временной интервал, в течение которого пакет доставляется от интерфейса отправителя в точку назначения. Измеряется в миллисекундах.

Запрос на передачу данных (Data Link Broadcast). Запрос, который использует протокол CDP, чтобы обнаружить работающие с протоколом CDP соседние маршрутизаторы Cisco. См. также *Протокол CDP*.

Запрос на прерывание (Interrupt ReQuest – IRQ). Уникальный запрос, который позволяет сообщить процессору компьютера, что устройство, использующее данный IRQ, требует ресурсов процессора.

Запрос протокола AARP (AARP Broadcast). Отправляется всем станциям в сети AppleTalk для сопоставления аппаратных адресов и логических адресов пакетов.

Зона (Zone). Логическая группа различных сегментов сети AppleTalk (аналогично рабочим группам в сетях с непосредственным доступом компании Microsoft).

Идентификационный номер передачи данных (Data Link Connection Identifier – DLCI). Число, которое применяется для контроля доставки пакетов, отправленных через коммутируемую сеть (например, сеть Frame-Relay). Такая проверка производится путем сопоставления логических адресов (например, IP-адресов) маршрутизатора-отправителя и маршрутизатора-получателя и номера DLCI виртуальной линии, которая используется для связи. См. также *Протокол Frame-Relay*.

Идентификационный номер ресурса (Service Profile Identifier – SPID). Номер, предназначенный для идентификации канала ISDN относительно коммутатора, который соединяется с устройством ISDN телефонной системы. Каждый канал должен иметь свой идентификационный номер.

Инкапсуляция (Encapsulation). Особая оболочка для данных с заголовком протокола. Например, сообщения Ethernet заключаются в оболочку с заголовком Ethernet перед тем, как отправиться по назначению.

Интерпретатор Exec (Exec). Операционная система Cisco IOS задействует интерпретатор для исполнения команд (он преобразует команду в нужный формат, а затем запускает ее). Пользовательский и привилегированный режимы считаются различными уровнями интерпретатора Exec.

Интерфейс (Interface), или *порт*. Физическое соединение между маршрутизатором и сетью определенного типа.

Интерфейс LAN (LAN Interface). Интерфейс маршрутизатора, который предоставляет порт для подсоединения определенной архитектуры LAN, такой как Ethernet или Token Ring.

Интерфейс LMI (Local Management Interface). Стандарт сигналов, применяемый между маршрутизатором и коммутатором Frame-Relay. Маршрутизаторы Cisco поддерживают три типа интерфейсов LMI: Cisco, ansi и q933a.

Интерфейс WAN (WAN Interface). Последовательный или специальный интерфейс, например ISDN, используемый для обеспечения WAN-соединений. См. также *Последовательный интерфейс*.

Интерфейс без IP-адреса (IP Unnumbered). Последовательный интерфейс маршрутизатора, который был сконфигурирован без IP-адреса (при этом такой интерфейс также участвует в маршрутизации пакетов IP).

Интерфейс для передачи данных по оптоволоконному кабелю (Fiber Distributed Data Interface). Соединение, работающее посредством высокоскоростных каналов для связи между различными сетями. Интерфейс FDDI использует оптоволоконный кабель, который укладывается в виде кольца. В качестве методики доступа применяется передача маркера, скорость передачи данных не менее 100 Мбит/с.

Интерфейс командной строки (Command-Line Interface – CLI). Интерфейс операционной системы Cisco IOS на консоли маршрутизатора или виртуальном терминале, который позволяет вводить команды операционной системы IOS.

Кампусная сеть (Campus). Объединенная сеть, состоящая из нескольких сетей LAN. См. также *Сеть*.

Класс A (Class A). Крупные сети IP, которые поддерживают свыше 16 млн адресов узлов.

Класс B (Class B). Средние сети IP, которые поддерживают свыше 65 тыс. адресов узлов.

Класс C (Class C). Небольшие сети IP, которые поддерживают 254 адреса узлов.

Класс D (Class D). Класс сетей IP, сетевые адреса которых применяются различными группами пользователей для получения данных от определенного приложения или сервера. Примером может служить сеть Microsoft NetShow, которая способна посылать одну и ту же информацию одновременно большому числу пользователей.

Класс E (Class E). IP-адреса экспериментального класса, недоступные для общего использования.

Клиенты (Clients). Компьютеры в сети, которые могут задействовать ресурсы (принтеры и файлы), предоставляемые сервером.

Кольцевой интерфейс (Loopback Interface). Программный интерфейс, который эмулирует физический порт и используется для сохранения трафика данных, предназначенного для вышедшего из строя аппаратного устройства. См. также *Логический интерфейс*.

Команды для работы с портами (Port Commands). Ряд команд, с помощью которых можно указать определенный интерфейс или контроллер для конфигурирования; за ними должны следовать подкоманды, предоставляющие дополнительную информацию по конфигурации. См. также *Подкоманды*.

Коммутаторы (Switches). Сетевые устройства канального уровня модели OSI, которые служат для сохранения или увеличения пропускной способности сети посредством сегментации. Они применяются для передачи пакетов по указанному адресу с помощью аппаратных адресов MAC (аналогично мостам). Поскольку коммутаторы основаны на аппаратных, а не на программных средствах, они передают пакеты данных быстрее, чем мосты.

Коммутация (Switching). Пересылка пакетов на маршрутизаторе от входящего интерфейса к исходящему.

Коммутация каналов (Circuit Switching). Методика, при которой между отправителем и получателем устанавливается особое соединение. Данные перемещаются через канал (линию), который был выделен специально для данного сеанса связи[1].

Коммутация пакетов (Packet Switching). Сетевая методика, при которой данные в виде потока битов разделяются на пакеты. Каждый пакет использует собственную служебную информацию и коммутируется по сети независимо от других пакетов.

Консоль маршрутизатора (Router Console). Компьютер, функционирующий как терминал для маршрутизатора. Применяется для просмотра и ввода параметров конфигурации маршрутизатора.

Консольный кабель (Roll-Over Cable). Кабель для соединения консоли компьютера и маршрутизатора.

Концентратор (Hub). Центральное коммутационное устройство, работающее на физическом уровне модели OSI, к которому подключаются компьютеры в сети; чаще всего используется в топологии «звезда».

Критический ресурс (Bottleneck), или *узкое место*. Устройство, замедляющее трафик в сети.

Линия DDS (Digital Data Service). Выделенные цифровые линии, использующиеся для пересылки информации. Включают систему Т-несущей, которая обеспечивает поддержку различных линий и скоростей передачи данных.

---

[1] Примером сети с коммутацией каналов служит обычная телефонная сеть. – *Прим. научн. ред.*

Логический, или *виртуальный*, *интерфейс* (Logical Interface). Программный интерфейс, который создается средствами операционной системы IOS маршрутизатора. См. также *Кольцевой интерфейс*, *Нулевой интерфейс* и *Туннельный интерфейс*.

Логическое умножение (Anding). Операция, производимая маршрутизатором (наравне с сопоставлением IP-адреса и маски подсети) для вычисления сетевого адреса.

Локальная сеть (Local Area Network – LAN). Компьютерная сеть, которая ограничена небольшой локальной территорией, например пределами одного здания.

Маршрутизатор (Router). Устройство, работающее на сетевом уровне модели OSI и используемое для связи сетей LAN через соединения LAN и WAN. Маршрутизатор применяет комбинацию аппаратных средств и программного обеспечения для пересылки пакетов между сетями (маршрутизаторы Cisco работают под управлением операционной системы Cisco IOS).

Маска подсети (Subnet Mask). Набор из 32 бит, сгруппированных в четыре октета. С его помощью можно определить, какие биты IP-адреса составляют сетевой адрес, какие – адрес подсети и какие – адрес узла.

Международные номера данных (International Data Numbers). См. *Схема адресации X.121*.

Методика предостережений (Beaconing). Особая методика борьбы с неполадками архитектуры Token Ring, на основе которой узлы в кольце определяют состояние сети при неисправности кабеля или сбое в работе соседнего узла.

Метрика (Metric). Методика, используемая алгоритмами маршрутизации для выявления наилучшего пути передачи информации. В качестве метрики могут применяться различные факторы: длина пути, стоимость отправления пакетов по определенному маршруту или надежность пути между отправителем и получателем.

Множественный доступ с контролем несущей и обнаружением конфликтов (Carrier Sense Multiple Access with Collision Detection – CSMA/CD). Методика доступа к среде передачи в сетях Ethernet. Если узел, отправляющий данные, обнаружит конфликт, он отправит сообщение повторно, когда в линии не будет сигнала.

Множественный доступ с контролем несущей и предупреждением конфликтов (Carrier Sense Multiple Access with Collision Avoidance – CSMA/CA). Методика доступа к среде передачи в сетях AppleTalk. Устройство, которое готово к отправке данных через сеть, предупредит об отправке все другие узлы в сети.

Модель DOD (DOD Model). В то время, когда разрабатывался стек протоколов TCP/IP, Министерство обороны создало собственную модель – модель DOD, или модель DARPA, показывающую, как функционируют различные протоколы стека TCP/IP.

Модель взаимодействия открытых систем OSI (Open Systems Interconnection Model). Концептуальная модель работы сетей, принятая в конце 70-х годов Международной организацией ISO. В 1984 году эта модель стала международным стандартом для сетевых соединений. Она предоставляет концептуальную схему, основанную на нескольких уровнях (стеках протоколов) и поясняющую, как данные перемещаются по сети.

Модем ISDN (ISDN Modem). См. *Адаптер терминала*.

Мосты (Bridges). Сетевые устройства, работающие на канальном уровне модели OSI. Используются для разделения больших сетей, когда высокий трафик в них начинает замедлять общую передачу информации.

Нагрузка (Load). Текущий трафик для определенного интерфейса. Нагрузка измеряется динамически и отображается в долях от числа 255 (255/255 считается максимальной нагрузкой).

Надежность (Reliability). Отношение ожидаемых сообщений о наличии связи к полученным. См. также *Сообщения о наличии связи*.

Нерасширенный сегмент (Nonextended Segment). Сегмент сети AppleTalk, которому присвоен только один сетевой номер.

Нулевой интерфейс (Null Interface). Программный интерфейс, который отбрасывает все пакеты данных при получении. См. также *Логический интерфейс*.

Область (Area). Часть сети, в состав которой входит несколько маршрутизаторов. Несколько областей можно объединить в более крупную область – домен маршрутизации.

Обобщенная маска (Wildcard Mask). Маска из 32 бит, которая используется вместе с IP-адресами для определения, какая часть IP-адреса будет игнорироваться предписаниями «отклонить» и «разрешить» в списке доступа.

Общая коммутируемая телефонная сеть (Public Switched Telephone Network – PSTN). Инфраструктура телефонной связи, поддерживаемая компанией Baby Bells.

Общая, или *частная*, *сеть* (Public Data Network or Private Data Network). Коммутируемая сеть, управляемая провайдером. Сети PDN обеспечивают соединения WAN между сетями LAN.

Оконечное оборудование канала передачи (Data Circuit Terminating Equipment – DCE). Оборудование, которое предоставляет информацию по временному интервалу, чтобы синхронизировать связь между оконечным оборудованием пользователя (DTE) и коммутируемой сетью. См. также *Оконечное оборудование пользователя*.

Оконечное оборудование пользователя (Digital Terminal Equipment – DTE). Устройство, которое соединяется с оконечным оборудованием провайдера (DCE) и обеспечивает связь с коммутируемой сетью. См. также *Оконечное оборудование канала передачи*.

Октет (Octet). Восемь бит информации; одна из четырех частей IP-адреса.

Организация международных стандартов (International Standards Organization – ISO). Организация, разрабатывающая стандарты для любой сферы деятельности, начиная от технических параметров сетей и заканчивая принципами ведения бизнеса на новом глобальном рынке. Данные стандарты определяют концептуальную сетевую модель OSI. См. также *Модель взаимодействия открытых систем OSI*.

Ослабление (Attenuation). Ослабление сигнала передачи данных при перемещении по кабелю.

Основной канал (Baseband). Способ связи, при котором для передачи потока битов используется полная пропускная способность носителя.

Память Flash RAM. Память, которую можно стирать и перепрограммировать. Используется для сохранения версии операционной системы Cisco IOS, с которой работает маршрутизатор. Здесь также можно хранить другие версии Cisco IOS (например, модифицированную), поэтому обновление операционной системы не составит труда.

Память NVRAM (Nonvolatile RAM). Память RAM, которая применяется для сохранения файла стартовой конфигурации маршрутизатора. Из памяти NVRAM разрешается удалить информацию или скопировать туда текущую конфигурацию маршрутизатора. При перезагрузке маршрутизатора данные в NVRAM не стираются.

Память RAM (Random Access Memory). Память RAM аналогично динамической памяти персональных компьютеров представляет собой временное хранилище информации (когда адресная информация пакетов данных проверяется маршрутизатором, сами пакеты находятся в памяти RAM) и содержит, в частности, текущую таблицу маршрутизации.

Память ROM (Read Only Memory). Чипы памяти, на которых записано программное обеспечение. Здесь хранится автоматический тест, проводимый при загрузке (POST), и программа загрузки для маршрутизатора.

Первые биты (Leading Bits). Первые три бита сетевого IP-адреса. Существуют определенные требования для первых битов первого октета каждого из трех классов сетей (A, B и C). В первом бите адресов сети класса A должны быть только нули; в адресах сети класса B первый бит первого октета равен единице, а второй – нулю; в адресах сетей класса C первые два бита первого октета – единицы, а третий бит – нуль.

Повторители (Repeaters). Устройства, которые берут полученный от сетевых устройств сигнал и повторяют его таким образом, что он проходит по сети дальше, чем было возможно изначально. Современные концентраторы, помимо ретрансляции полученного сигнала по всем своим интерфейсам, выполняют функции повторителей.

Пограничный, или *корневой*, *маршрутизатор* (Border Router). Многофункциональный маршрутизатор, который используется для связи между автономными системами.

Подкоманды (Subcommands). Команды, которые предоставляют особую информацию по конфигурации для указанного интерфейса или контроллера. См. также *Команды для работы с портами*.

Подуровень LLC (Logical Link Control). Подуровень канального уровня модели OSI, который создает и поддерживает связь между компьютером-отправителем и компьютером-получателем во время передачи данных.

Пользовательский режим (User Mode). Базовый уровень доступа маршрутизатора. Команды этого режима позволяют просмотреть конфигурацию маршрутизатора, но не дают возможности изменить ее. См. также *Привилегированный режим* и *Режим конфигурации*.

Порт (Port). См. *Интерфейс*.

Последовательный интерфейс (Serial Interface). Адаптеры, или порты маршрутизатора, которые применяются в качестве интерфейсов для WAN-соединений. Сначала порт маршрутизатора подключается к кабелю, например V.35, а затем – к устройству WAN DCE. См. также *Оконечное оборудование канала передачи*.

Последовательные адаптеры (Serial Adapters). Адаптеры, которые поставляются в комплекте с маршрутизатором и используются для соединения консольного кабеля и COM-порта компьютера.

Предписания «отклонить» (Deny Statements). Директивы в списке доступа, которые запрещают трафик от определенных сетей или узлов связи для входящих или исходящих пакетов на интерфейсе маршрутизатора.

Предписания «разрешить» (Permit Statements). Директивы в списке доступа, которые разрешают трафику от определенных сетей или узлов связи входить на данный интерфейс или выходить с него.

Привилегированный режим (Privileged Mode). Уровень полного доступа к маршрутизатору, позволяющий просмотреть и изменить параметры конфигурации маршрутизатора или войти в режим конфигурации. См. также *Режим конфигурации*.

Пропускная способность (Bandwidth). Количество битов информации, которое носитель способен передать за 1 с.

Протокол (Protocol). Особая программа, определяющая, как сетевые компьютеры отправляют и получают данные.

Протокол AARP (AppleTalk Address Resolution Protocol). Протокол сетевого уровня модели OSI, который сопоставляет сетевые адреса AppleTalk и аппаратные адреса. Он запрашивает все станции в сети, чтобы найти соответствие между аппаратными и логическими адресами пакетов данных.

Протокол ARP (Address Resolution Protocol). Протокол стека TCP/IP, работающий на сетевом уровне и использующийся для сопоставления IP-адресов и аппаратных адресов узлов.

Протокол BGP (Border Gateway Protocol). Стандартный протокол EGP для сети Internet, обычно применяемый для маршрутизации вне доменов. Он обеспечивает пересылку данных между несколькими маршрутизаторами, которые служат пограничными для автономных систем.

Протокол CDP (Cisco Discovery Protocol). Протокол компании Cisco, предоставляющий доступ к информации на соседних маршрутизаторах. См. также *Соседи*.

Протокол DDP (Datagram Delivery Protocol). Протокол сетевого уровня AppleTalk, который обеспечивает доставку датаграмм (аналогично протоколу UDP стека TCP/IP).

Протокол EGP (Exterior Gateway Protocol). Маршрутизирующий протокол, который служит для передачи данных между доменами маршрутизации. См. также *Протокол BGP*.

Протокол Frame-Relay (Frame-Relay). WAN-протокол передачи данных, применяющий для связи между различными устройствами виртуальные линии, которые обозначаются при помощи идентификационного номера DLCI (его предоставляет провайдер Frame-Relay). См. также *Идентификационный номер передачи данных*.

Протокол FTP (File Transfer Protocol). Протокол-приложение стека TCP/IP, который обеспечивает передачу файлов между компьютерами.

Протокол HDLC (High Level Data Link Control). Синхронный WAN-протокол канального уровня модели OSI. Протокол HDLC, используемый маршрутизаторами Cisco, является собственностью компании Cisco.

Протокол ICMP (Internet Control Message Protocol). Протокол для обработки и контроля сообщений, который применяется маршрутизаторами при отправке сообщений хостам, посылающим данные для маршрутизации.

Протокол IGP (Interior Gateway Protocol). Маршрутизирующий протокол, который обеспечивает обмен пакетами внутри домена маршрутизации. Для каждого маршрутизатора внутри домена должны быть сконфигурированы такие протоколы IGP, как RIP или IGRP. См. также *Протокол RIP*, *Протокол IGRP* и *Протокол OSPF*.

Протокол IGRP (Interior Gateway Routing Protocol). Протокол маршрутизации по алгоритму вектора расстояния, разработанный компанией Cisco в 80-е годы. Он использует суммарную метрику, которая учитывает несколько переменных, и лишен некоторых недостатков протокола RIP, таких как метрика счетчика переходов и невозможность маршрутизации пакетов при наличии более 15 переходов.

Протокол IPX (Internet Package Exchange Protocol). Транспортный протокол, обеспечивающий систему адресации для стека IPX/SPX. Работая на сетевом

и транспортном уровнях модели OSI, он управляет движением пакетов по сети при помощи протокола маршрутизации IPX RIP.

Протокол IPX RIP (IPX Routing Information Protocol). Протокол маршрутизации для сетей IPX, применяющий две метрики: счетчик времени (1/18 с) и счетчик переходов.

Протокол NBP (Name Binding Protocol). Протокол транспортного уровня модели OSI, который сопоставляет адреса низших уровней и имена сети AppleTalk, идентифицирующие доступные сетевые ресурсы (в частности, принтер или сервер).

Протокол NCP (Netware Core Protocol). Протокол стека IPX/SPX, который выполняет сетевые функции на уровнях приложения, представления и сеансовом уровне модели OSI.

Протокол NetBEUI (NetBIOS Extended User Interface). Простой и быстрый сетевой протокол, предназначенный для работы с интерфейсом NetBIOS в небольших сетях Microsoft и IBM.

Протокол NLSP (NetWare Link Services Protocol). Созданный компанией NetWare протокол, который применяется в качестве сконфигурированного маршрутизирующего протокола для IPX-маршрутизации вместо IPX RIP.

Протокол OSPF (Open Shortest Path First). Альтернатива протоколу RIP. OSPF использует алгоритм нахождения кратчайшего пути, который позволяет вычислить самый короткий, быстрый и надежный путь от источника до пункта назначения при маршрутизации пакетов. См. также *Протокол IGP*.

Протокол PPP (Point-to-Point Protocol). Один из наиболее распространенных протоколов, обеспечивающих WAN-соединение для различных интерфейсов.

Протокол RIP (Routing Information Protocol). Маршрутизирующий протокол, работающий по алгоритму вектора расстояния и использующий в качестве метрики счетчик переходов. Он суммирует информацию в таблице маршрутизации при помощи адресов сетей IP (основных сетевых адресов).

Протокол RTMP (Routing Table Maintenance Protocol). Протокол транспортного уровня модели OSI, отвечающий за создание и поддержку таблиц маршрутизации для маршрутизаторов в сетях AppleTalk.

Протокол SAP (Service Advertisement Protocol). Протокол, который выдает информацию о доступных ресурсах в сети NetWare.

Протокол SMTP (Simple Mail Transport Protocol). Протокол уровня приложения стека TCP/IP, который обеспечивает пересылку почтовых сообщений между компьютерами.

Протокол SNMP (Simple Network Management Protocol). Протокол уровня приложения стека TCP/IP, служащий для мониторинга состояния сети. Работает

с программами-агентами, посылающими информацию по определенным параметрам сети.

Протокол SPX (Sequence Packet Exchange). Транспортный протокол стека IPX/SPX, который предоставляет протоколам высших уровней прямое соединение между отправителем и получателем.

Протокол TCP (Transport Control Protocol). Протокол, обеспечивающий виртуальную линию связи между программами-приложениями на компьютере-отправителе и компьютере-получателе в сети TCP/IP.

Протокол Telnet. Протокол эмуляции терминала (часть стека TCP/IP), который позволяет соединять локальный компьютер с удаленным или с другим устройством, например маршрутизатором.

Протокол TFTP (Trivial File Transfer Protocol). Сокращенная версия протокола FTP, предназначенная для пересылки файлов без аутентификации (ввода имени пользователя и пароля).

Протокол UDP (User Datagram Protocol). Транспортный протокол стека TCP/IP, который обеспечивает соединение между протоколами высших уровней модели OSI, не требующими синхронизации протокола TCP. См. также *Протокол TCP*.

Протокол ZIP (Zone Information Protocol). Протокол сетевого и транспортного уровней модели OSI, используемый для назначения логических сетевых адресов узлам в сети AppleTalk.

Протокол маршрутизации (Routing Protocol). Сетевой протокол, который обеспечивает работу протоколов сетевого уровня модели OSI для маршрутизации пакетов. Протоколы маршрутизации позволяют маршрутизатору создать таблицу маршрутизации и передать данные из этой таблицы другим устройствам.

Расширенный сегмент (Extended Segment). Сегмент сети AppleTalk, которому был назначен диапазон сетевых номеров.

Режим асинхронной передачи (Asynchronous Transfer Mode – ATM). Усовершенствованный протокол передачи пакетов данных, который работает с пакетами фиксированных размеров (53 байта) – ячейками – для увеличения пропускной способности при передаче данных. Обычно используется в высокоскоростных оптоволоконных сетях. См. также *Ячейки* и *Сеть SONET*.

Режим конфигурации (Configuration Mode). Режим маршрутизатора, который позволяет изменять конфигурацию маршрутизатора при помощи общих команд и команд для работы с интерфейсами.

Рефлектометр (Time Domain Reflectometer – TDR). Устройство, предназначенное для диагностики коротких замыканий и обрывов кабеля, а также для определения, в какой именно точке кабеля имеется неисправность.

Сервер (Server). Устройство, которое предоставляет компьютерам-клиентам сетевые ресурсы.

Сервер TFTP (TFTP Server). Компьютер, работающий с программным обеспечением TFTP и предназначенный для сохранения файлов конфигурации маршрутизатора и Cisco IOS. Допустимо копировать файлы с маршрутизатора на сервер TFTP и обратно.

Сетевая карта (Network Interface Card – NIC), или *сетевой адаптер*. Устройство, которое обеспечивает соединение между компьютером и физической средой сети. Интерфейс NIC переводит данные в биты.

Сетевая операционная система IOS (Internetworking Operating System). Операционная система, созданная компанией Cisco, которая предоставляет аппаратным средствам маршрутизатора возможность пересылать пакеты. IOS поддерживает набор команд и программное обеспечение для мониторинга и конфигурирования маршрутизатора.

Сетевая операционная система NOS (Network Operating System). Любое количество программ на основе сервера – Windows NT, Novell NetWare и AppleTalk, – которые поддерживают соединения LAN.

Сетевой номер IPX (IPX Network Number). Первая часть IPX-адреса, которая может включать до 16 шестнадцатеричных знаков (32 бита). Остальные 12 шестнадцатеричных знаков (48 бит) представляют собой адрес узла связи.

Сетевые системы компании Xerox (Xerox Network Systems – XNS). В 60-е годы группа ученых Исследовательского центра Xerox Palo Alto разработала сетевую операционную систему XNS. Протоколы системы Novell NetWare во многом основываются на стеке сетевых протоколов XNS.

Сеть (Network). Группа компьютеров и соответствующих аппаратных средств, объединенных между собой.

Сеть intranet. Корпоративная сеть, которая не является частью глобальной сети Internet, но использует такие протоколы Internet, как SMTP (для работы с почтовыми сообщениями), HTTP (для Web-браузеров) и др., для обмена информацией между корпоративными пользователями.

Сеть ISDN (Integrated Services Digital Network). Цифровая технология связи, которая функционирует поверх обычных телефонных линий. Модем ISDN служит для связи устройства и телефонной сети. Имеются две версии сети ISDN: сеть базовой скорости BRI ISDN и сеть высокой скорости PRI ISDN.

Сеть SONET (Synchronous Optical Network). Оптоволоконная сеть, разработанная Исследовательским центром Bell Communications. Обеспечивает голосовую связь, передачу данных и изображения на высокой скорости.

Сеть WAN (Wide Area Network). Несколько соединенных между собой сетей. Может охватывать большую по площади территорию.

Сеть с непосредственным доступом (Peer-to-Peer Network). Локальная сеть, которая работает без сервера, но предоставляет подключенным компьютерам доступ к общим ресурсам, таким как файлы и принтеры. Примером могут служить рабочие группы Microsoft.

Сеть с сервером (Server-Based Network). Сеть, где компьютеры-клиенты идентифицируются сервером, который поддерживает центральное хранилище для файлов и другие ресурсы, в частности принтеры.

Синхронная связь (Synchronous Communication). Последовательные соединения, использующие часовой механизм для расчета времени перемещения данных от компьютера-отправителя компьютеру-получателю.

Система LocalTalk. Система кабелей, применяемая для связи компьютеров Macintosh (защищенные двужильные кабели с особым адаптером Macintosh).

Соединение через модем (Dial-up Connection). Самое простое и дешевое соединение для передачи данных, которое задействует модем для связи между компьютерами или другими аналогичными устройствами через телефонную линию.

Сообщения о наличии связи (Keepalives). Сообщения, отправляемые сетевыми устройствами, чтобы проинформировать другие сетевые устройства о наличии связи.

Соседи (Neighbors). Маршрутизаторы, которые напрямую подсоединены к данному маршрутизатору через соединение LAN или WAN.

Список доступа (Access List). Список предписаний «разрешить» и «отклонить», которые помогают регулировать входящий и исходящий трафик на маршрутизаторе.

Статическая маршрутизация (Static Routing). Способ, при котором маршрутные таблицы создаются и изменяются сетевым администратором вручную.

Статические алгоритмы (Static Algorithms). Информация о структуре сети, которую сетевой администратор вводит в таблицу маршрутизации.

Стек протоколов AppleTalk. Разработанный компанией Apple стек сетевых протоколов, предоставляющий сетевую поддержку для компьютеров Apple Macintosh.

Стек протоколов DECnet. Стек сетевых протоколов, созданный компанией Digital Equipment Corporation.

Стек протоколов IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange – IPX/SPX). Стек сетевых протоколов компании NetWare для связи между сетями LAN; его протоколы, как и протоколы TCP/IP, не полностью накладываются на уровни модели OSI. Стек IPX/SPX получил широкое распростране-

ние в ранних локальных сетях Novell NetWare, поскольку обеспечивал высокую производительность и не требовал таких накладных расходов, как стек TCP/IP.

Стек протоколов TCP/IP (Transmission Control Protocol/Internet Protocol). Маршрутизируемый стек протоколов, который может функционировать на различных платформах (Windows, UNIX и т.д.) и принимается большинством сетевых операционных систем в качестве сетевого протокола по умолчанию.

Схема адресации X.121 (X.121), или *международные номера*. Соглашение об идентификации абонентов в телефонной сети, которая используется WAN-протоколом X.25. Номер в данной схеме включает от 1 до 14 десятичных цифр; он идентифицирует локальный X.121-адрес последовательного интерфейса и должен быть сконфигурирован для маршрутизатора, на котором задействована X.25-маршрутизация.

Сходимость (Convergence). Время, которое требуется всем маршрутизаторам в сети для того, чтобы учесть изменения в ее структуре. Чем дольше длится этот процесс, тем выше вероятность, что пакеты данных будут отправлены по недоступным маршрутам.

Счетчик времени (Clock Ticks). Метрика, используемая протоколом RIP стека IPX/SPX. За единицу отсчета принимается 1/18 с.

Счетчик переходов (Hop Count). Метрика протокола RIP (переход – это перемещение пакета от одного маршрутизатора к другому). См. также *Протокол RIP*.

Текущая конфигурация (Running Configuration). Конфигурация маршрутизатора, которая является текущей в памяти RAM.

Топология (Topology). Физическая структура сети. Она влияет, например, на используемый тип кабеля и собственно на архитектуру сети (такую, как «кольцо», «шина» или «звезда»).

Топология «звезда» (Star Topology). Топология сети, в которой все компьютеры подсоединяются через отдельные кабели к центральному сетевому концентратору.

Топология «кольцо» (Ring Topology). Компьютеры и другие узлы последовательно подключаются к проводу в виде кольца. В таком случае каждый узел, получив информацию, пересылает ее следующему узлу по кольцу.

Топология «петля» (Mesh Topology). Структура сети, в которой устройства используют резервные соединения для предотвращения неисправностей в среде передачи. Сети с такой топологией также называются полносвязными.

Топология «шина» (Bus Topology). Структура сети, характеризующаяся наличием единого сетевого кабеля, к которому через определенные интервалы подключаются сетевые компьютеры.

Точка доступа к ресурсу (Service Access Point – SAP). Подуровень LLC канального уровня модели OSI создает такие точки для того, чтобы компьютер-отправи-

тель мог соединяться с протоколами высших уровней модели OSI на узле-получателе.

Туннельный интерфейс (Tunnel Interface). Логический интерфейс, используемый для перемещения пакетов данных определенного типа сетевой архитектуры через соединение, не поддерживающее данные пакеты. См. также *Логический интерфейс*.

Узел (Node). Любое устройство в сети: компьютер, маршрутизатор или сервер.

Устройство CSU/DSU (Channel Service Unit/Digital Service Unit). Устройство, которое соединяет оборудование сети LAN (маршрутизатор) с цифровой телефонной линией.

Устройство MAU (Multistation Access Unit). Сети Token Ring имеют конфигурацию «звезда». Устройство доступа MAU предоставляет логическое кольцо, на котором работает сеть, и обеспечивает центральную связь между узлами.

Устройство проверки сигнала (Breakout Box). Устройство, проверяющее, поступает ли сигнал от подключенного к маршрутизатору устройства CSU/DSU.

Утилита ping (Packet InterNet Groper). Утилита, которая используется для тестирования соединения между узлами (хостами, серверами или маршрутизаторами) в сети IP.

Циклическая проверка избыточности (Cyclical Redundancy Check), или *контрольная сумма*. Концевая метка, добавляемая к каждому кадру протоколами канального уровня модели OSI для проверки, все ли кадры получены без ошибок. Как правило, это математический расчет, который производится сначала компьютером-отправителем, а затем компьютером-получателем. Если результаты двух проверок совпадают, значит, кадр доставлен без повреждений.

Широковещательный шторм (Broadcast Storms). Ситуация, при которой сеть Ethernet переполняется широковещательными сообщениями.

Шлюз (Gateway). Программно-аппаратный комплекс, применяемый для связи между сетями, которые работают с разными сетевыми протоколами, то есть требуют сопоставления протоколов, например для связи между компьютером IBM AS400 и сетью LAN на базе PC.

Шлюз по умолчанию (Default Gateway). Адрес интерфейса маршрутизатора, к которому подсоединена сеть LAN. Каждое устройство в сети LAN использует адрес данного интерфейса в качестве шлюза по умолчанию.

Ячейки (Cells). Пакеты данных фиксированного размера, которые задействуются в сетях с асинхронной передачей. См. также *Режим асинхронной передачи*.

Предметный указатель

K

M

H

O

П

Джо Хабракен

Маршрутизаторы Cisco
Практическое применение

Главный редактор *Мовчан Д. А.*
Перевод *Осипов А. И., Федосеев Р. В.*
Выпускающий редактор *Левицкая Т. В.*
Технический редактор *Александрова О. С.*
Верстка *Дудатий А. М.*
Графика *Шаклунов А. К.*
Дизайн обложки *Панкусова Е. Н.*

Гарнитура «Петербург». Печать офсетная.
Усл. печ. л. 20. Тираж 3000 экз. Зак. №

Издательство «ДМК Пресс», 105023, Москва, пл. Журавлева, д. 2/8.
Электронные адреса: www.dmkpress.ru, info@dmk.ru

Отпечатано в ГУП «Чеховский полиграфический комбинат»
142300, г. Чехов, ул. Полиграфистов, 1.